

# **ESCUELA POLITÉCNICA NACIONAL**

## **FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA**

### **ANÁLISIS DE LA SEGURIDAD DE APLICACIONES WEB CRÍTICAS DEL MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO**

#### **PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN**

**MILTON JOSÉ TITUAÑA VILLA**  
milton.tituana@hotmail.com

**DIRECTOR: MSc. GABRIEL ROBERTO LÓPEZ FONSECA**  
gabriel.lopez@epn.edu.ec

**CO-DIRECTOR: MSc. FRANKLIN LEONEL SÁNCHEZ CATOTA**  
franklin.sanchez@epn.edu.ec

Quito, julio 2017

## **DECLARACIÓN**

Yo Milton José Tituaña Villa, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

---

Milton José Tituaña Villa

## **CERTIFICACIÓN**

Certifico que el presente trabajo fue desarrollado por Milton José Tituaña Villa, bajo mi supervisión.

---

**MSc. Gabriel López**  
**DIRECTOR DEL TRABAJO DE TITULACIÓN**

---

**MSc. Franklin Sánchez**  
**CO-DIRECTOR DEL TRABAJO DE TITULACIÓN**

## **AGRADECIMIENTOS**

Agradezco a mis padres Salomón y Lilia los mejores del mundo, por todo su amor, comprensión y ser guía en mi vida personal y al apoyo incondicional que me brindaron en mi vida académica, a mi ñaño Santi por ser un ejemplo de persona, me animó y ayudó cuando más lo necesitaba, los pilares fundamentales que permitieron culminar con éxito este objetivo profesional.

Al MSc. Gabriel López y al MSc. Franklin Sánchez por su paciencia y ayuda, por brindarme sus conocimientos y tiempo para guiarme a lo largo del desarrollo de este trabajo de titulación.

A toda mi familia, amigos y personas especiales que estuvieron presentes en los momentos difíciles de mi vida que me animaron y alentaron para poder cumplir con este sueño.

Al Ing. Diego Aguirre y al Departamento de Producción de la Dirección Metropolitana de Informática, por la asesoría y facilidades brindadas durante el desarrollo del presente trabajo de titulación.

Finalmente quiero agradecer a todos los profesores que impartieron sus conocimientos y dedicación para formarnos como futuros profesionales.

*Milton*

## DEDICATORIA

Dedico este trabajo de titulación a mi papi Salomón, ya que por su esfuerzo y trabajo, su sueño y el mío se volvieron realidad; y a pesar de no estar presente físicamente, sé que siempre ha estado conmigo para guiarme y cuidarme.

A mi mami Lilia por demostrarme de manera incondicional su amor y comprensión, por haberme soportado todo el tiempo, por creer en mí, por ser mi guía y apoyo siempre, por ser la persona más importante en mi vida.

A mi ñaño Santi por sus acciones ejemplares, por brindarme su amistad, conocimiento y ayuda cuando más lo necesitaba.

A mi familia y amigos por estar presentes en los momentos buenos y sobre todo en los momentos difíciles de mi vida, por brindarme la fortaleza y el coraje necesario para culminar este trabajo de titulación.

*Milton*

## CONTENIDO

DECLARACIÓN .....	i
CERTIFICACIÓN .....	ii
AGRADECIMIENTOS .....	iii
DEDICATORIA.....	iv
CONTENIDO.....	v
ÍNDICE DE FIGURAS .....	xi
ÍNDICE DE TABLAS .....	xvii
RESUMEN .....	xviii
PRESENTACIÓN.....	xix
CAPÍTULO 1 .....	1
MARCO TEÓRICO.....	1
1.1. INTRODUCCIÓN .....	1
1.2. SEGURIDAD DE LA INFORMACIÓN .....	2
1.2.1. DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN .....	2
1.2.2. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN .....	3
1.2.3. IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN.....	4
1.2.4. ATACANTES .....	4
1.3. SEGURIDAD EN APLICACIONES WEB .....	5
1.3.1. DEFINICIÓN DE SEGURIDAD EN APLICACIONES WEB .....	5
1.3.2. IMPORTANCIA DE LA SEGURIDAD EN APLICACIONES WEB.....	6
1.3.3. VULNERABILIDADES, AMENAZAS, RIESGOS Y ATAQUES ASOCIADOS CON APLICACIONES WEB .....	6
1.4. HACKING ÉTICO .....	11
1.4.1. DEFINICIÓN DE HACKING ÉTICO .....	11
1.4.2. TIPOS DE HACKING ÉTICO.....	12
1.5. METODOLOGÍA Y HERRAMIENTAS.....	12
1.5.1. METODOLOGÍA.....	13
1.5.2. HERRAMIENTAS .....	17

CAPÍTULO 2 .....	24
SITUACIÓN ACTUAL Y REQUERIMIENTOS.....	24
2.1. MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO .....	24
2.2. PLAN ESTRATÉGICO .....	24
2.2.1. MISIÓN.....	24
2.2.2. VISIÓN .....	24
2.2.3. OBJETIVOS ESTRATÉGICOS.....	24
2.2.4. POLÍTICAS GENERALES .....	25
2.2.5. ESTRUCTURA ORGÁNICA DEL MDMQ.....	27
2.2.6. DIRECCIÓN METROPOLITANA DE INFORMÁTICA .....	27
2.3. APLICACIONES Y SERVICIOS WEB QUE PRESTA EL MDMQ .....	29
2.3.1. PORTAL DEL MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO.....	30
2.3.2. AGENCIA PÚBLICA DE NOTICIAS DE QUITO .....	30
2.3.3. LICENCIA METROPOLITANA ÚNICA PARA EL EJERCICIO DE ACTIVIDADES ECONÓMICAS (LUAE) EN LÍNEA.....	31
2.3.4. SECRETARÍA DE EDUCACIÓN, RECREACIÓN Y DEPORTE.....	32
2.3.5. INFORME DE REGULACIÓN METROPOLITANA (IRM).....	33
2.3.6. INFORME DE COMPATIBILIDAD DE USO DE SUELOS (ICUS).....	34
2.3.7. SISTEMA IMPOSITIVO MUNICIPAL DE QUITO – DECLARACIÓN DE PATENTES.....	34
2.3.8. SISTEMA DE PAGO DE IMPUESTOS POR INTERNET .....	35
2.3.9. SISTEMA INTEGRADO DE REGISTRO CATASTRAL .....	35
2.3.10. RADIO MUNICIPAL.....	36
2.4. ANÁLISIS DE LA SITUACIÓN ACTUAL .....	37
2.4.1. DECLARACIÓN DE APLICABILIDAD (SoA).....	37
2.5. ANÁLISIS DE APLICACIONES WEB CRÍTICAS .....	46
2.5.1. MATRIZ DE DEPENDENCIAS .....	46
2.5.2. PRIORIDAD DE LOS SERVICIOS .....	48
2.6. APLICACIONES WEB CRÍTICAS.....	49
2.6.1. MATRIZ DE IMPACTO ENTRE APLICACIONES/SISTEMAS.....	52

CAPÍTULO 3 .....	56
PRUEBAS DE PENETRACIÓN: IMPLEMENTACIÓN DE EVALUACIÓN DE SEGURIDAD .....	56
3.1. RECOPIACIÓN DE INFORMACIÓN .....	58
3.1.1. DESCUBRIMIENTO CON MOTORES DE BÚSQUEDA Y RECONOCIMIENTO POR FUGAS DE INFORMACIÓN (OTG-INFO-001).....	58
3.1.2. FINGERPRINT DEL SERVIDOR WEB (OTG-INFO-002).....	60
3.1.3. REVISIÓN DE META-ARCHIVOS POR FUGAS DE INFORMACIÓN (OTG-INFO-003) .....	62
3.1.4. ENUMERAR APLICACIONES EN EL SERVIDOR WEB (OTG-INFO-004).....	63
3.1.5. REVISAR COMENTARIOS EN LA PAGINA WEB Y METADATOS POR FUGAS DE INFORMACIÓN (OTG-INFO-005) .....	64
3.1.6. IDENTIFICAR LOS PUNTOS DE ENTRADA DE LA APLICACIÓN (OTG-INFO-006) .....	66
3.1.7. MAPEAR RUTAS DE EJECUCIÓN A TRAVÉS DE LA APLICACIÓN (OTG-INFO-007) .....	67
3.1.8. FINGERPRINT EL FRAMEWORK DE LA APLICACIÓN WEB (OTG-INFO-008) .....	68
3.1.9. FINGERPRINT A LA APLICACIÓN WEB (OTG-INFO-009).....	69
3.2. PRUEBAS DE GESTIÓN DE LA CONFIGURACIÓN Y LA IMPLEMENTACIÓN .....	71
3.2.1. PRUEBA DE CONFIGURACIÓN DE RED/INFRAESTRUCTURA (OTG-CONFIG-001).....	71
3.2.2. PRUEBA DE CONFIGURACIÓN DE LA PLATAFORMA DE LA APLICACIÓN (OTG-CONFIG-002) .....	72
3.2.3. ARCHIVOS DE BACKUP Y NO REFERENCIADOS CON INFORMACIÓN SENSIBLE (OTG-CONFIG-004).....	74
3.2.4. ENUMERAR INTERFACES DE ADMINISTRACIÓN DE APLICACIONES Y DE INFRAESTRUCTURA (OTG-CONFIG-005) .....	74
3.2.5. PRUEBA DE MÉTODOS HTTP (OTG-CONFIG-006) .....	75



3.2.6. PRUEBA DE SEGURIDAD DE TRANSPORTE ESTRICTO HTTP - HSTS (OTG-CONFIG-007) .....	76
3.2.7. PRUEBA DE POLÍTICA DE DOMINIO CRUZADO RIA (OTG-CONFIG-008).....	78
3.3. PRUEBAS DE AUTORIZACIÓN .....	79
3.3.1. PRUEBA DE DIRECTORIO/PATH TRAVERSAL (OTG-AUTHZ-001) ..	79
3.3.2. PRUEBA DE ESCALAMIENTO DE PRIVILEGIOS (OTG-AUTHZ-003)	81
3.3.3. PRUEBA DE REFERENCIA DIRECTA INSEGURA A OBJETOS (OTG-AUTHZ-004).....	82
3.4. PRUEBAS DE GESTIÓN DE SESIONES.....	83
3.4.1. PRUEBA DE FALSIFICACIÓN DE PETICIONES EN SITIOS CRUZADOS - CSRF (OTG-SESS-005).....	83
3.5. PRUEBAS DE VALIDACIÓN DE ENTRADA .....	84
3.5.1. PRUEBA DE CROSS SITE SCRIPTING REFLEJADO (OTG-INPVAL-001).....	85
3.5.2. PRUEBA DE CROSS SITE SCRIPTING ALMACENADO (OTG-INPVAL-002).....	86
3.5.3. PRUEBA DE MANIPULACIÓN HTTP (OTG-INPVAL-003) .....	87
3.5.4. PRUEBA DE INYECCIÓN SQL (OTG-INPVAL-005).....	89
3.5.5. PRUEBA DE INCLUSIÓN LOCAL DE ARCHIVOS (OTG-INPVAL-012)	91
3.5.6. PRUEBA DE INYECCIÓN DE COMANDOS (OTG-INPVAL-013).....	92
3.6. MANEJO DE ERRORES.....	93
3.6.1. ANÁLISIS DE CÓDIGOS DE ERROR (OTG-ERR-001).....	94
3.7. CRIPTOGRAFÍA .....	96
3.7.1. PRUEBA DE CIFRADO TLS/SSL DÉBIL Y PROTECCIÓN INSUFICIENTE DE CAPA DE TRANSPORTE (OTG-CRYPST-001) .....	96
3.7.2. PRUEBA DE INFORMACIÓN SENSIBLE ENVIADA POR CANALES SIN ENCRIPtar (OTG-CRYPT-003).....	98
3.8. OBJETIVOS DE LAS PRUEBAS DE SEGURIDAD Y HERRAMIENTAS A UTILIZAR PARA ALCANZAR LOS MISMOS .....	99
3.9. DISEÑO DEL AMBIENTE DE PRUEBAS .....	102

CAPÍTULO 4 .....	105
RESULTADOS .....	105
4.1. RESULTADO DE PRUEBAS PARA EL PORTAL WEB DEL MDMQ .....	105
4.1.1. RESULTADO DE PRUEBAS: RECOPIACIÓN DE INFORMACIÓN .	105
4.1.2. RESULTADO DE PRUEBAS: GESTIÓN DE LA CONFIGURACIÓN Y LA IMPLEMENTACIÓN .....	116
4.1.3. RESULTADO DE PRUEBAS: AUTORIZACIÓN .....	122
4.1.4. RESULTADO DE PRUEBAS: GESTIÓN DE SESIONES .....	124
4.1.5. RESULTADO DE PRUEBAS: VALIDACIÓN DE ENTRADA .....	124
4.1.6. RESULTADO DE PRUEBAS: MANEJO DE ERRORES .....	129
4.1.7. RESULTADO DE PRUEBAS: CRIPTOGRAFÍA .....	130
4.2. RESULTADO DE PRUEBAS PARA EL PORTAL DE PAGO DE IMPUESTOS POR INTERNET .....	131
4.2.1. RESULTADO DE PRUEBAS: RECOPIACIÓN DE INFORMACIÓN .	131
4.2.2. RESULTADO DE PRUEBAS: GESTIÓN DE LA CONFIGURACIÓN Y LA IMPLEMENTACIÓN .....	140
4.2.3. RESULTADO DE PRUEBAS: AUTORIZACIÓN .....	145
4.2.4. RESULTADO DE PRUEBAS: GESTIÓN DE SESIONES .....	147
4.2.5. RESULTADO DE PRUEBAS: VALIDACIÓN DE ENTRADA .....	147
4.2.6. RESULTADO DE PRUEBAS: MANEJO DE ERRORES .....	152
4.2.7. RESULTADO DE PRUEBAS: CRIPTOGRAFÍA .....	153
4.3. ANÁLISIS DE RESULTADO PARA EL PORTAL WEB DEL MDMQ .....	154
4.4. ANÁLISIS DE RESULTADO PARA EL PORTAL DE PAGO DE IMPUESTOS POR INTERNET .....	158
4.5. MITIGACIÓN DE VULNERABILIDADES PARA EL PORTAL WEB DEL MDMQ .....	162
4.6. MITIGACIÓN DE VULNERABILIDADES PARA EL PORTAL DE PAGO DE IMPUESTOS POR INTERNET .....	164
4.7. VULNERABILIDADES ENCONTRADAS, COMANDOS Y HERRAMIENTAS UTILIZADAS EN EL DESARROLLO DEL TRABAJO .....	166
CAPÍTULO 5 .....	173

CONCLUSIONES Y RECOMENDACIONES .....	173
5.1. CONCLUSIONES.....	173
5.2. RECOMENDACIONES .....	175
REFERENCIAS BIBLIOGRÁFICAS .....	178
ANEXOS .....	191

## ÍNDICE DE FIGURAS

Figura 1.1 Principios de la seguridad de la información .....	4
Figura 1.2 Relación entre vulnerabilidad, amenaza y riesgo .....	7
Figura 1.3 Ataque Man in the middle (MITM) .....	8
Figura 1.4 Captura de tráfico con wireshark .....	8
Figura 1.5 Ataque de inyección SQL.....	9
Figura 1.6 CSRF .....	9
Figura 1.7 Procedimiento CSRF .....	10
Figura 1.8 Ataque de Denegación de Servicio (DoS).....	10
Figura 1.9 Sitio web deformado ( <i>defaced</i> ) .....	11
Figura 1.10 Diferencias entre tipos de <i>hacking</i> ético.....	13
Figura 1.11 Flujo de trabajo del entorno de pruebas OWASP.....	14
Figura 1.12 Fases del hacking .....	17
Figura 1.13 Interfaz de trabajo Kali Rolling 2016.2.....	18
Figura 2.1 Estructura Orgánica del MDMQ .....	28
Figura 2.2 Portal del MDMQ.....	30
Figura 2.3 Portal de prensa del MDMQ.....	31
Figura 2.4 Portal de la LUAE.....	32
Figura 2.5 Secretaría de Educación, Recreación y Deportes del MDMQ.....	32
Figura 2.6 Informe de Regulación Metropolitana.....	33
Figura 2.7 Informe de compatibilidad de uso de suelos .....	34
Figura 2.8 Sistema de Patentes .....	35
Figura 2.9 Sistema de pago de impuestos por Internet.....	35
Figura 2.10 SIREC-Q .....	36
Figura 2.11 Radio Municipal.....	37
Figura 3.1 Búsqueda avanzada en Google .....	60
Figura 3.2 Fingerprint del servidor web con netcat.....	61
Figura 3.3 Fingerprint con greghatcher.com.....	61
Figura 3.4 Archivo robots.txt.....	62

Figura 3.5 Descarga del archivo robots.txt con wget.....	63
Figura 3.6 Enumerando servicios con nmap .....	64
Figura 3.7 Comentarios en el código de una página web .....	65
Figura 3.8 Revisión de metadatos con desenmascara.me.....	65
Figura 3.9 Solicitud POST analizada con Burp Suite .....	66
Figura 3.10 Spidering con OWASP ZAP .....	68
Figura 3.11 Spidering con Burp Suite.....	68
Figura 3.12 Fingerprinting del framework de una aplicación web.....	69
Figura 3.13 Fingerprint de una aplicación con wappalyzer .....	70
Figura 3.14 Diagrama de infraestructura de red.....	71
Figura 3.15 Módulos activos en un servidor Apache.....	73
Figura 3.16 Modulos/features activos en un servidor IIS.....	73
Figura 3.17 Interfaz de administrador.....	75
Figura 3.18 Métodos HTTP que soporta un servidor web .....	76
Figura 3.19 Implementación de HSTS .....	77
Figura 3.20 Análisis de HSTS con Qualys Inc.....	78
Figura 3.21 Contenido del archivo crossdomain.xml.....	79
Figura 3.22 Ataque de path traversal .....	80
Figura 3.23 Path traversal con dotdotpwn.....	81
Figura 3.24 Escalamiento de privilegios con OWASP ZAP .....	82
Figura 3.25 Modificación de parámetro, prueba referencia directa insegura a objetos .....	83
Figura 3.26 Cross site request forgery .....	84
Figura 3.27 XSS reflejado con xsser .....	86
Figura 3.28 XSS Reflejado con el navegador.....	86
Figura 3.29 XSS almacenado.....	87
Figura 3.30 Manipulación HTTP .....	88
Figura 3.31 Error en la base de datos .....	89
Figura 3.32 Inyección SQL.....	90
Figura 3.33 Inyección SQL con sqlmap.....	91
Figura 3.34 LFI con un navegador web.....	92

Figura 3.35 Inyección de comando .....	93
Figura 3.36 Inyección de comandos con commix.....	94
Figura 3.37 Mensaje de error no personalizado .....	95
Figura 3.38 Mensaje de error generado con telnet.....	95
Figura 3.39 Verificación SSL/TLS con nmap.....	97
Figura 3.40 Información de seguridad de un sitio web .....	97
Figura 3.41 Credenciales en texto claro con Nessus .....	98
Figura 3.42 Tráfico encriptado visto con wireshark .....	99
Figura 3.42 Esquema de las pruebas de penetración desde dentro de la organización .....	103
Figura 3.42 Esquema de pruebas desde fuera de la organización .....	103
Figura 4.1 Búsqueda de subdominios .....	106
Figura 4.2 Búsqueda de interfaz de administración Joomla.....	107
Figura 4.3 Búsqueda de interfaz de administración Wordpress .....	107
Figura 4.4 Búsqueda de interfaz de administración Drupal.....	107
Figura 4.5 Búsqueda de páginas propensas a XSS e inyección SQL.....	108
Figura 4.6 Búsqueda de la versión y tipo de Servidor Web.....	108
Figura 4.7 Fingerprint del servidor web con httpprint .....	109
Figura 4.8 Fingerprint del servidor web con gregthatcher.com .....	109
Figura 4.9 Descarga y visualización de robots.txt con wget y tail respectivamente	110
Figura 4.10 Visualización de robots.txt con el navegador web.....	111
Figura 4.11 Enumerando aplicaciones con nmap .....	111
Figura 4.12 Metadatos con desenmascara.me .....	112
Figura 4.13 Revisión de comentarios en el código fuente de la página web.....	112
Figura 4.14 Solicitud con el método GET .....	113
Figura 4.15 Spidering con Burp Suite.....	113
Figura 4.16 Spidering con ZAP .....	114
Figura 4.17 Fingerprint del framework de la aplicación .....	115
Figura 4.18 Fingerprint a la aplicación web con wappalyzer .....	115
Figura 4.19 Fingerprint a la aplicación web con whatweb .....	116
Figura 4.20 Diagrama de red.....	117

Figura 4.21 Interfaz de administración Joomla.....	119
Figura 4.22 Métodos configurados en el servidor web .....	120
Figura 4.23 Implementación de HSTS .....	121
Figura 4.24 Resultado de SSL Server Test.....	121
Figura 4.25 Archivo crossdomain.xml .....	121
Figura 4.26 Directorio traversal con dotdotpwn .....	122
Figura 4.27 Directorio traversal de forma manual .....	122
Figura 4.28 Página sin cambio de parámetro id .....	123
Figura 4.29 Página con el parámetro id modificado .....	123
Figura 4.30 XSS con xsser.....	124
Figura 4.31 XSS con el navegador.....	125
Figura 4.32 Respuesta al método TRACE .....	126
Figura 4.33 Respuesta al método PUT .....	126
Figura 4.34 Error en la consulta .....	127
Figura 4.35 SQLi con sqlmap .....	127
Figura 4.36 LFI con dotdotpwn.....	128
Figura 4.37 Inyección de comandos con commix .....	128
Figura 4.38 Mensaje de error de página inexistente .....	129
Figura 4.39 Petición de una página inexistente con telnet .....	129
Figura 4.40 Servicios que utilizan SSL/TLS .....	130
Figura 4.41 Revisión manual del certificado.....	130
Figura 4.42 Prueba de SSL/TLS con Nessus.....	131
Figura 4.43 Búsqueda de subdominios .....	132
Figura 4.44 Búsqueda de interfaz de administración Joomla.....	132
Figura 4.45 Búsqueda de interfaz de administración Wordpress .....	133
Figura 4.46 Búsqueda de interfaz de administración Drupal.....	133
Figura 4.47 Búsqueda de páginas propensas a XSS e inyección SQL.....	133
Figura 4.48 Búsqueda de la versión y tipo de Servidor Web.....	134
Figura 4.49 Fingerprint del servidor web con httprint .....	134
Figura 4.50 Fingerprint del servidor con wappalyzer.....	135
Figura 4.51 Descarga de robots.txt con wget .....	135

Figura 4.52 Visualización de robots.txt con ZAP .....	136
Figura 4.53 Enumerando aplicaciones con nmap .....	136
Figura 4.54 Metadatos con desenmascara.me .....	137
Figura 4.55 Revisión de comentarios en el código fuente de la página web .....	137
Figura 4.56 Solicitud con el método post .....	138
Figura 4.57 Spidering con Burp Suite.....	138
Figura 4.58 Fingerprint del framework de la aplicación .....	139
Figura 4.59 Fingerprint a la aplicación web con whatweb .....	140
Figura 4.60 Fingerprint a la aplicación web con BuiltWith .....	140
Figura 4.62 Ingreso a interfaz de administración Joomla .....	142
Figura 4.63 Ingreso a interfaz de administración WordPress.....	142
Figura 4.64 Ingreso a interfaz de administración Drupal .....	143
Figura 4.65 Métodos configurados en el servidor web .....	143
Figura 4.66 Implementación de HSTS .....	144
Figura 4.67 Resultado de SSL Server Test.....	144
Figura 4.68 Archivo crossdomain.xml .....	145
Figura 4.69 Path traversal con dotdotpwn.....	145
Figura 4.70 Path traversal modificando la URL .....	146
Figura 4.71 Página sin modificar parámetro.....	146
Figura 4.72 Página sin modificar parámetro.....	147
Figura 4.73 XSS con xsser .....	147
Figura 4.74 XXS en la URL .....	148
Figura 4.75 XSS en la entrada de datos .....	148
Figura 4.76 Solicitud con el método TRACE .....	149
Figura 4.77 Solicitud con el método PUT .....	149
Figura 4.78 Inyección SQL de forma manual .....	150
Figura 4.79 SQLi con sqlmap.....	150
Figura 4.80 LFI con dotdotpwn.....	151
Figura 4.81 Inyección de comandos con commix.....	151
Figura 4.82 Mensaje de error de página inexistente .....	152
Figura 4.83 Petición de una página inexistente con telnet .....	152



Figura 4.84 Información sobre SSL/TLS .....	153
Figura 4.85 Información SSL/TLS con sslyze.....	153
Figura 4.86 Captura de tráfico con wireshark.....	154

## ÍNDICE DE TABLAS

Tabla 2.1 Matriz de dependencia .....	47
Tabla 2.2 Aplicaciones/sistemas por prioridad .....	49
Tabla 2.3 Matriz de impacto .....	54
Tabla 2.4 Matriz de impacto sobre la organización .....	55
Tabla 3.1 Objetivos y herramientas utilizadas .....	102
Tabla 3.2 Descripción de hardware y software del equipo atacante .....	104
Tabla 4.1 Módulos del servidor web .....	118
Tabla 4.2 Features del servidor web .....	141
Tabla 4.3 Análisis de resultados portal MDMQ .....	158
Tabla 4.4 Análisis de resultados Pago de Impuestos por Internet.....	162
Tabla 4.5 Remediación de vulnerabilidad del portal del MDMQ.....	164
Tabla 4.6 Remediación de vulnerabilidad para Pago de Impuestos por Internet ....	165
Tabla 4.6 Vulnerabilidades encontradas, herramientas utilizadas portal web MDMQ .....	168
Tabla 4.7 Vulnerabilidades encontradas, herramientas utilizadas portal pagos por Internet .....	171
Tabla 4.8 Vulnerabilidades conocidas para el software encontrado en las pruebas de seguridad.....	172

## RESUMEN

El presente trabajo de titulación tiene por objetivo realizar un análisis de seguridad en las aplicaciones y portales web que dispone el Municipio del Distrito Metropolitano de Quito, con el propósito de verificar si en estos se presenten o no vulnerabilidades que puedan ser explotadas. El trabajo consta de los siguientes capítulos.

En el primer capítulo se revisa la importancia de la seguridad de la información, así como la importancia de mantener y desarrollar aplicaciones web seguras, se habla sobre los principales riesgos y ataques a los que se encuentran expuestas por brindar sus servicios a través del Internet. Se habla sobre la metodología y herramientas utilizadas para el desarrollo del trabajo.

En el segundo capítulo se identifican las 2 direcciones IP que alojan a las aplicaciones web más críticas, sobre las cuales se realiza el test de penetración para identificar vulnerabilidades tecnológicas. Para esto se analiza la situación actual de las aplicaciones que presta el Municipio del Distrito Metropolitano de Quito, se analiza la dependencia que existe entre aplicaciones y se hace un análisis de prioridades..

En el tercer capítulo se describen las diferentes pruebas de penetración que se realizan a las aplicaciones web críticas que presta el Municipio del Distrito Metropolitano de Quito, estas se seleccionan de todas las pruebas que se detallan en la guía OWASP V4 (Proyecto Abierto de Seguridad de Aplicaciones Web), aquellas que se adapten más al funcionamiento de las mismas.

En el cuarto capítulo se documentan las pruebas de seguridad realizadas, así como los resultados obtenidos de las mismas. Se presenta también el respectivo análisis de resultados, los cuales permiten identificar vulnerabilidades o determinar si se tratan de falsos positivos. También se proponen las formas de mitigar las vulnerabilidades encontradas. Finalmente, en el quinto capítulo se listan las conclusiones y recomendaciones que se obtuvieron durante el desarrollo del trabajo.

## PRESENTACIÓN

La información es el activo más importante para las organizaciones y empresas, el uso y transporte adecuado de esta información es de vital importancia para la actividad fundamentales del negocio. Actualmente las actividades de los negocios se las realizan casi en su totalidad a través del Internet por medio de aplicaciones y portales web, volviendo aún más crítica la forma de compartir y mantener segura la información. Es por este motivo que se necesita verificar que tan seguros son los procedimientos y métodos que han sido implementados en las aplicaciones y portales web para el intercambio de información.

Son varios los mecanismos aplicables para evaluar la seguridad en aplicaciones y portales web, así como para desarrollar y mantener aplicaciones seguras, con el propósito de garantizar la disponibilidad, integridad y confidencialidad de la información.

En el presente trabajo, se realiza un análisis de vulnerabilidades en las aplicaciones web críticas que presta el Municipio del Distrito Metropolitano de Quito, para esto se realizan varias pruebas de seguridad en dichas aplicaciones con el fin de identificar vulnerabilidades tecnológicas.

El diseño de las pruebas de seguridad se basó en la Guía del Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP V4), identificando primeramente aquellas pruebas que son aplicables al modelo y funcionamiento de las aplicaciones web que presta el Municipio del Distrito Metropolitano de Quito.

Por último, se realiza el análisis de los resultados obtenidos del test de penetración, esto con el objetivo de identificar las vulnerabilidades o los falsos positivos, y así poder proponer la forma de remediar las mismas.

# CAPÍTULO 1

## MARCO TEÓRICO

En este capítulo se realiza una rápida descripción acerca de la Seguridad de la Información, su importancia y los principales elementos que intervienen en la misma, además se habla sobre aspectos importantes de Seguridad en Aplicaciones Web.

En la sección 1.4 se habla acerca del Hacking Ético y los principales métodos de Pruebas de Penetración.

En la sección 1.5 se definen las vulnerabilidades, amenazas, ataques y atacantes más notables que afectan a la Seguridad en Aplicaciones Web.

Finalmente se detallan la metodología y las herramientas para el desarrollo de la investigación.

### 1.1. INTRODUCCIÓN

En este mundo donde la tecnología crece firme y continuamente de una forma dominante, la interconectividad e interoperabilidad de redes se ha vuelto cada vez más necesarias, incluso las empresas y organizaciones han puesto en manos de las TIC<sup>1</sup> el funcionamiento de sus negocios. A través de las redes corporativas y del mismo modo en el Internet, se transmiten a cada segundo grandes volúmenes de datos, información que es vital para empresas y organizaciones o simplemente de una persona que desea leer su correo electrónico o hacer una consulta en la red. Hoy en día es común escuchar sobre la pérdida y fuga de información, hackeo, caída de servicio, fraudes, espionaje y sabotaje electrónico<sup>2</sup>, etc. Esto se debe a la falta de preocupación con respecto a la seguridad de la información, y poca concientización de parte de las organizaciones para proteger su información.

---

<sup>1</sup> TIC son aquellas herramientas computacionales e informáticas que procesan, almacenan, resumen, recuperan y presentan información representada de la más variada forma.

<sup>2</sup> Borrar, suprimir o modificar sin autorización funciones o datos de la computadora con intención de obstaculizar el funcionamiento normal del sistema.

La implantación de controles de seguridad es una tarea importante que toda organización debe realizar, dichos controles proporcionan directrices y buenas prácticas de seguridad de la información en ámbitos como: políticas de seguridad, gestión de activos, control de acceso, seguridad física y ambiental, seguridad de las comunicaciones, etc., con el propósito de reducir al mínimo los riesgos de pérdida, robo o manipulación de la información.

Por lo anteriormente expuesto, la seguridad de la información se considera como una necesidad en la actualidad, entre sus principales objetivos se tiene: gestionar los incidentes de seguridad, monitorear activos con información crítica, generar análisis y reportes de vulnerabilidades, detectar incidentes de seguridad y mitigarlos, etc.

## **1.2. SEGURIDAD DE LA INFORMACIÓN [4], [22]-[24]**

### **1.2.1. DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN**

La seguridad informática comenzó a extenderse a otras áreas, es así que se convirtió en un dominio transversal para las TI.

Apareció entonces el concepto de Seguridad de la Información, mismo que considerará la data y los procesos que la generan. Hoy en día la información, junto a los procesos y sistemas, hardware y software, redes de comunicaciones, recursos humanos, etc., son activos de información muy importantes para una organización.

Los activos de información pueden ser bases de datos, archivos, contratos, acuerdos, manuales de usuarios, material de entrenamiento, planes de continuidad, cualquier componente tecnológico o humano que almacene información vital para la organización.

La seguridad de la información se puede definir como el conjunto de métodos y estrategias que las organizaciones ponen en práctica para proteger y defender sus activos de información, buscando mantener la confidencialidad, disponibilidad e integridad, componentes esenciales para mantener la competitividad y rentabilidad de la organización y la continuidad del negocio.

Los activos de información son la parte más importante de una organización[4][5], por esta razón deben ser gestionados, asegurados y protegidos contra cualquier incidente que signifique una amenaza o riesgo.

### 1.2.2. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información consiste en proteger los activos de la organización en contra problemas de integridad, lectura, revelación, uso ilegítimo, y accesos no autorizados, etc.

Todas estas medidas se enfocan en los siguientes principios.

- **Confidencialidad:** La información puede ser accedida sólo por el personal autorizado; quiere decir que no se encuentra disponible para personas, entidades o procesos no autorizados.
- **Integridad:** Asegurar que la información se mantenga fiable, exacta, completa e inalterada, desde su origen, hasta su destino.
- **Disponibilidad:** La información debe estar siempre disponible cuando el personal o proceso autorizado así lo requiera.
- **Autenticidad:** Verifica si la identidad de un individuo que va hacer un intercambio de información es legítima; para esto se realiza una prueba de autenticación<sup>3</sup>.
- **Accountability:** Cada persona es responsable o propietaria de un activo de información; con este principio se pueden rastrear las operaciones hechas por esta persona sobre el activo que es de su propiedad.
- **No repudio:** Con este principio se demuestra que una operación o evento ha tenido lugar; es decir, no se puede negar después que la persona o entidad realizó dicha operación.

En la figura 1.1 se muestran los principios de la seguridad de la información, se puede ver que tres de ellos tienen un vínculo más estrecho y por lo que son considerados como principales.

---

<sup>3</sup> La autenticación es el acto o proceso para el establecimiento o confirmación de algo (o alguien) como real.

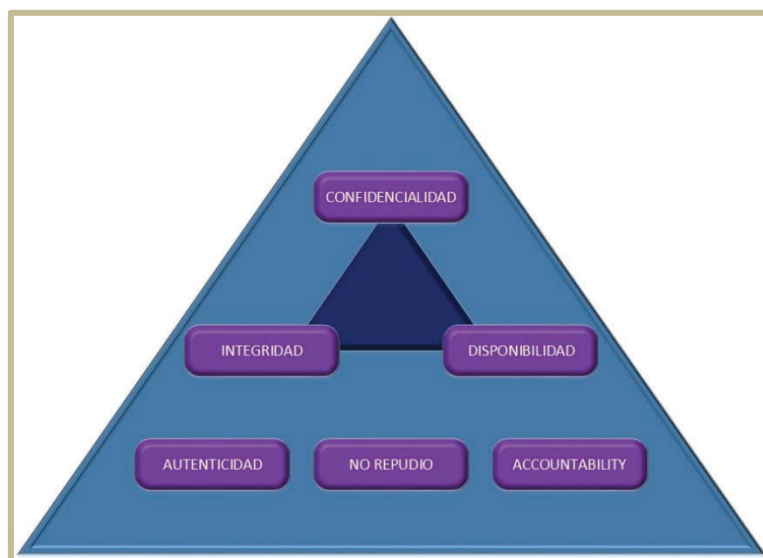


Figura 1.1 Principios de la seguridad de la información [8]

### 1.2.3. IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN

Debido a los avances de las TIC y las comunicaciones descentralizadas, las organizaciones se ven en la necesidad de proteger y asegurar la información cuya alteración, divulgación, destrucción o pérdida afecte a la continuidad del negocio y que pueda afectar a la entidad tanto económicamente como al prestigio de la misma.

La seguridad de la información es un proceso continuo que compromete no solamente los aspectos tecnológicos de una entidad, sino que envuelve también al aspecto humano, es por eso que se necesita una buena gestión y configuración de la infraestructura tecnológica, así como una debida capacitación hacia los empleados que se enfoque en concientizar acerca de las posibles amenazas y riesgos a los que se encuentran expuesta nuestra información.

### 1.2.4. ATACANTES [42]-[45]

Un atacante es una persona con conocimientos en informática, programación, *networking*<sup>4</sup>, etc., que haciendo uso de diferentes herramientas tratan de ingresar a los sistemas informáticos de organizaciones con el fin de desestabilizar el sistema,

---

<sup>4</sup> *Networking* es la construcción, diseño y uso de una red, incluyendo la parte física, la selección y uso de protocolos de telecomunicaciones.



causar daño o simplemente por probar sus habilidades. Entre los atacantes más comunes podemos encontrar a los siguientes [42], [44]:

- *Script kiddie*: Es un término despectivo utilizado en la jerga de Internet para referirse a personas con falta de conocimiento en Informática, que hacen uso de herramientas y *scripts* desarrollados por otras personas para ocasionar daño a sistemas informáticos.
- *Cracker*: Es una persona con altos conocimientos en informática y utiliza los mismos para ingresar a los sistemas informáticos de manera ilegal con el único propósito de causar daño o por obtener tipo de beneficio.
- *Phreaker*: Son personas con gran conocimiento en sistemas telefónicos de todo tipo, utilizan estos conocimientos para manipular la red telefónica para acceder a servicios no autorizados, por ejemplo llamadas internacionales.
- *Spammer*: Son personas que hacen un envío masivo de correos conteniendo correos basura, enlaces y publicidad con la cual se puede beneficiar; estas direcciones de correo electrónico son robadas o compradas.
- *Phisher*: Es la persona que utiliza la ingeniería social o técnicas de spam para obtener información confidencial como números de tarjetas de crédito, cuentas bancarias, contraseñas, etc.
- *Hacker*: Es un atacante con gran conocimientos en tecnologías de la información, programación, bases de datos, telecomunicaciones, hardware, software, etc., que ingresan a los sistemas informáticos de terceras personas con el propósito de demostrar su conocimiento y habilidades, pero sin el ánimo de ocasionar daños en ellos.

### **1.3. SEGURIDAD EN APLICACIONES WEB [10], [11], [25]-[27]**

#### **1.3.1. DEFINICIÓN DE SEGURIDAD EN APLICACIONES WEB**

La seguridad en aplicaciones web es una rama de la seguridad de la información que se enfoca exclusivamente en proteger la confidencialidad, integridad y disponibilidad de los datos en sitios web, servicios web y aplicaciones web.

### **1.3.2. IMPORTANCIA DE LA SEGURIDAD EN APLICACIONES WEB [48]**

En la actualidad el Internet ha trascendido en la vida de las personas, así como en el ámbito laboral de las organizaciones. Desde el Internet se puede realizar absolutamente todo, compras, ventas, transacciones bancarias, consultas, acceso a redes sociales, que contienen mucha información muy importante para sus propietarios.

Este proceso de intercambio de información hace uso de una herramienta denominada aplicación web, la cual se conecta a un servidor web mediante una interfaz web<sup>5</sup> a través del Internet. Estas aplicaciones han ayudado al desarrollo político, social, económico y educativo por lo que cada vez se han convertido en aplicaciones más críticas, por esta y otras razones es importante desarrollar aplicaciones web seguras para poder compartir información.

### **1.3.3. VULNERABILIDADES, AMENAZAS, RIESGOS Y ATAQUES ASOCIADOS CON APLICACIONES WEB [38]-[41], [46], [47]**

Vulnerabilidad es una debilidad o falla presente en un sistema informático o red de información, la cual puede comprometer la seguridad del sistema. Las vulnerabilidades más comunes que se presentan en aplicaciones web son [38]-[40]:

- Software mal configurado
- Software desactualizado
- Falta de seguridad en archivos
- Irresponsabilidad
- Control de privilegios

Amenaza es todo evento o acción capaz de aprovecharse de las vulnerabilidades y que pueden ocasionar problemas de seguridad en el sistema. Las amenazas pueden ser internas o externas a nuestro sistema. Entre las amenazas más comunes se tiene las siguientes [40], [41]:

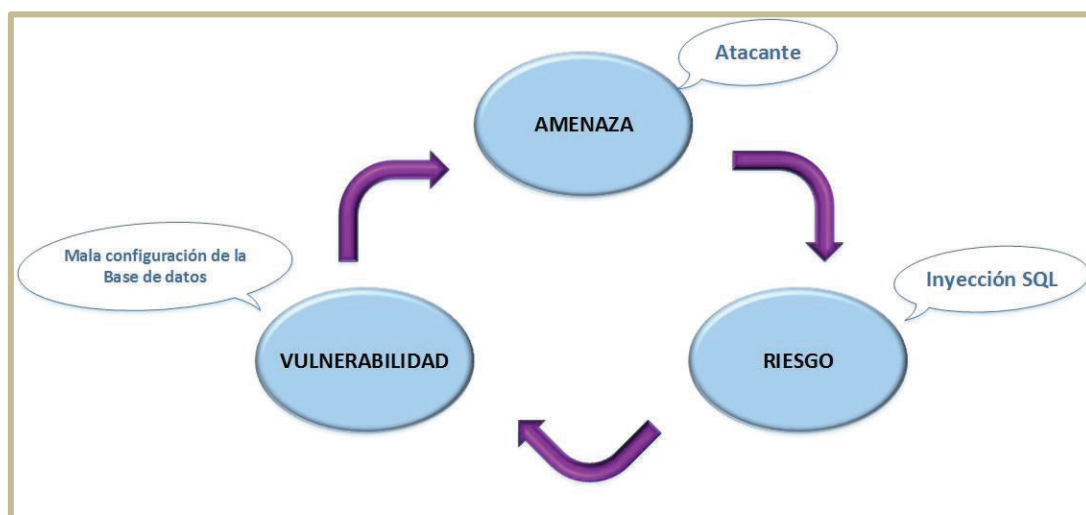
---

<sup>5</sup> Interfaz es un conjunto de elementos en la pantalla que permiten al usuario realizar acciones sobre el Sitio Web que está visitando.

- Malware, virus, spyware, troyanos
- Atacante
- Acceso no autorizado
- Interrupciones en el servicio
- Fallo en equipos
- Desastres naturales
- Negligencia

Riesgo es una medida probable en que una o varias amenazas potenciales se materialicen usando una vulnerabilidad, provocando un impacto con daños o pérdidas.

En la figura 1.2 se observa la relación entre vulnerabilidad, riesgo y la amenaza.



**Figura 1.2 Relación entre vulnerabilidad, amenaza y riesgo [12]**

Ataque es cualquier acción planeada por un individuo, que con el uso de herramientas pretende violar la seguridad del sistema. Los ataques más comunes son los siguientes [40], [46], [47]:

- Hombre en el medio: En inglés *Man in the middle* o MITM, es un ataque en el cual una persona puede alterar, leer y reenviar mensajes a voluntad, entre la víctima y el servidor.

La figura 1.3 muestra cómo se produce el ataque del hombre en el medio.

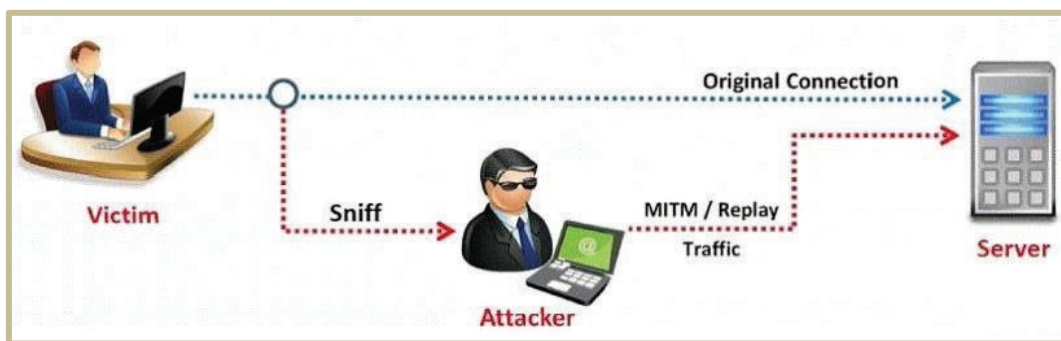


Figura 1.3 Ataque Man in the middle (MITM) [13]

- Análisis de tráfico: Con este procedimiento el atacante puede interceptar y observar la información y el tipo de datos que circula a través del canal de información, para este ataque se utilizan herramientas llamadas *sniffers*<sup>6</sup>. La figura 1.4 muestra una captura de tráfico de red con wireshark.

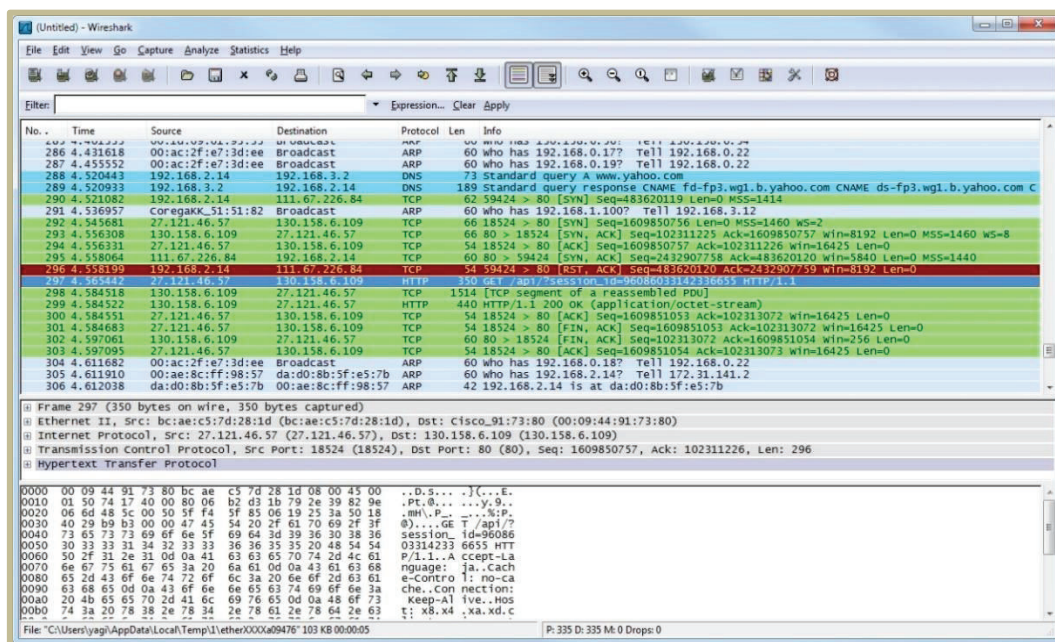


Figura 1.4 Captura de tráfico con wireshark [14]

- Suplantación de identidad: También conocido como *Phishing*, es un ataque que utiliza la Ingeniería Social<sup>7</sup>, el cual busca reunir información confidencial de la víctima, como contraseñas o números de tarjetas de crédito, para esto se hace pasar por una entidad de confianza en una supuesta comunicación oficial.

<sup>6</sup> *Sniffer* programa de captura de las tramas de una red de computadoras para su análisis.

<sup>7</sup> Ingeniería social son técnicas y habilidades sociales utilizadas para la obtención de información de terceros.

- Inyección SQL: Este ataque se produce cuando un usuario malicioso puede insertar comandos SQL en una consulta SQL, si la inyección es exitosa el atacante puede acceder, modificar, eliminar datos sensibles de la base de datos. En la figura 1.8 se presente el esquema de un ataque de inyección SQL.



Figura 1.5 Ataque de inyección SQL [16]

- Un ataque de falsificación de peticiones en sitios cruzados (*Cross Site Request Forgery* - CSRF), tiene como finalidad obligar al usuario a que él mismo realice acciones no deseadas en la aplicación en la que se encuentra autenticado. Este tipo de ataque se dirige únicamente al cambio de estado y no al robo de información. Un ataque exitoso de falsificación de petición en sitios cruzados puede hacer cambios de estado en la aplicación, como por ejemplo transferencia de dinero, cambiar dirección de correo o cambiar una contraseña. En la figura 1.5 y 1.6 se explica el procedimiento de un ataque de CSRF [21].

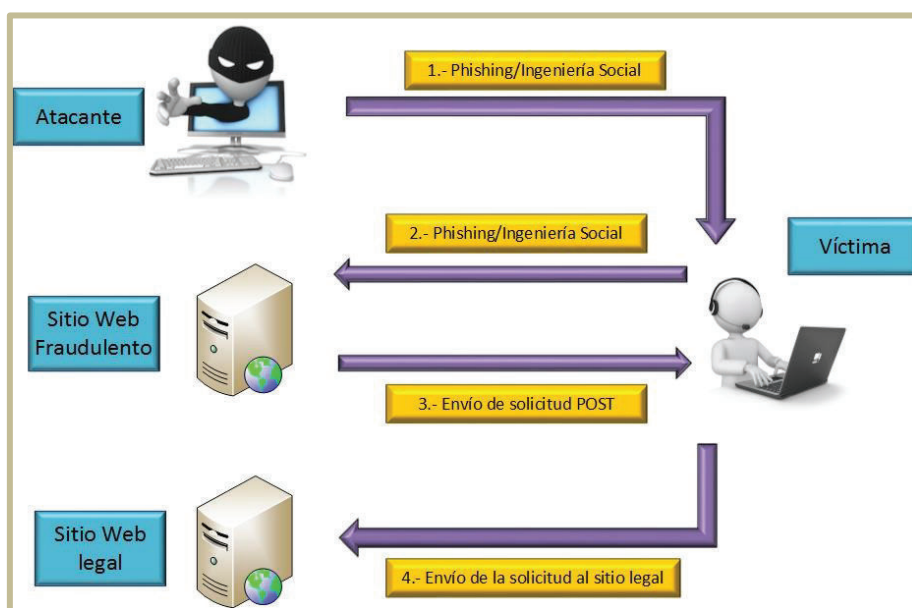


Figura 1.6 CSRF[21]

1.- El atacante utiliza uno de los métodos de phishing o ingeniería social, por ejemplo, envía un correo electrónico que contiene un enlace malicioso a la víctima.

2.- La víctima hace clic en el enlace malicioso y es redirigida al sitio web del atacante. Ahora el atacante necesita engañar a la víctima para hacer clic en un elemento malicioso colocado en la página.

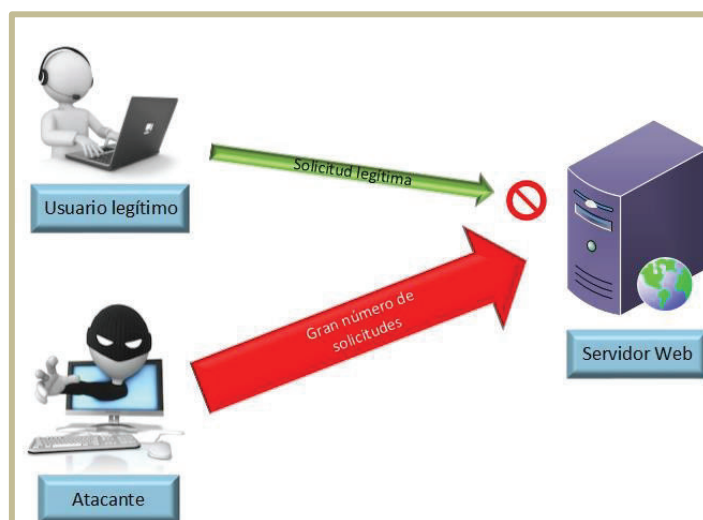
3.- En el ejemplo siguiente, cuando la víctima hace clic en el botón Enviar "Donar a la caridad", se enviará una solicitud POST regular:

```
<form action = "http://yourwebsite.com/transfermoney.aspx" method = "POST">
<Input type = "hidden" name = "account" value = "Atacante" />
<Input type = "hidden" name = "amount" value = "9999" />
<Input type = "submit" value = "Donar a la caridad" />
</form>
```

4.- La solicitud POST se envía al servidor con las credenciales de la víctima (cookie de autenticación). El servidor web procesa la solicitud y envía \$ 9999 a la cuenta del atacante. El hecho más importante aquí es que la víctima no es consciente de ningún comportamiento sospechoso.

**Figura 1.7 Procedimiento CSRF [21]**

- Denegación de servicio: Conocido como DoS, el objetivo de este ataque es dejar sin disponibilidad a un recurso de red o servidor de manera temporal o indefinida para los usuarios genuinos. Hay muchas maneras de generar este ataque, la más común es enviar un gran número de solicitudes al servidor, esto sobrecarga los recursos del mismo, impidiendo aceptar solicitudes de usuarios legítimos dejándoles sin acceso al servidor. En la figura 1.7 se presenta cómo procede un ataque de DoS.



**Figura 1.8 Ataque de Denegación de Servicio (DoS) [15]**

- *Defacement*: Este ataque consiste en deformar, hacer cambios no autorizados en la apariencia de una página web o de un sitio completo. La figura 1.9 muestra una página web afectada por defacement.



Figura 1.9 Sitio web deformado (*defaced*) [17]

## 1.4. HACKING ÉTICO [4], [28]

### 1.4.1. DEFINICIÓN DE HACKING ÉTICO

El hacking ético consiste en el uso del conocimiento en seguridad de la información para realizar pruebas de penetración en equipos y redes de información para encontrar vulnerabilidades explotables que podrían ser aprovechadas por *hackers* maliciosos. Esta información es luego utilizada por las organizaciones para mejorar sus sistemas de seguridad, evitando o minimizando eventos que puedan afectar su seguridad. Para ser un *hacker* ético se debe tener un amplio conocimiento en seguridad de la información, *hardware*, *software*, redes, programación, sistemas operativos, etc., y seguir un conjunto de principios morales y éticos que han sido establecidos en las comunidades virtuales de *hackers*, entre los cuales se puede encontrar los siguientes:

- Respetar la privacidad de la persona que contrata el servicio de hacking ético.
- Una vez terminado el trabajo se debe dejar todo cerrado, para que cualquier persona o él mismo no pueda explotar la vulnerabilidad después de cierto tiempo.

- Dar conocimiento de todas y cada una de las vulnerabilidades presentes a la persona que contrató el servicio de hacking ético.

#### **1.4.2. TIPOS DE HACKING ÉTICO**

Para realizar el proceso de hacking ético se necesita realizar pruebas de penetración con el fin de encontrar las posibles fallas de configuración, escalar privilegios, hacer ataques de fuerza bruta, etc., y dependiendo la información que se facilite para hacer dichas pruebas se pueden encontrar tres tipos [4], [18]:

- Prueba de caja negra: En este tipo de pruebas no se tiene idea de lo que va a examinar, el analista de seguridad<sup>8</sup> solo cuenta con la información pública de la organización, es por este motivo que el tiempo de ejecución de este tipo de pruebas es bastante largo y generalmente este se realiza desde fuera de la organización.
- Prueba de caja gris: No existe una definición exacta, pero se puede decir que es una combinación de pruebas de caja blanca y caja negra, ya que el analista cuenta con poca o limitada información acerca del funcionamiento de la aplicación o documentación de la red.
- Prueba de caja blanca: En este tipo de pruebas de penetración el profesional de seguridad cuenta con información detallada sobre la infraestructura de la red, sistemas informáticos, códigos fuente, direccionamiento de red, etc., otorgados por la organización, este tipo de pruebas simula ataques internos, ya que usuarios internos tienen acceso a información sensible y documentación de la misma. Comparado con las pruebas de caja negra se lo puede realizar en un tiempo más corto.

En la figura 1.10 se aprecia las diferencias entre los tipos de pruebas de penetración.

### **1.5. METODOLOGÍA Y HERRAMIENTAS**

En esta sección se describe la metodología escogida y las herramientas utilizadas para el desarrollo del presente trabajo.

---

<sup>8</sup> Analista de seguridad es la persona encargado en realizar las pruebas de penetración.



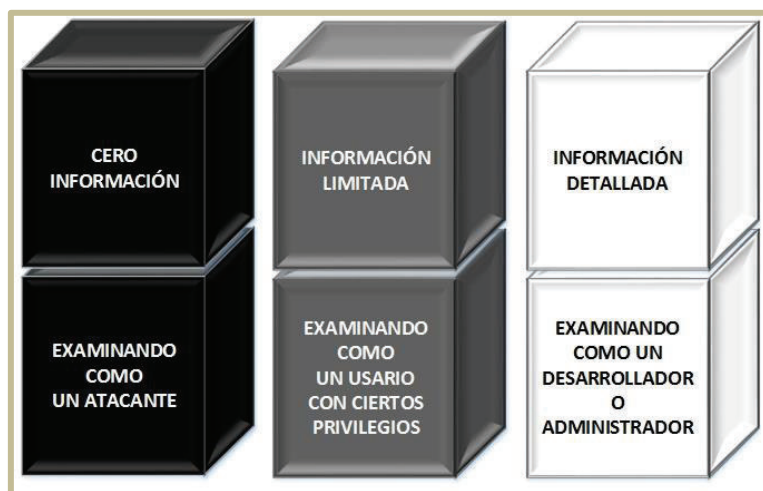


Figura 1.10 Diferencias entre tipos de *hacking* ético [18]

### 1.5.1. METODOLOGÍA [1], [2]

Existen variadas metodologías y estándares para la realización de pruebas de penetración entre las cuales se puede mencionar los siguientes:

- *Open Web Application Security Project (OWASP) guía de pruebas V 4.0.*
- *Penetration Testing Execution Standar (PTEST)*
- *Payment Card Industry Penetration Testing Guide (PCIDSS)*
- *Penetration Testing Framework*
- *Tehnickal Guide to Information Security Testing and Assessment (NIST800-115)*
- *Information System Security Assessment Framework (ISSAF)*
- *Open Source Security Testing Methodology Manual (OSSTMM)*

Para el desarrollo del presente trabajo de titulación se ha escogido OWASP V 4.0 por las siguientes razones:

- Esta detalla pruebas de seguridad específicamente para aplicaciones y sitios web y dado que las aplicaciones permitidas por el MDMQ para el análisis son de este tipo, la Guía se acopla de mejor manera a este trabajo de titulación.
- OWASP es una comunidad a nivel internacional que también se preocupa en ayudar a las organizaciones a desarrollar, implementar y mantener aplicaciones web seguras.

- Toda la documentación, guías, foros de OWASP son abiertos y gratuitos para cualquier organización interesada en optimizar la seguridad de sus aplicaciones web.
- OWASP puede ayudar tanto a organizaciones grandes como pequeñas a mejorar la seguridad de sus aplicaciones web.
- OWASP apoya la innovación y los experimentos para dar solución a los nuevos desafíos de seguridad.

La figura 1.11 muestra el flujo de trabajo del entorno de pruebas OWASP.

El desarrollo del presente trabajo se basará en la sección 4.1 Prueba de penetración de la aplicación de la guía OWASP. Esta prueba de penetración nos permitirá hacer la comprobación de que tan segura es nuestra aplicación web. Esta prueba de penetración se divide en las siguientes fases [1]:

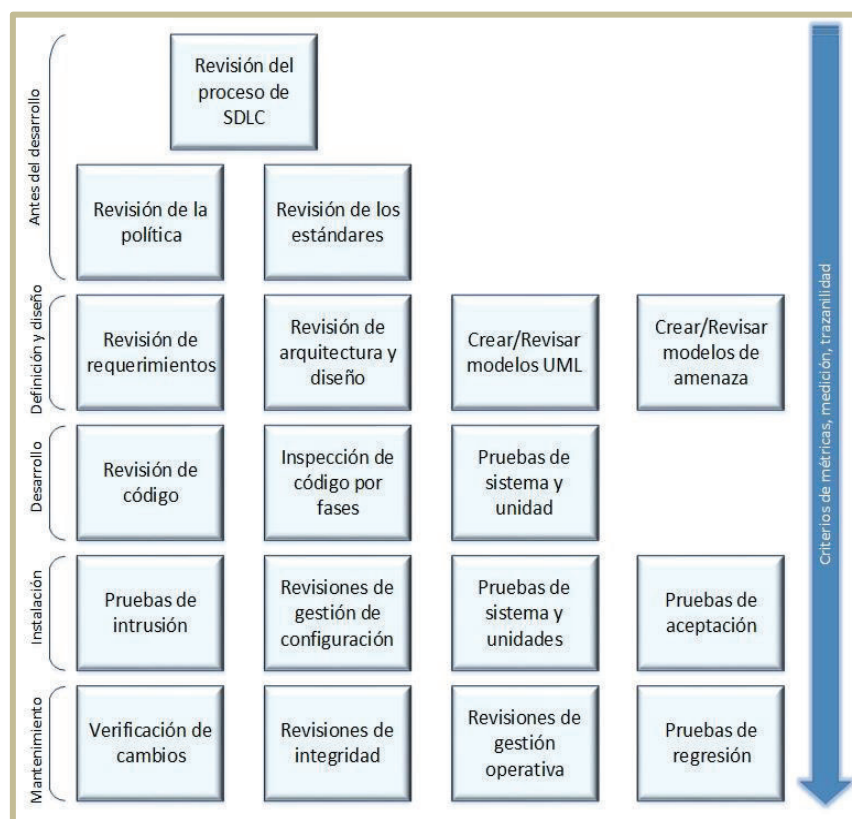


Figura 1.11 Flujo de trabajo del entorno de pruebas OWASP [1]

- **FASE 1: Modo Pasivo:** En esta fase se pretende entender la lógica de la aplicación, aquí se puede utilizar un proxy HTTP<sup>9</sup> para capturar información que transita en la red. De este modo se podrá reunir información de las *cookies* y cabeceras HTTP<sup>10</sup> analizando las solicitudes y respuestas HTTP.
- **FASE 2: Modo activo:** En esta fase el analista empieza usar la metodología para la prueba de penetración. Este grupo de pruebas se han dividido en 11 subcategorías:
  1. **Recopilación de información:** El objetivo principal de esta fase es reunir la mayor cantidad de información sobre la aplicación. Para obtener esta información se puede usar escáner de vulnerabilidades, motores de búsqueda, proxis, etc.
  2. **Pruebas de gestión de la configuración y la implementación:** Tener conocimiento sobre la arquitectura o topología de red nos puede dar una idea de que tan protegida se encuentra la aplicación web, también podrían revelar información importante como métodos de autenticación, funciones administrativas, información de los *logs*, respaldos, métodos HTTP<sup>11</sup> permitidos, etc.
  3. **Pruebas de gestión de identidad:** Esta fase tiene que ver con el usuario, se verifican los roles de usuarios dentro de la aplicación, cómo se realiza el proceso de registro de usuarios, etc.
  4. **Pruebas de autenticación:** En esta parte de la prueba de penetración se verifica como es el proceso de autenticación, si las credenciales viajan en canales seguros, mecanismos de recuperar contraseñas, políticas de contraseñas seguras, etc.
  5. **Pruebas de autorización:** El proceso de autorización viene después de la autenticación, en este tipo de evaluación se va a verificar si se puede evitar el sistema de autorización o si existe forma de ganar privilegios más allá de los que tiene asignado el analista.

---

<sup>9</sup> *Hypertext Transfer Protocol* o HTTP, protocolo de transferencia de hipertexto.

<sup>10</sup> Las Cabeceras HTTP son parámetros que se envían en una petición o respuesta HTTP al cliente o al servidor.

<sup>11</sup> Métodos HTTP se utilizan para realizar acciones en el servidor web, también están diseñados para ayudar a los desarrolladores a implementar y probar aplicaciones

6. **Pruebas de gestión de sesiones:** El control de la comunicación entre el usuario y el sitio<sup>12</sup> web es muy importante, es esta etapa de la prueba de penetración se verifican las formas en que la aplicación se comunica con el usuario mediante la gestión de sesiones.
7. **Pruebas de validación de entrada:** Una de las debilidades que se encuentran en las aplicaciones es la falta de validación correcta de los datos de entrada. En esta parte de la prueba de penetración se verifica cómo se comporta la aplicación ante cualquier tipo de datos de entrada.
8. **Manejo de errores:** En esta sección se analiza como se manejan los mensajes de error, si estos están personalizados o son los que vienen configurados por defecto, ya que estos podrían revelar información sensible acerca de versiones o tipos de servidor.
9. **Criptografía:** En esta parte de la prueba se analiza si los datos sensibles viajan a través de canales seguros, también se verificará la fortaleza del cifrado SSL/TLS<sup>13</sup>.
10. **Pruebas de lógica empresarial:** En esta parte se verifica si la aplicación está siendo utilizada solo para los fines que fue creada o si sigue las reglas del negocio.
11. **Pruebas del lado del cliente:** Estas pruebas se ejecutan desde el lado del cliente, usando para eso un navegador web o un *plug-in* instalado en el mismo.

Las fases de ataque o fases de *hacking* en la que se basa el trabajo son las siguientes [1], [30], [33], [34]:

- **Reconocimiento:** En esta etapa de la prueba de penetración, el atacante reúne toda la información disponible sobre el objetivo, las formas de recopilación de información más comunes es por medio de motores de búsqueda, información de DNS, ingeniería social, etc. Esta etapa corresponde a la Fase 1 de la Guía de Pruebas OWASP V 4.0 [1].

---

<sup>12</sup> Un sitio web es una colección de páginas web relacionadas y comunes a un dominio de Internet.

<sup>13</sup> *Transport Layer Security* (TLS; seguridad de la capa de transporte») y *Secure Sockets Layer* (SSL; capa de puertos seguros) son protocolos que proporcionan comunicaciones seguras.

- **Escaneo:** En esta etapa el atacante utiliza toda la información obtenida en el proceso de recolección, datos como sistemas operativos, puertos abiertos, servicios activos, con esto busca vulnerabilidades conocidas y puntos por donde se pueda penetrar a los sistemas. Esta etapa corresponde a la Fase 2 de la Guía de Pruebas OWASP V 4.0 [1].
- **Explotación:** Esta etapa corresponde al ataque en sí mismo, explotar las vulnerabilidades encontradas en la fase de escaneo, comprometer al sistema objetivo.
- **Manteniendo el acceso:** Si la fase de explotación tuvo éxito, el siguiente paso es mantener el acceso al sistema vulnerado, con el propósito de utilizar todos los recursos del mismo o para escanear y explotar vulnerabilidades otros sistemas.

La figura 1.12 muestra las fases del *hacking*.

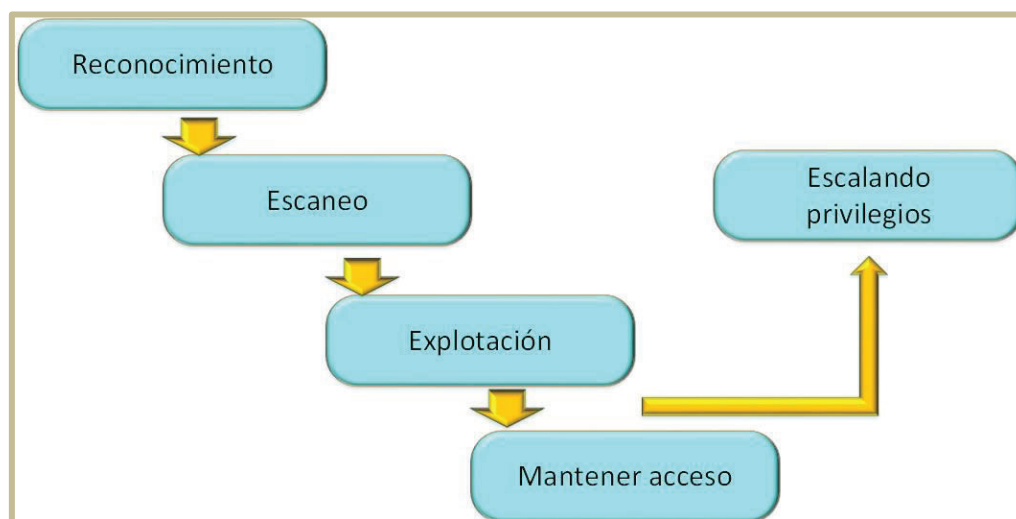


Figura 1.12 Fases del hacking [19]

### 1.5.2. HERRAMIENTAS [20]

Para el desarrollo del trabajo se escogió Kali Rolling 2016.2 por las siguientes razones:

- Kali es una distribución de Linux que sirve para realizar auditorías de seguridad y pruebas de penetración.

- Cuenta con más de 300 herramientas de explotación para realizar los pruebas de penetración.
- Kali está dirigido a todo el público, a partir de los profesionales de seguridad y hackers profesionales como por personas que están empezando en el mundo de la seguridad informática.
- Al ser una distribución de código abierto su utilización no tiene ningún costo.
- Puede ser utilizado como un *live-cd*, esto quiere decir que puede ser ejecutada completamente desde un CD/DVD o desde una unidad flash USB.

En la figura 1.13 se muestra la interfaz de trabajo de Kali Linux.

Luego, se describen brevemente las herramientas que ayudaran a realizar la prueba de penetración descrita en la guía OWASP, tanto las que se encuentran incluidas en Kali Linux como las que no lo están.

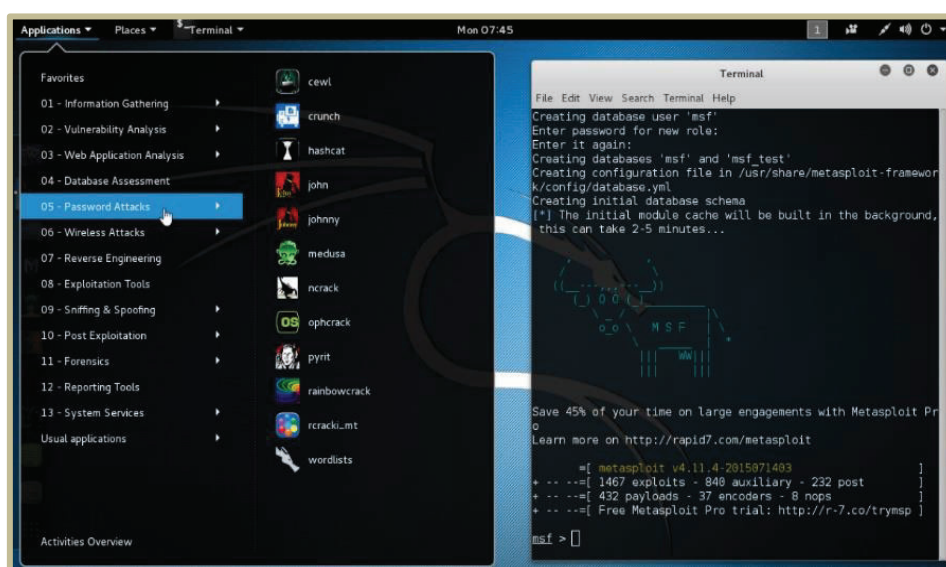


Figura 1.13 Interfaz de trabajo Kali Rolling 2016.2[20]

**Burp Suite [88]:** Burp Suite es un conjunto de herramientas que ayudará a realizar pruebas de penetración en aplicaciones web, entre sus principales funciones tenemos un servidor proxy, *web spidering*<sup>14</sup> y escáner de vulnerabilidades. Viene incluida en Kali Rolling 2016.2.

<sup>14</sup> Araña web es un programa que inspecciona las páginas del Internet de forma automatizada .

### **OWASP Zed Attack Proxy (ZAP) [1], [89]**

Esta herramienta de código abierto viene incluida en Kali Rolling 2016.2 y es una de las más populares en el momento de monitorear la seguridad en las aplicaciones web, su principal función es trabajar como servidor proxy, con esto se podrá revisar todas las peticiones y respuestas entre el cliente y el servidor.

### **Nessus [31], [32]**

Esta aplicación con entorno gráfico permitirá encontrar vulnerabilidades conocidas en equipos y servidores de cualquier tipo, proporcionará los CVE<sup>15</sup> de la misma y si existe alguna forma de mitigarla.

### **Nikto [1], [90]**

Esta herramienta incluida en Kali Rolling 2016.2 es de código abierto y basada en comandos permitirá encontrar vulnerabilidades conocidas en los servidores web que alojan a las aplicaciones, puede detectar malas configuraciones, realizar ataques de fuerza bruta, determinar si la aplicación es vulnerable al XSS<sup>16</sup>, etc.

### **Telnet [1], [91]**

Herramienta libre a base de comandos, sirve para realizar conexiones remotas al servidor y lograr recopilar información del mismo. Esta herramienta esta incluida en Kali Rolling 2016.2.

### **Nmap [1], [35]**

Esta herramienta de código abierto, ayuda a evaluar la seguridad de los servidores web, proporcionará información de equipos disponibles, puertos abiertos, servicios disponibles, nombre de la aplicación, sistema operativo, etc., también permite el uso de scripts para comprobar vulnerabilidades conocidas. Kali Rolling 2016.2 contiene esta herramienta.

---

<sup>15</sup> *Common Vulnerabilities and Exposures* es un diccionario de nombres comunes, para vulnerabilidades de seguridad conocidas públicamente.

<sup>16</sup> *Cross-Site Scripting* (XSS) un tipo de ataque por inyección de código.

### **Httpprint [1], [92]**

Httpprint es una herramienta incluida en Kali Rolling 2016.2, se basa en consola y se puede usar en la fase de recolección de información del servidor web, es decir su tipo y versión.

### **Whatweb [1], [93]**

Esta herramienta de código abierto y basada en consola ayuda a descubrir información acerca del sitio web, como el gestor de contenido, tecnología aplicada, versiones, etc. Kali Rolling 2016.2 incluye esta herramienta.

### **Netcat [1], [94]**

Esta utilidad de red basada en consola permite abrir puertos en el servidor web, y se la utiliza como una herramienta de *debugging*<sup>17</sup> y exploración. Kali Rolling 2016.2 contiene esta herramienta.

### **Curl [1], [95]**

Esta herramienta basada en consola permite transferir archivos desde y hacia el servidor web usando cualquiera de los protocolos que soporta, también es útil para realizar solicitudes HTTP/HTTPS, está incluida en Kali Rolling 2016.2.

### **Sslyze [1], [97]**

SSLyze es una herramienta gratuita, basado en consola que permite verificar si existen defectos o malas configuraciones en la implementación SSL del servidor a conectarse. Kali Rolling 2016.2 contiene esta herramienta.

### **Dotdotpwn [1], [99]**

Esta herramienta basada en consola permite descubrir si la aplicación web es vulnerable a la inclusión de archivos locales o a la ruta traversal de una manera automatizada y está integrada en Kali Rolling 2016.2.

---

<sup>17</sup> Depuración de programas es el proceso de identificar y corregir errores de programación.



**Wget [1], [96]**

Wget incluida en Kali Rolling 2016.2, es una herramienta de código abierto que se basa en consola y que permite descargar archivos usando HTTP/HTTPS y FTP.

**SQLMap [1], [47]**

SQLmap es una herramienta de código abierto, incluida en Kali Rolling 2016.2 que permite realizar de manera automatizada detección y ataques de inyección SQL.

**Sslscan [1], [98]**

SSLscan es una herramienta gratuita integrada en Kali Rolling 2016.2 que permite evaluar la fortaleza del cifrado SSL/TLS de un servidor web remoto.

**Xsser [1], [100]**

Esta herramienta maneja una interfaz gráfica y permite identificar si la aplicación web es vulnerable a la XSS (XSS), de una manera automatizada. Kali Rolling 2016.2 incluye esta herramienta.

**Dirbuster [1], [101]**

Esta herramienta incluida en Kali Rolling 2016.2 permite realizar por fuerza bruta la búsqueda de páginas y directorios ocultos en un servidor o aplicación web, cuenta con una interfaz gráfica para facilitar su uso.

**Slowloris [102]**

Slowloris es una herramienta gratuita basada en consola, permite realizar ataques de Denegación de Servicio contra servidores.

**Wappalyzer de Firefox [103]**

Es una extensión de Mozilla Firefox que permite conocer información sobre la tecnología del sitio web a estudiar, información como el sistema gestor de contenido (CMS), sistema gestor de aprendizaje (LMS), servidor web, etc.

### **GregThatcher.com [107]**

GregThatcher.com es una página web que permite realizar fingerprint al servidor web.

### **Firebug de Firefox [104]**

Firebug es una extensión de Mozilla Firefox que cuenta con un gran número de herramientas de desarrollo web, para editar, depurar y supervisar páginas web.

### **Maltego [1], [105]**

Maltego es una herramienta que cuenta con interfaz gráfica incluida en Kali Rolling 2016.2, esta permitirá recolectar la mayor cantidad la información disponible sobre de un objetivo, persona o empresa, disponible en Internet.

### **FOCA [106]**

FOCA es una herramienta gratuita para Microsoft Windows, la cual permite extraer metadatos ocultos en documentos de Microsoft Office, Libre Office<sup>18</sup>, PDF<sup>19</sup>, etc.

### **BuiltWith Technology Lookup [108]**

El objetivo de BuiltWith es ayudar a los desarrolladores web, investigadores y diseñadores a averiguar qué tecnologías utilizan las páginas web.

### **Desenmascara.me [109]**

Este sitio es una herramienta gratuita web que permite revisar ciertos aspectos de seguridad de alguna página web objetivo de estudio, en especial revisar si existen metadatos que revelen información sensible.

### **Wireshark [14]**

Es un analizador de tráfico de red incluido en Kali Rolling 2016.2.

---

<sup>18</sup> LibreOffice es un paquete de *software* de oficina libre y de código abierto.

<sup>19</sup> PDF (*Portable Document Format*, formato de documento portátil) es un formato de almacenamiento para documentos digitales independiente de plataformas de software o hardware.

**SSL Server Test [110]**

Qualys Inc., es un proveedor de seguridad en la nube, y mediante esta página web permite de forma gratuita analizar la configuración SSL de cualquier servidor web.

**Commix [1], [111]**

Herramienta de código abierto incluida en Kali Rolling 2016.2, que ayuda a realizar pruebas de inyección de código de forma automatizada.

**Google Hacking [112]**

También conocida como Parámetros de Búsqueda Avanzados de Google (PEBAG), es una técnica que mediante el uso de parámetros especiales realiza búsquedas avanzadas en Google, su objetivo es encontrar información sensible o brechas de seguridad en sistemas informáticos pudiendo esto afectar organizaciones o personas.

## **CAPÍTULO 2**

### **SITUACIÓN ACTUAL Y REQUERIMIENTOS**

En este capítulo se realiza una rápida descripción acerca del Municipio del Distrito Metropolitano de Quito, sus funciones y objetivos principales.

También se trata sobre la dependencia del MDMQ que maneja la parte tecnológica. Además, se hace un breve análisis sobre la situación actual de las aplicaciones web en cuestiones de seguridad, para esto se utilizará una Declaración de Aplicabilidad (SoA), tomada de referencia de la Norma ISO/IEC 27001 [5].

El análisis de requerimientos se menciona en la sección 2.5 del presente capítulo, aquí se revisará la información necesaria para determinar las dos aplicaciones más críticas para en ellas realizar la prueba de penetración.

#### **2.1. MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO [3]**

El Municipio del Distrito Metropolitano de Quito es un Gobierno Autónomo Descentralizado el cual tiene control dentro del Distrito Metropolitano de Quito.

#### **2.2. PLAN ESTRATÉGICO [3]**

##### **2.2.1. MISIÓN**

Quito capital del sol, ciudad próspera y atractiva, democrática y solidaria, centro estratégico y turístico, eje cultural de América.

##### **2.2.2. VISIÓN**

Es un órgano de gobierno que actúa como facilitador de los esfuerzos de la comunidad en la planificación, ejecución, generación, distribución y uso de los servicios que hacen posible la realización de sus aspiraciones sociales.

##### **2.2.3. OBJETIVOS ESTRATÉGICOS**

- Integración Social

- Desarrollo Humano Sustentable
- Democracia Participativa
- Medio Ambiente Sano

#### **2.2.4. POLÍTICAS GENERALES**

- **ÉTICA POLÍTICA**

- a) Desarrollar los valores de honradez, solidaridad, responsabilidad social, participación, creatividad, superación, respeto, amor a la Patria y a la ciudad.
- b) Combatir con medios legales y presión ciudadana las prácticas corruptas en todas sus expresiones, dentro y fuera del Municipio.
- c) Dar ejemplo de honestidad en el comportamiento individual y colectivo de las autoridades.
- d) Rendir de cuentas y propiciar contraloría social.

- **SOLIDARIDAD**

- a) Sistema tributario universal, progresivo y equitativo.
- b) Plan social para erradicar la pobreza, el paternalismo y el asistencialismo.
- c) Políticas públicas sustentadas en valores de cooperación, reciprocidad, simetría social y altruismo.

- **PARTICIPACIÓN CIDADADANA**

- a) Participación de la población de barrios, parroquias urbanas, rurales y zonas metropolitanas en la planificación, ejecución y control de la acción municipal.
- b) Normativa municipal para asegurar la contraloría social sobre la gestión municipal.
- c) Participación de representantes ciudadanos/as en los directorios de las empresas municipales.

- **ECONOMÍA COMPARTIDA**

- a) Crecimiento económico sostenido de la ciudad basado en la integración de los sectores públicos, privados y comunitarios.

- b) Transformación de las empresas municipales incorporando criterios modernos de administración para la eficiencia y equidad en la prestación de servicios.

- **DESCENTRALIZACIÓN**

- a) Distritos descentralizados como espacios geográficos y poblacionales con identidades definidas.
- b) Pasar de la organización municipal funcional a la territorial para posibilitar la identificación y participación de la ciudadanía en una administración municipal democrática.
- c) Acercar a funcionarios/as y ciudadanos/as, en forma ágil, oportuna, cordial y técnica.

- **DESARROLLO INSTITUCIONAL**

- a) Promover la creación o fortalecimiento de organizaciones representativas que se expresen en cabildos o juntas, como consejos consultivos o sectoriales que orienten la acción municipal.
- b) Capacitar y dar estabilidad a los recursos humanos municipales, para una administración técnica y profesional.
- c) Aplicar planes de motivación y estímulos para lograr la participación comprometida de los servidores/as municipales.

- **RELACIONES INSTITUCIONALES**

- a) Coordinación permanente con el gobierno central, Banco del Estado, organismos nacionales de cooperación y crédito.
- b) Coordinación estrecha con el gobierno provincial para la atención a las parroquias rurales del Distrito.
- c) Coordinación y cooperación con los Municipios y Consejos Provinciales del país a través de AME<sup>20</sup> y CONGOPE<sup>21</sup>.

- **RELACIONES INTERNACIONALES**

- a) Relaciones estrechas con países amigos para lograr su apoyo a programas del Distrito Metropolitano.

---

<sup>20</sup> Asociación de Municipalidades de Ecuador

<sup>21</sup> Consorcio de Gobiernos Autónomos Provinciales del Ecuador

### **2.2.5. ESTRUCTURA ORGÁNICA DEL MDMQ**

En la figura 2.1 se muestra la Estructura Orgánica Funcional de la Dependencia del Municipio del Distrito Metropolitano de Quito.

### **2.2.6. DIRECCIÓN METROPOLITANA DE INFORMÁTICA [3]**

La Dirección Metropolitana de Informa (DMI) es la dependencia del MDMQ que se encarga de reunir toda la parte tecnológica en atención al medio interno y externo. Controla el *software*, *hardware*, normas y procedimientos, comunicaciones y estándares de los elementos técnicos.

También dirige y evalúa el planeamiento tecnológico institucional, optimiza los sistemas, facilitando la ejecución de los procesos operativos a través de sistemas informáticos, se encarga también del soporte técnico y la seguridad de la información.

#### **2.2.6.1. Misión**

Administrar eficientemente los recursos informáticos mediante la utilización de tecnologías de información (TI) y la automatización de procesos, a fin de apoyar de manera eficaz la gestión y la toma de decisiones en beneficio de la colectividad.

#### **2.2.6.2. Funciones Específicas**

- Conocer y aplicar leyes, reglamentos, instructivos y manuales de procedimientos, relacionados con la Gestión de los Recursos Informáticos y de la Información en la Municipalidad.
- Participar en los procesos de planificación de mediano y largo plazos, así como en la definición y ejecución de procesos de control, definiendo, ejecutando y controlando pasos y procedimientos que deben observarse en la Gestión de los Recursos Informáticos y de la Información.
- Participar como Secretario Asesor Técnico en el Comité Informático, asistiendo y asesorando en materia de tecnología informática y de sistemas de información





- Asesorar en el desarrollo de los sistemas de información internos y externos suministrados por los diferentes proveedores, con el propósito de que se ajusten a las necesidades institucionales y compatibilicen con los sistemas que se encuentran en producción en la institución.
- Planificar, organizar, ejecutar, controlar y evaluar proyectos y actividades de desarrollo de sistemas de información que faciliten la gestión de los diversos procesos institucionales en función del Plan Estratégico de Sistemas.
- Realizar análisis técnicos y el mantenimiento preventivo y correctivo al equipamiento informático de la municipalidad.
- Brindar asistencia técnica a los diversos usuarios de los sistemas de información y herramientas de escritorio en la Municipalidad.
- Determinar objetivos y políticas de tecnología de información y de administración de recursos informáticos.
- Identificar las necesidades de tecnología informática de todas las dependencias municipales y generar el Plan Anual de Adquisiciones de Recursos Informáticos para conocimiento y aprobación del Comité Informático.
- Elaborar y ejecutar en coordinación con las dependencias involucradas en los procesos de adquisición y pagos, el calendario de adquisición y dotación de equipos en función de las prioridades definidas en el Plan Anual de Adquisición respectivo.
- Participar conjuntamente con la Auditoría Interna en la realización de las Auditorías Informáticas en las distintas dependencias municipales.
- Administrar todos los recursos técnicos de la Dirección: sistemas en desarrollo, producción, sistemas de comunicación, entre otros.
- Desarrollar y mantener Sistemas de Información en función de las necesidades institucionales.

### **2.3. APLICACIONES Y SERVICIOS WEB QUE PRESTA EL MDMQ**

El Municipio del Distrito Metropolitano de Quito brinda sus aplicaciones en línea tanto a clientes como a personal administrativo, estos incluyen trámites, pagos en línea y consulta de información, basándose en la tecnología actual. Entre las aplicaciones y servicios ofrecidos se tienen los siguientes:

### 2.3.1. PORTAL DEL MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO

Es la página principal del MDMQ y sirve como su portada, representa la imagen de la institución, brinda información sobre reglamentos, obras, leyes, trámites.

Su función primordial es servir como portal hacia los demás dependencias y servicios que brinda el MDMQ.

En la figura 2.2 se muestra el portal web del MDMQ.

### 2.3.2. AGENCIA PÚBLICA DE NOTICIAS DE QUITO

Este portal web ofrece varios servicios: buscadores, foros, opiniones y noticias actualizadas al instante, tomando en cuenta temas como la salud, movilidad, seguridad, cultura y turismo dentro del DMQ.

La importancia radica en que esta información sea verás y cumpla con el principio de integridad.

En la figura 2.3 se muestra la página principal del portal de prensa del MDMQ.



Figura 2.2 Portal del MDMQ



**Figura 2.3 Portal de prensa del MDMQ**

### **2.3.3. LICENCIA METROPOLITANA ÚNICA PARA EL EJERCICIO DE ACTIVIDADES ECONÓMICAS (LUAE) EN LÍNEA**

La Licencia Única de Actividades Económicas (LUAE) es el documento indispensable que habilita a cualquier establecimiento dentro del DMQ ejercer cualquier actividad económica. La LUAE integra los siguientes permisos y/o autorizaciones administrativas:

- Informe de compatibilidad y Uso de suelos (ICUS)
- Permiso sanitario
- Permiso de funcionamiento de bomberos
- Permiso ambiental
- Identificación de la actividad económica
- Licencia única anual de funcionamiento de las actividades turísticas
- Permiso anual de funcionamiento de la Intendencia General de Policía

Es te portal le permite iniciar proceso de obtención de la LUAE, también sirve para revisar el estado de vigencia de la misma.

En la figura 2.4 se observa el portal de la LUAE.



Figura 2.4 Portal de la LUAE

#### 2.3.4. SECRETARÍA DE EDUCACIÓN, RECREACIÓN Y DEPORTE

La Secretaría de Educación, Recreación y Deporte tiene como misión ser la instancia técnica política del Municipio del Distrito Metropolitano de Quito que administra los establecimientos municipales y genera e implementa políticas públicas locales complementarias para la universalización, inclusión, calidad educativa, distribución de servicios educativos como aporte a la garantía del derecho a la educación para toda la población del DMQ en función de la normativa vigente.

La figura 2.5 muestra la página principal de la Secretaría de Educación del MDMQ.



Figura 2.5 Secretaría de Educación, Recreación y Deportes del MDMQ

### 2.3.5. INFORME DE REGULACIÓN METROPOLITANA (IRM)

El Sistema de Regulación Metropolitana, nos permite obtener y modificar información del propietario, ubicación, superficie del terreno, áreas construidas, las especificaciones obligatorias para fraccionar el suelo, como son: lote y frente mínimo, afectación por vías, áreas de protección de riberas de ríos, quebradas y otras especiales.

Especificaciones obligatorias para la construcción de un edificio, su altura máxima, el área libre mínima, los retiros obligatorios, los usos, factibilidades de servicios de infraestructura y además las regulaciones que deben observarse cuando el predio se encuentre atravesado por oleoductos o poliductos, acueductos, líneas de alta tensión, o esté ubicado en la zona de protección y conos de aproximación de los aeropuertos.

Los datos aquí representados están referidos al Plan de Uso y Ocupación del Suelo e instrumentos de planificación complementarios, vigentes en el DMQ.

En la figura 2.6 se observa un ejemplo de Informe de Regulación Metropolitana para un predio del MDMQ.

**QUITO** ALCALDÍA **Servicios Ciudadanos**

Guía de Trámites | Servicios en Línea | Formularios | Contactenos

**Informe de Regulación Metropolitana - LOTE EN PROPIEDAD HORIZONTAL**

DATOS DEL TITULAR DE DOMINIO	
C.C./R.U.C.	1702899400
Nombre o razón social:	

DATOS DEL PREDIO	
Número de predio:	189307
Geo clave:	170102280167002924
Clave catastral anterior:	31104 09 002 009 002 004
Alicuota total:	0.450119 %
En derechos y acciones:	NO

ÁREAS DE CONSTRUCCIÓN	
Área de construcción cubierta:	75.00 m2
Área de construcción abierta:	6.00 m2
Área bruta total de	81.00 m2

**IMPLANTACIÓN GRÁFICA DEL LOTE**

Mapa de ubicación del lote en Manglaralto, Quito. Vías: ALONSO DE LA FUENTE, LUIS BRUNEL, GUILLERMO WICKHAM, GERARDO REINER. Parcelas: B-22 (SU1), 497.090, 495.840, 496.420, 496.750. Coordenadas: 977.0, 977.0.

**NOVEDADES**

Ordenanza vigente:  
ORDENANZA METROPOLITANA MODIFICATORIA DE LA ORDENANZA METROPOLITANA No. 0041, DEL PLAN METROPOLITANO DE DESARROLLO Y ORDENAMIENTO TERRITORIAL DEL DISTRITO METROPOLITANO DE QUITO No. 0127

Resolución vigente para incremento de pisos No. 13-2016

Figura 2.6 Informe de Regulación Metropolitana

### 2.3.6. INFORME DE COMPATIBILIDAD DE USO DE SUELOS (ICUS)

El Sistema de Compatibilidad de Uso de Suelos, nos permite obtener y modificar información del propietario, ubicación, superficie del terreno, áreas construidas, las especificaciones obligatorias para fraccionar el suelo, también muestra información básica sobre los usos permitidos o prohibidos para la implantación de usos y actividades en los predios de la circunscripción territorial del Distrito Metropolitano de Quito. Los datos aquí representados están referidos al Plan de Uso y Ocupación del Suelo e instrumentos de planificación complementarios, vigentes en el DMQ.

La figura 2.7 muestra un ejemplo de Informe de Compatibilidad de Uso de Suelos.

### 2.3.7. SISTEMA IMPOSITIVO MUNICIPAL DE QUITO – DECLARACIÓN DE PATENTES

Con el Sistema de Patentes en línea se puede obtener el registro laboral obligatorio para los profesionales que trabajan de manera independiente sin relación con un empleador, se aplica a personas naturales, jurídicas, sociedades nacionales o extranjeras domiciliadas en el Quito que ejerzan actividades industriales, comerciales, financieras, inmobiliarias y profesionales.

En la figura 2.8 se muestra la interfaz principal del Sistema de Patentes.

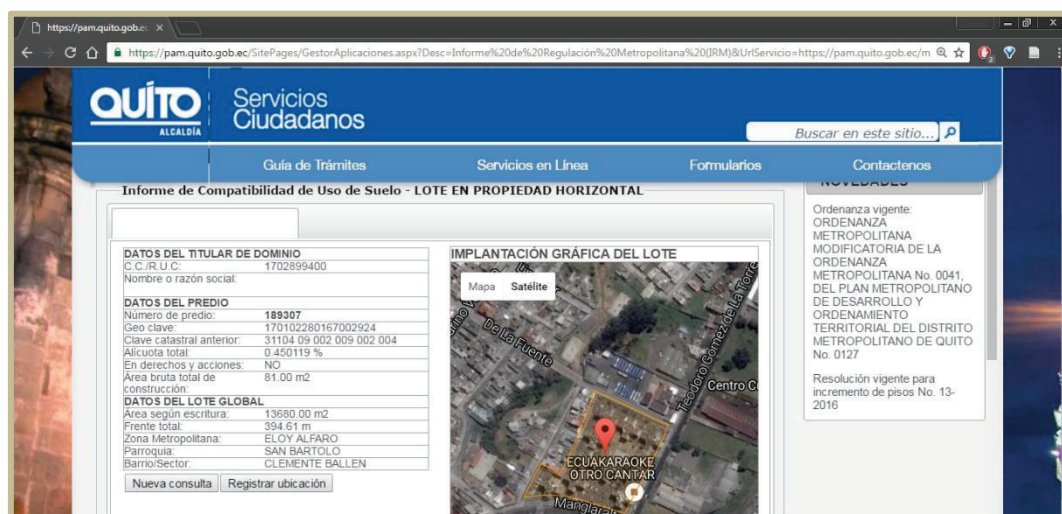
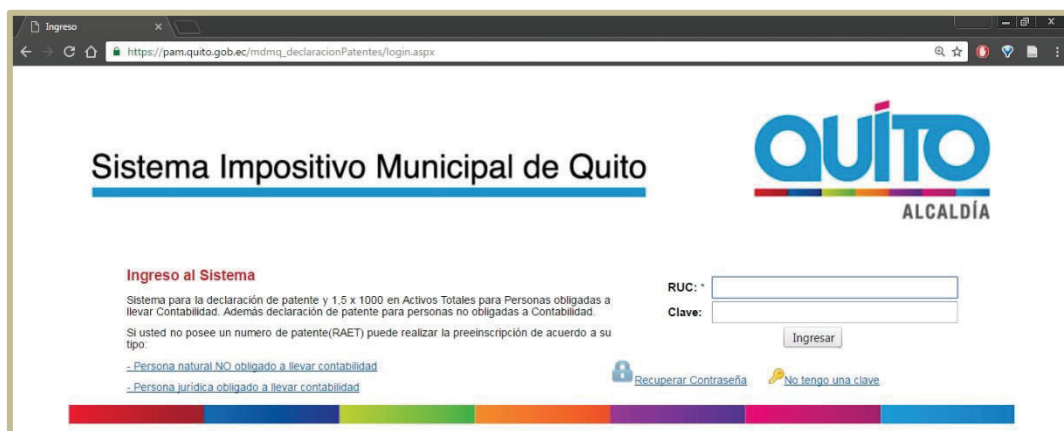


Figura 2.7 Informe de compatibilidad de uso de suelos

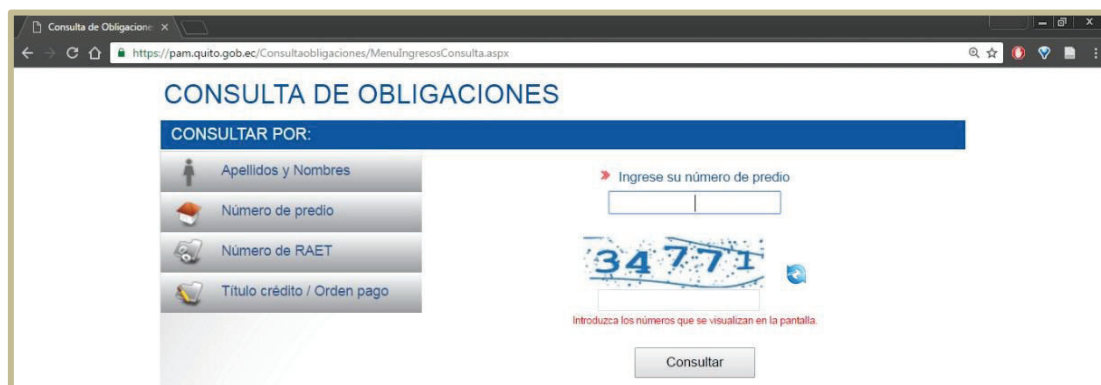


**Figura 2.8 Sistema de Patentes**

### 2.3.8. SISTEMA DE PAGO DE IMPUESTOS POR INTERNET

EL Municipio del Distrito Metropolitano de Quito tiene a disposición de los usuarios el canal de recaudación Botón de Pagos a través de su página Web el mismo que permite realizar las consultadas y/o pagos de sus títulos emitidos por concepto de impuestos, tasas y contribuciones.

La figura 2.9 muestra la interfaz del Sistema de Pago de Impuestos por Internet.



**Figura 2.9 Sistema de pago de impuestos por Internet**

### 2.3.9. SISTEMA INTEGRADO DE REGISTRO CATASTRAL

El Sistema de Registro Catastral del Distrito Metropolitano de Quito (SIREC-Q) permite a inmobiliarias o público en general registrar propiedades horizontales en el catastro, además gestiona la tramitación y las operaciones con la información

alfanumérica como: número de predio, clave catastral, nombre del propietario, parroquia, avalúo del terreno, etc. En la figura 2.10 se observa la interfaz principal del Sistema Integrado de Registro Catastral.



Figura 2.10 SIREC-Q

### 2.3.10. RADIO MUNICIPAL

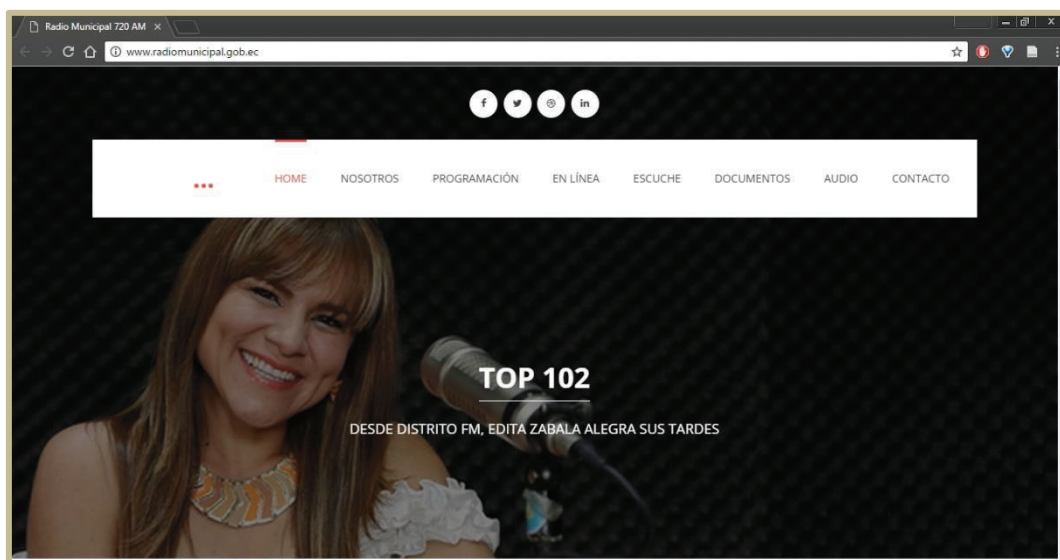
El Municipio del Distrito Metropolitano de Quito cuenta con un medio de comunicación radial creada por el Concejo Municipal de Quito el 05 de febrero de 1953 con el nombre de “Radio Difusora Municipal”.

Este medio ha venido funcionando como una emisora institucional, financiada con presupuesto del gobierno local. Desde el año 2009, la emisora pasa a ser parte de la Secretaría Metropolitana de Comunicación, este cambio, conllevó el que se dé un nuevo enfoque al rol de Radio Municipal, otorgándole un carácter de medio público; lo que implica una nueva visión de los conceptos de participación ciudadana en la gestión municipal.

Así, se concibe a la radio, como una emisora participativa, con un rol de vigilancia y observatorio sobre la calidad de los servicios del Distrito Metropolitano y sobre la calidad de la gestión del gobierno local y como un instrumento para la rendición de cuentas de las autoridades municipales.

En la figura 2.11 se presenta la página web de la Radio Municipal.





**Figura 2.11 Radio Municipal**

## **2.4. ANÁLISIS DE LA SITUACIÓN ACTUAL [4], [9]**

El análisis de situación actual ayudará a conocer la manera en la que la organización está abordando los aspectos concernientes a la seguridad de la información, para posteriormente poder dar soluciones para reducir o mitigar las falencias del sistema de seguridad actualmente implantado.

Para realizar el análisis se utilizará una Declaración de Aplicabilidad[9] (*Statement of Applicability*) obtenido de la Norma ISO/IEC 27001[5], con la cual identificar los procesos que ha adoptado la organización para reducir los niveles de riesgo a causa de incidentes relacionados con la seguridad de la información.

### **2.4.1. DECLARACIÓN DE APLICABILIDAD (SoA) [9]**

La Declaración de Aplicabilidad es un listado de los controles de seguridad establecidos en la Norma ISO/IEC 27001 [5], este sirve para revisar que medidas de seguridad han sido tomadas en cuenta dentro de la organización y cuales han sido dejadas de lado.

La lista de control para la Declaración de Aplicabilidad se encuentra detallada en el Anexo A.

#### **2.4.1.1. Políticas de seguridad - A.5**

En la DMI del MDMQ disponen de un documento formal aprobado por el Director Metropolitano de Informática, en el cual constan todas las políticas de seguridad implantadas, las cuales han sido debidamente comunicadas y deben ser cumplidas por todos los empleados y organizaciones externas.

Este documento no ha sido revisado regularmente, ni se han hecho cambios significativos con el fin de asegurar la eficiencia y efectividad del mismo [84].

#### **2.4.1.2. Aspectos organizativos de la seguridad de la información – A.6**

En cuanto al manejo de la seguridad de la información, la Dirección apoya constantemente la seguridad dentro de la organización, pero no existe un departamento dedicado a la seguridad de la información.

Las actividades de seguridad de la información están parcialmente coordinadas por los diferentes departamentos de la organización, pero no se han definido claramente sus responsabilidades.

Los nuevos servicios, *hardware*, *software*, son debidamente autorizados por la dirección, con el fin de asegurar la compatibilidad con el sistema.

Los empleados están sujetos a acuerdos de confidencialidad para la no divulgación de la información, que son renovados periódicamente y que tienen vigencia hasta tiempo después de la salida del miembro de la organización [85].

Existen procesos definidos para contactar y comunicar de forma oportuna los eventos de seguridad de la información, así como los que infringen los aspectos legales.

Con respecto a las entidades externas se especifica el tipo de acceso que tendrá (físico, lógico), servicios de procesamiento utilizados (almacenamiento, transferencia), valor y sensibilidad de la información, personal autorizado y verificación de la autorización.

#### **2.4.1.3. Gestión de activos – A.7**

La organización dispone de un inventario de todos los activos importantes, en el cual se encuentra información como; el tipo de activo, número de serie, ubicación, tanto de los equipos funcionales como los dados de baja y almacenados en bodega.

También están registrados los responsables y propietarios de cada uno de los activos de la organización.

No se han desarrollado procedimientos adecuados para etiquetar y manejar la información, por lo que no ha sido debidamente clasificada tomando en cuenta su valor, requerimiento, sensibilidad e importancia dentro de la organización.

#### **2.4.1.4. Seguridad ligada a los recursos humanos – A.8 [86]**

Con el fin de verificar la integridad de empleados, contratistas o terceros que quieran ingresar al grupo de trabajo de la organización, estos se someten a chequeo de antecedentes laborales y personales, con el fin de confirmar si cumple o no con el perfil requerido.

Una que vez que el interesado cumple con los requisitos y es aceptado, este debe aceptar y firmar el contrato de empleo, donde se establecen las funciones y responsabilidades para el manejo de la información dentro y fuera de la organización, en concordancia con las políticas y procedimientos de la misma.

No existe un proceso bien definido el cual provea conocimiento, capacitación y actualización de manera regular de las políticas y procedimientos organizacionales referentes a la seguridad de la información.

No obstante existen procesos disciplinarios en contra de los empleados que han cometido violaciones en la seguridad.

Existen sanciones económicas y hasta la remoción del cargo si se comprobase una violación a la seguridad de la información.

Para asegurar que los empleados, contratistas y terceros salgan de la organización de una manera ordenada, se les comunica las responsabilidades legales, los términos y condiciones laborales que deben cumplir durante un periodo después de terminar las actividades dentro de la organización, asimismo se obliga a estos a devolver todo activo relacionado con la organización tales como; dispositivos electrónicos, llaves, tarjetas de identificación y tarjetas de acceso tanto físico como lógico.

Si bien la organización cuenta con un proceso establecido para el cese de actividades y devolución de activos, algunos derechos de acceso no han sido retirados del todo, en el caso de contraseñas de acceso, identificaciones y tarjetas de acceso.

#### **2.4.1.5. Seguridad física y ambiental – A.9**

Para evitar el acceso no autorizado y prevenir daño o intromisiones en las instalaciones de la organización, el perímetro de seguridad está claramente definido y protege mediante accesos físicos, no solo a la institución sino también a los activos. Se cuenta con personal de seguridad que controla el acceso a las instalaciones de la organización, para el ingreso a los diferentes departamentos, se realiza control de acceso mediante tarjetas y usando un control biométrico. Para el acceso al data center además de la identificación biométrica, es necesario el ingreso de una clave numérica.

La salud y seguridad de las oficinas se han diseñado de una manera adecuada, estas cuentan con la debida ventilación y un sistema de protección contra incendios.

Para evitar la pérdida, daño o robo de los activos, estos han sido ubicados de forma estratégica dentro de las instalaciones con el propósito de reducir este riesgo.

Los activos cuentan con los sistemas de apoyo necesarios para enfrentar fallas o interrupciones de los servicios públicos, principalmente del suministro eléctrico. El cableado tanto de energía como de comunicaciones, cuentan con la debida protección ante daño o interceptación.

Los equipos reciben periódicamente el debido mantenimiento preventivo y correctivo para preservar el correcto desempeño de sus funciones.

Si bien la seguridad de los activos dentro de la institución está bien definida, no cuenta con procedimientos de seguridad necesarios para trabajar con equipos fuera de la organización, como tampoco se hace la debida verificación de traslado de activos con la debido autorización.

Antes del retiro de un activo, la organización se asegura que el contenido haya sido removido de manera eficaz para que este no pueda ser recuperado, la eliminación del activo se hace con la respectiva autorización y debido registro.

#### **2.4.1.6. Seguridad operativa y comunicaciones – A.10**

La seguridad de las operaciones y comunicaciones se refiere a los procedimientos que ofrecen protección contra software malicioso, mantiene la integridad y disponibilidad de la información, se encarga del monitoreo y registro de eventos de seguridad de la información, gestiona los cambios en los sistemas informáticos y asegura la información que se envía por las redes de telecomunicaciones, es decir, el flujo de datos y la infraestructura por la cual viaja la misma.

Todos los cambios a los activos y sistemas son debidamente planificados, monitoreados y notificados por las personas respectivas, sin embargo estos no están debidamente documentados.

Para reducir el riesgo de acceso no autorizado, modificación, uso malintencionado de los activos de la organización, se ha distribuido (segregado) responsabilidades a los diferentes departamentos de la misma.

La Dirección se asegura de la implementación y cumplimiento de controles para los cambios en los sistemas de información, también se encarga de separar los equipos que se encuentran en fase de desarrollo y prueba, para que no puedan afectar el correcto funcionamiento de los sistemas ya implementados.

En lo que se refiere a la entrega de servicios de terceros, la dirección se asegura que se implementen y mantengan los niveles de servicio incluidos en el contrato de entrega, también se monitorea y controla los cambios en los servicios de terceros, incluyendo mantenimiento y políticas, como procedimientos y controles de la seguridad, aunque los reportes provistos por terceros no han sido revisados de forma regular.

Con respecto a controles de software malicioso, no se tiene bien establecido procedimientos o controles para el uso de software no autorizado, o revisiones regulares de software. Tampoco se han implantado correctamente procedimientos para protección contra códigos maliciosos y no existe un plan adecuado para la continuidad del negocio, si éste es dañado por código malicioso. En cuestiones de código móvil, no cuenta con ningún procedimiento de control si estos ejecutan acciones no autorizadas, para bloquear su uso, para bloquear su recepción o autenticación del mismo.

Existen respaldo y copias de seguridad de información y configuraciones para disminuir el tiempo de no disponibilidad de un sistema, pero no se han establecido claramente procedimientos o servicios de respaldo adecuados para hacer estas copias de seguridad, aunque en el área de redes si se cuenta con rutas redundantes y alta disponibilidad en los equipos de interconectividad.

Para proteger la información tanto almacenada como la transportada por la red se cuenta con un *Firewall* (Cisco ASA), el cual provee de políticas de acceso y salida de la información a la red. Además, el área de servidores se encuentra dentro de un segmento de red diferente (DMZ<sup>23</sup>) para su protección.

No se encuentran establecidos procesos adecuados para la eliminación de medios que contengan información sensible cuando estos ya no son necesarios. Para el uso de dispositivos removibles se hace a discreción de los empleados, sin un procedimiento de gestión implantado. Tampoco se tiene un control formal para el

---

<sup>23</sup> Zona desmilitarizada (DMZ, *demilitarized zone*) es una zona segura que se ubica entre la red interna de una organización y una red externa.

correcto almacenamiento, distribución, clasificación de la información contra la divulgación, mal uso, acceso no autorizado. Sin embargo, la documentación con la que se cuenta se encuentra debidamente almacenada con seguridad.

Aunque están definidos acuerdos para el intercambio de información entre la organización y terceros, no cuenta con procedimientos claros para contrarrestar la interceptación, modificación o copiado de información en el transcurso de su intercambio con ellos.

Tampoco se provee la debida protección de los medios que contienen información sensible durante su transporte fuera de la organización y no se garantiza el intercambio de mensajes electrónicos, su integridad o disponibilidad.

La organización no considera aspectos de seguridad, nivel de confianza, integridad de la información disponible al público o en el comercio electrónico, pero las transacciones en línea cuentan con total seguridad en contra de modificación, copia o duplicación y garantiza la atomicidad<sup>24</sup> de la misma.

No existe un registro de auditoría de seguridad, donde se incluya, fecha, hora y detalle del evento de seguridad, aunque si se cuenta con un procedimiento para monitorear regularmente el acceso, cambios o intentos de cambio del sistema.

Se registran eventos del operador y del administrador del sistema de una manera informal, sin la debida protección contra el acceso y la manipulación no autorizada.

No se ha establecido una sincronización de tiempo exacta y convenida entre los sistemas de procesamiento de información.

#### **2.4.1.7. Control de acceso – A.11**

Existen políticas de acceso establecidas y difundidas claramente para el acceso y distribución de información, servicios y procesos del negocio dentro de la organización.

---

<sup>24</sup> La atomicidad es la propiedad que asegura que una operación se ha realizado o no, y por lo tanto ante un fallo del sistema no puede quedar a medias.

No existe un proceso formal para dar de alta o baja los usuarios con el propósito de dar o quitar privilegios de acceso a los servicios y sistemas, tampoco se controla de forma adecuada la asignación de privilegios.

La gestión de claves de usuarios se hace mediante el Directorio Activo<sup>25</sup>, pero no mediante un proceso formal establecido que garantice calidad en las mismas. Tampoco la dirección se preocupa de revisar periódicamente los privilegios de acceso que se han concedido a los usuarios.

No se demanda a los usuarios el cumplimiento de buenas prácticas para el establecimiento, confidencialidad, cambio regular y uso de contraseñas. Tampoco se concientiza a los usuarios sobre la protección de equipos desatendidos. No hay un procedimiento formal para restringir el acceso de usuarios a los servicios de red y redes que han sido específicamente autorizados a usar.

En cuestiones de accesos remotos se utiliza un shell seguro<sup>26</sup> para las conexiones a los servidores y se tiene en constante control los puertos de acceso físicos y lógicos utilizados para diagnóstico y configuración.

Los servicios de información, usuarios y sistemas se encuentran debidamente segregados para disminuir los riesgos de un uso fraudulento de los mismos.

Para evitar el acceso no autorizado a los sistemas, las sesiones se cierran automáticamente después de cierto tiempo de inactividad. También se han definido límites en los tiempos de conexión a las aplicaciones de alto riesgo, no obstante el control de acceso a los sistemas no se lo realiza de manera formal.

#### **2.4.1.8. Adquisición desarrollo y mantenimiento de los sistemas de información – A.12**

Se realizó un análisis adecuado para identificar debidamente los requisitos de seguridad para el desarrollo e implementación de los sistemas informáticos y aplicaciones.

---

<sup>25</sup> *Active Directory* servicio de directorio en una red distribuida de computadores.

<sup>26</sup> SSH (*Secure Shell*) sirve para acceder a máquinas remotas a través de una red de forma segura.



Para garantizar el correcto uso e integridad de la información usada en las aplicaciones, se emplean procedimientos apropiados para validar los datos tanto de entrada como de salida, así como durante el procesamiento de la misma.

Con el fin de preservar la confidencialidad, integridad y autenticidad de la información relacionada a las aplicaciones se han implantado procedimientos para el uso de controles criptográficos, por lo que se implementa procesos de gestión de claves criptográficas, principalmente para su generación y almacenamiento.

Existen procedimientos bien definidos que limitan el acceso al código de la aplicación, sin embargo, no se controla de manera adecuada la instalación del programa, ni se selecciona de manera apropiada los datos que se utilizan para realizar las pruebas en la nueva aplicación.

No se han establecido formalmente controles para la implementación de cambios y revisiones técnicas en las aplicaciones, aunque durante su ejecución éstas son controladas de manera estricta.

También existen procedimientos para evaluar y monitorear aplicaciones que han sido desarrolladas por terceros.

#### **2.4.1.9. Gestión de incidentes en la seguridad de la información – A.13**

Todos los eventos y debilidades de seguridad identificados y observados por usuarios, empleados y terceros a la organización son debidamente reportados a los departamentos y jefes de áreas competentes, pero no están establecidos procedimientos para evaluar, clasificar y cuantificar estos incidentes ocurridos.

Cuando se produce un incidente de seguridad existen procedimientos establecidos para realizar el seguimiento respectivo al causante, en el cual se debe mantener y presentar evidencias de lo sucedido para hacer cumplir las acciones legales respectivas.

No existe un departamento dedicado específicamente a al cuidado de la Seguridad de la Información.

#### **2.4.1.10. Aspectos de seguridad de la información en la gestión de continuidad del negocio – A.14**

La organización no cuenta con un proceso debidamente implantado para garantizar la continuidad del negocio, por lo tanto este no tiene el apropiado mantenimiento, actualización o evaluación para garantizar su efectividad.

#### **2.4.1.11. Cumplimiento – A.15**

Si bien existe un documento con políticas de seguridad establecidas, no se ha implantado un procedimiento formal para asegurar su cumplimiento, tampoco se verifica que los sistemas de información cumplan con los estándares adoptados por la organización.

No existe regulación de controles criptográficos.

Todos los registros importantes para la organización y la información personal de los empleados, usuarios y entidades externas, tienen cierto nivel de protección, el cual no es el más adecuado, dado que estos se encuentran en documentos físicos (papel, CDs, DVDs) o guardados en forma digital en servidores de archivos que no cuentan con restricciones de acceso o políticas estrictas de divulgación de la información.

### **2.5. ANÁLISIS DE APLICACIONES WEB CRÍTICAS**

Este punto analiza los requerimientos de dependencia entre sistemas y aplicaciones web, y la prioridad que tiene cada uno de ellos dentro de toda la infraestructura tecnológica.

Con este análisis se van a escoger las dos aplicaciones más críticas, para las cuales se realizarán las pruebas de penetración.

#### **2.5.1. MATRIZ DE DEPENDENCIAS [87]**

En este documento proporcionado por la Dirección Metropolitana de Informática, se puede observar cómo se relacionan entre sí los diferentes sistemas o aplicaciones web que proporciona el Municipio del Distrito Metropolitano de Quito.

En esta matriz constan los diferentes sistemas internos<sup>27</sup> del MDMQ, así como los portales y aplicaciones web (sistemas externos<sup>28</sup>) que proporcionan a la ciudadanía para la gestión y administración de las obligaciones con el mismo.

Dicha matriz relaciona los sistemas, tanto internos como externos al MDMQ y muestra la dependencia directa entre los mismos.

Para saber si un sistema depende de otro, debe existir un casillero pintado (azul) en la matriz de dependencias.

En la tabla 2.1 se muestra un extracto de la matriz de dependencias de los servicios y aplicaciones del MDMQ.

SERVICIO	IRM	ICUS	Portal de Prensa	Recaudación *	Radio Municipal	Portal Quito *	Convenios	SIREC-Q	SAO	TOC	Personas	Seguridades	Portal LUAE	Portal Educación	SIMET-Q	Patentes
Sistema Territorial IRM	■					■					■	■				
Sistema Territorial ICUS		■				■					■	■				
Portal de Prensa			■			■										
Recaudación				■		■										
Radio Municipal					■											
Portal del Municipio						■										
Convenios							■									
SIREC-Q				■		■		■				■				
SAO				■					■			■				
TOC				■						■						
Personas											■	■				
Seguridades												■				
Portal LUAE						■							■			
Portal Educación						■								■		
SIMET-Q				■		■									■	
Sistema de Patentes						■										■

**Tabla 2.1 Matriz de dependencia**

<sup>27</sup> Sistema Interno: Sistema o aplicación que se utiliza únicamente dentro de la organización. (Fuente: Dirección Metropolitana de Informática – Departamento de Producción)

<sup>28</sup> Sistema Externo: Sistema o aplicación que usa para personas fuera de la institución, para la ciudadanía. (Fuente: Dirección Metropolitana de Informática – Departamento de Producción)

Por ejemplo: se puede apreciar que los sistemas **IRM**, **ICUS**, **Recaudación** y **SIREC-Q** dependen del sistema **Portal Web** y que el sistema **SIREC-Q** además depende del sistema **Recaudación**. De esta manera es como se relacionan los sistemas entre sí y con ello se puede analizar el impacto que ocasionaría en el funcionamiento de los demás si uno de estos llega a fallar, en el presente ejemplo se puede determinar que si el **Portal Web** del MDMQ falla, causa un impacto en el funcionamiento o actividades desarrolladas por los sistemas: **IRM**, **ICUS**, **Recaudación** y **SIREC-Q**.

Los ítems resaltados con gris corresponden a aplicaciones que presta el Municipio de Quito a la ciudadanía, mientras que los demás corresponden a sistemas internos y portales web.

El formato de la matriz de dependencias de las aplicaciones web y sistemas que administra la DMI se encuentra en el Anexo B.

### 2.5.2. PRIORIDAD DE LOS SERVICIOS [37]

En este documento se puede observar el orden por prioridad en que las aplicaciones web y sistemas han sido colocadas, desde los que tienen prioridad muy alta hasta los que poseen una prioridad baja.

En la tabla 2.2 se observa un listado de la prioridad que tienen los diferentes sistemas y aplicaciones con que cuenta el MDMQ. Se puede notar que las aplicaciones y sistemas presentes en la tabla poseen una prioridad **Muy Alta**. Estas serán tomadas en cuenta al momento de escoger las más críticas.

Prioridad	Servicio Informático / Infraestructura	Usuarios Finales
1. Muy Alta	Infraestructura del Data Center	MDMQ
1. Muy Alta	<b>Página del Municipio</b>	<b>Ciudadanía</b>
1. Muy Alta	Portal Intranet	MDMQ
1. Muy Alta	Sistema de Administración de Requerimientos	Alcaldía, Administración Central
1. Muy Alta	Directorio activo	MDMQ
1. Muy Alta	MDMQ_PAM	Servicios Ciudadanos, Ciudadanía

Prioridad	Servicio Informático / Infraestructura	Usuarios Finales
1. Muy Alta	Reportes Gerenciales de Recaudación	Alcaldía, Administración Central
1. Muy Alta	Sistema de Claves de Patentes	DMTF
1. Muy Alta	Sistema de Patentes	DMTF
1. Muy Alta	<b>Sistema de Recaudación de Tributos</b>	<b>DMF, ciudadanía</b>

Tabla 2.2 Aplicaciones/sistemas por prioridad

El formato del listado de prioridades de las aplicaciones web y sistemas que administra la DMI se encuentra en el Anexo C.

## 2.6. APLICACIONES WEB CRÍTICAS

En esta sección se van a escoger cuáles son las dos aplicaciones web más críticas, y sobre éstas se realizarán las pruebas de seguridad. Para ello se utiliza la matriz de dependencia y el listado de prioridad final de los servicios y aplicaciones del MDMQ [37]. Como se aprecia en la sección 2.5.1 existen tres sistemas, los cuales tienen mayor influencia en los demás.

El primero es Recaudación, este sistema es el encargado del cobro de obligaciones que la ciudadanía tiene con el MDMQ a través del Internet. Revisando la matriz de dependencias este sistema causa impacto directo sobre las siguientes habitaciones:

- **SIREC-Q:** El Sistema de Registro Catastral del Distrito Metropolitano de Quito (SIREC-Q) permite a inmobiliarias o público en general registrar propiedades horizontales en el catastro de la ciudad.
- **TOC:** Sistema interno que utiliza el personal encargado de la parte de recaudación de obligaciones que los ciudadanos tienen con el MDMQ.
- **SIMET-Q:** El Sistema Metropolitano de Transferencia de Dominio, es un sistema interno que utiliza el personal autorizado para realizar transferencias de dominios territoriales dentro del DMQ.

- **SAO:** Es un sistema de consulta interna que es utilizado por las personas encargadas de proveer información a la ciudadanía sobre deudas pendientes y pago de obligaciones que tienen los ciudadanos con el MDMQ.

El segundo es Seguridad, es un sistema interno del MDMQ que se encarga de proveer seguridad a los aplicativos, es decir políticas y control de acceso, este tiene relación directa con los siguientes sistemas:

- **IRM:** El Sistema de Regulación Metropolitana, permite obtener y modificar información del propietario, ubicación, superficie del terreno, áreas construidas y las especificaciones obligatorias para fraccionar el suelo.
- **ICUS:** El Sistema de Compatibilidad de Uso de Suelos, nos permite obtener y modificar información del propietario. Los datos presentados aquí están referidos al Plan de Uso y Ocupación del Suelo e instrumentos de planificación complementarios, vigentes en el DMQ.
- **SIREC-Q:** El Sistema de Registro Catastral del Distrito Metropolitano de Quito (SIREC-Q) permite a inmobiliarias o público en general registrar propiedades horizontales en el catastro de la ciudad.
- **SAO:** Es un sistema de consulta interna que es utilizado por las personas encargadas de proveer información a la ciudadanía sobre deudas pendientes y pago de obligaciones que tienen los ciudadanos con el MDMQ.
- **Personas:** Este sistema es de carácter interno, este sistema es encargado de proveer seguridades a nivel de usuarios, perfiles, restricciones y privilegios.

El tercero es el Portal web del MDMQ, este portal representa la imagen de la institución y es la puerta de enlace a otros servicios.

El portal causa impacto directo a los siguientes sistemas:

- **IRM:** El Sistema de Regulación Metropolitana, permite obtener y modificar información del propietario, ubicación, superficie del terreno, áreas construidas y las especificaciones obligatorias para fraccionar el suelo.

- **ICUS:** El Sistema de Compatibilidad de Uso de Suelos, nos permite obtener y modificar información del propietario. Los datos presentados aquí están referidos al Plan de Uso y Ocupación del Suelo e instrumentos de planificación complementarios, vigentes en el DMQ.
- **SIREC-Q:** El Sistema de Registro Catastral del Distrito Metropolitano de Quito (SIREC-Q) permite a inmobiliarias o público en general registrar propiedades horizontales en el catastro de la ciudad.
- **Recaudación:** Sistema de cobro de obligaciones de la ciudadanía con el Municipio del Distrito Metropolitano de Quito.
- **Portal LUAE:** La Licencia Única de Actividades Económicas (LUAE) es el documento indispensable que habilita a cualquier establecimiento dentro del DMQ ejercer cualquier actividad económica. Este sistema permite la obtención de la LUAE y ver el estado de vigencia de la misma.
- **Portal Educación:** La Secretaría de Educación y Deporte Municipal tiene como misión implementar políticas para la universalización, inclusión y calidad educativa, sobre los establecimientos municipales. El portal de educación nos permite conocer cómo se desarrolla este proceso.
- **Portal de Prensa:** Este portal web ofrece varios servicios: buscadores, foros, opiniones y noticias actualizadas al instante, tomando en cuenta temas como la salud, movilidad, seguridad, cultura y turismo dentro del DMQ. La importancia radica en que esta información sea verás y cumpla con el principio de integridad.
- **Sistema de Patentes:** La patente es un registro laboral obligatorio para los profesionales que trabajan de manera independiente, se aplica a personas naturales, jurídicas, sociedades nacionales o extranjeras domiciliadas en el DMQ que ejerzan actividades industriales, comerciales, financieras, inmobiliarias y profesionales. Este es un requisito previo a la obtención del RUC. El Sistema de Patentes sirve para declarar y pagar la Patente por Internet.

Se puede observar claramente que el portal web del MDMQ influye en el funcionamiento de varios servicios, ya que provee el acceso a los mismos, por lo cual debe ser tomado muy en cuenta.

Además, considerando la información detallada en la sección 2.5.2 se aprecia que existen varios sistemas que poseen una prioridad considerada como *Muy alta*, esto quiere decir que los procesos y funciones que realizan estos son muy importantes dentro del MDMQ y que de su funcionamiento y disponibilidad depende mucho la continuidad del negocio y el funcionamiento normal de sus actividades.

Entre los sistemas con prioridad *Muy alta* se tiene:

- Infraestructura del Data Center.
- Reportes gerenciales.
- El portal web del MDMQ.
- El sistema de recaudación de obligaciones por Internet.

#### **2.6.1. MATRIZ DE IMPACTO ENTRE APLICACIONES/SISTEMAS [4], [5], [36]**

Esta matriz de impacto ayuda en la determinación de las 2 aplicaciones más críticas del MDMQ. El método detallado a continuación es basado en los lineamientos de la norma ISO 27001 [5].

**El primer paso:** Listar los sistemas y/o aplicaciones involucrados:

- Portal Municipio de Quito
- Sistemas de Regulación Metropolitana (IRM)
- Informe de Compatibilidad de Uso de Suelo (ICUS)
- Sistema de Patentes
- Sistema de Pago de Impuestos por Internet
- Sistema de Registro Catastral (SIRECQ)
- Portal Prensa
- Portal Radio Municipal
- Portal LUEA Web
- Portal Educación

**El segundo paso:** Crear una matriz con los sistemas auditados y asignar valores en sus celdas referentes al impacto negativo que podría producir su afectación sobre: la



innovación, la excelencia en la gestión, el servicio al cliente, y la imagen y reputación de la organización y como estos influyen sobre la confidencialidad, disponibilidad e integridad de la información que se maneja en dicha entidad. Los valores de impacto utilizados como referencia, son los siguientes:

1: Muy bajo, 2: Bajo, 3: Medio, 4: Alto, 5: Muy alto

Cabe indicar que los valores de impacto fueron validados por el Departamento de Producción de la DMI del MDMQ. En la tabla 2.3 se muestra la matriz de impacto de los sistemas y/o aplicaciones del MDMQ.

**Tercer paso:** Con la tabla 2.3 se procede a calcular el valor promedio de cada fila, definiendo así los valores de impacto en la confidencialidad, integridad y disponibilidad. En la tabla 2.4 se aprecia el impacto que se produce en los diferentes aspectos de la organización.

Una vez hecho este análisis se procede a escoger las dos aplicaciones más críticas sobre las cuales se realizarán las pruebas de seguridad.

Analizando la Matriz de impacto sobre la organización, se aprecia que los servicios más importantes son: Recaudación, Seguridades y el Portal Web del MDMQ.

Si se considera el Listado de Prioridades los servicios prioritarios son: Recaudación y el Portal Web del MDMQ, entre otros. Considerando la matriz de impacto, los sistemas más importantes son:

- Recaudación (5) – Impacto muy alto.
- Portal web del MDMQ (5) – Impacto muy alto.

Por lo descrito anteriormente las aplicaciones consideradas como críticas son las siguientes; La primera aplicación que se escogió para realizar la prueba de penetración es el portal web del MDMQ, ya que posee una prioridad muy alta, representa la imagen de la institución y es el nexo hacia varios servicios y aplicaciones web que presta el Municipio de Quito y en la matriz de impacto posee un valor de (5).

Le segunda escogida para realizar las pruebas de penetración es el portal de pago de impuestos por Internet ya que tiene una prioridad muy alta, de él dependen los sistemas SIREC-Q, TOC, SIMET-Q y SAO. Además, al ser una aplicación web que maneja transacciones de dinero se considera un servicio muy crítico y en la matriz de impacto posee un valor de (5).

Los otros sistemas como Seguridades, Infraestructura del *Data Center* y Reportes Gerenciales, etc., si bien de ellos dependen varios sistemas o se han clasificado como sistemas con una prioridad muy alta, no son tomados en cuenta y son descartados para las pruebas de seguridad, dado que no se encuentran en el listado de los sistemas y aplicaciones que la DMI del MDMQ permitió analizar.

ACTIVOS DE LA INFORMACIÓN	CONFIDENCIALIDAD				DISPONIBILIDAD				INTEGRIDAD			
	Innovación	Excelencia en la Gestión	Servicio al Cliente	Imagen y Reputación	Innovación	Excelencia en la Gestión	Servicio al Cliente	Imagen y Reputación	Innovación	Excelencia en la Gestión	Servicio al Cliente	Imagen y Reputación
Portal Municipio de Quito	5	5	5	5	5	5	5	5	5	5	5	5
Sistemas de Regulación Metropolitana (IRM)	4	4	4	4	3	3	4	4	3	4	4	5
Informe de Compatibilidad de Uso de Suelo (ICUS)	4	4	4	4	3	3	4	4	3	4	4	5
Sistema de Patentes	4	4	4	4	3	3	4	4	3	4	4	5
Sistema de Pago de Impuestos por Internet	4	5	5	5	4	5	5	5	4	5	5	5
Sistema de Registro Catastral (SIRECQ)	4	3	4	4	4	3	4	4	4	4	4	5
Portal Prensa	3	3	5	5	3	3	5	5	3	3	5	5
Radio Municipal	3	3	5	5	3	3	5	5	3	3	5	5
Portal LUEA Web	2	3	5	4	2	3	5	4	2	3	5	4
Portal Educación	2	3	5	4	2	3	5	4	2	3	5	4

Tabla 2.3 Matriz de impacto

ACTIVOS DE LA INFORMACIÓN	CONFIDENCIALIDAD				DISPONIBILIDAD				INTEGRIDAD				IMPACTO			
	Innovación	Excelencia en la Gestión	Servicio al Cliente	Imagen y Reputación	Innovación	Excelencia en la Gestión	Servicio al Cliente	Imagen y Reputación	Innovación	Excelencia en la Gestión	Servicio al Cliente	Imagen y Reputación	Confidencialidad	Disponibilidad	Integridad	Total
Portal Municipio de Quito	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Sistemas de Regulación Metropolitana (IRM)	4	4	4	4	3	3	4	4	3	4	4	5	4	4	4	4
Informe de Compatibilidad de Uso de Suelo (ICUS)	4	4	4	4	3	3	4	4	3	4	4	5	4	4	4	4
Sistema de Patentes	4	4	4	4	3	3	4	4	3	4	4	5	4	4	4	4
Sistema de Pago de Impuestos por Internet	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5
Sistema de Registro Catastral (SIRECQ)	4	3	4	4	4	3	4	4	4	4	4	5	4	4	4	4
Portal Prensa	3	3	5	5	3	3	5	5	3	3	5	5	4	4	4	4
Radio Municipal	3	3	5	5	3	3	5	5	3	3	5	5	4	4	4	4
Portal LUEA Web	2	3	5	4	2	3	5	4	2	3	5	4	4	4	4	4
Portal Educación	2	3	5	4	2	3	5	4	2	3	5	4	4	4	4	4

Tabla 2.4 Matriz de impacto sobre la organización

## CAPÍTULO 3

### PRUEBAS DE PENETRACIÓN: IMPLEMENTACIÓN DE EVALUACIÓN DE SEGURIDAD

En este capítulo se describen las pruebas de seguridad que se van a realizar en las aplicaciones web, basadas en la Guía de Pruebas OWASP 4.0 [1], [49].

Para identificar de mejor manera la categoría a la que pertenece cada prueba de seguridad el proyecto OWASP, se ha creado una nomenclatura para cada una de ellas, la cual está formada de la siguiente manera:

#### OTG-INFO-001

- **OTG:** OWASP *TESTING GUIDE V 4.0* (Guía de Pruebas OWASP V 4.0).
- **INFO:** Categoría, en este caso Recopilación de Información (*Information Gathering*).
- **001:** Número de prueba dentro de la categoría, en este caso prueba número uno de la categoría Recopilación de Información.

Las categorías son las siguientes:

- Recopilación de Información (OTG-INFO).
- Pruebas de Gestión de la Configuración y la Implementación (OTG-CONFIG).
- Pruebas de Gestión de Identidad (OTG-IDENT)
- Pruebas de Autenticación (OTG-AUTHN)
- Pruebas de Autorización (OTG-AUTHZ).
- Pruebas de Gestión de Sesiones (OTG-SESS)
- Pruebas de Validación de Datos (OTG-INPVAL).
- Manejo de Errores (OTG-ERR).
- Criptografía (OTG-CRYPST).
- Pruebas de Lógica del Negocio (OTG-BUSLOGIC).

- Pruebas del lado del Cliente (OTG-CLIENT).

Cabe aclarar que no se han realizado todas las pruebas que se especifican en la Guía de Pruebas OWASP 4.0 [1], ya que no todas se pueden realizar a las aplicaciones web objeto de estudio. Debido a esto las pruebas pertenecientes a las siguientes categorías no son tomadas en cuenta:

- Pruebas de Gestión de Identidad (OTG-IDENT): Tienen que ver con políticas de usuarios, roles y aprovisionamiento de cuentas, las mismas que en los objetos de estudio no se encuentran implementadas.
- Pruebas de Autenticación (OTG-AUTHN): Referentes a la autenticación o verificación de identidad de usuario, estas no fueron tomadas en cuenta, ya que las aplicaciones web objetos del estudio no cuentan con un inicio de sesión o login.
- Pruebas de Gestión de Sesiones (OTG-SESS): Controla la interacción del usuario con la aplicación, está pendiente del usuario desde el momento del al autenticación hasta su desconexión. La prueba OTG-SESS-005, falsificación de peticiones en sitios cruzados si se toma en cuenta ya que ésta pertenece al *Top Ten OWASP 4.0* [1].
- Pruebas de Lógica del Negocio (OTG-BUSLOGIC): Prueba casos de abuso o mal uso de la aplicación, elaborando variaciones de las pruebas realizadas en las otras categorías.
- Pruebas del lado del Cliente (OTG-CLIENT): Pruebas hechas desde un navegador web o con un complemento del mismo, son variaciones de las pruebas realizadas en las otras categorías.

Las categorías las cuales son consideradas para realizar las pruebas de seguridad, las mismas que están detalladas en sus respectivas secciones son las siguientes:

- Recopilación de Información (OTG-INFO).
- Pruebas de Gestión de la Configuración y la Implementación (OTG-CONFIG).
- Pruebas de Autorización (OTG-AUTHZ).
- Pruebas de Validación de Datos (OTG-INPVAL).

- Manejo de Errores (OTG-ERR).
- Criptografía (OTG-CRYPST).

Es importante mencionar que por cuestiones de seguridad algunos datos de los ejemplos van a ser anonimizados, por ejemplo las direcciones IP y las URL<sup>29</sup>.

### **3.1. RECOPIACIÓN DE INFORMACIÓN**

El objetivo de estas pruebas es recolectar la mayor cantidad de información disponible sobre el objetivo. Cualquier información es importante, desde la publicada en Internet hasta la obtenida con herramientas diseñadas para esto.

#### **3.1.1. DESCUBRIMIENTO CON MOTORES DE BÚSQUEDA Y RECONOCIMIENTO POR FUGAS DE INFORMACIÓN (OTG-INFO-001)**

El objetivo de esta prueba es buscar información de diseño y/o configuración de la aplicación que se encuentra expuesta en el Internet.

Con el fin de encontrar esta información se pueden utilizar motores de búsqueda como Google, Bing, Shodan, Yahoo, etc.

Para eso se utilizan expresiones especiales para realizar búsquedas avanzadas. Entre la información que se puede encontrar se tiene:

- Diagramas de red
- Nombres de usuarios y contraseñas
- Direcciones de correos
- Directorios sensibles
- Mensajes de error
- Archivos que contienen nombres de usuarios
- Archivos con información sensible
- Archivos que contienen contraseñas
- Versiones y tipos de servidores web

---

<sup>29</sup> Localizador Uniforme de Recursos (URL, *Uniform Resource Locator*)

- Archivos con configuraciones del servidor web

A continuación se muestran ejemplos de búsquedas avanzadas para el descubrimiento de información importante:

- Búsqueda de subdominios del objetivo: *site: ejemplo.com*
- Búsqueda de interfaz de administración Joomla: *site: ejemplo.com /administrator*
- Búsqueda de interfaz de administración WordPress: *site: ejemplo.com /wp-admin*
- Búsqueda de interfaz de administración Drupal: *site: ejemplo.com /user*
- Páginas con parámetros susceptibles a inyección SQL: *site: ejemplo.com "php?id="*
- Búsqueda de versión y tipo de servidor web Apache: *site: ejemplo.com intitle:index.of "Apache/\*"*
- Servidores con un archivo *password.txt*: *intitle:"index of" "Index of /" password.txt*
- Usuarios y contraseñas de bases de datos MySQL: *filetype:inc intext:mysql\_connect password -please -could -port*
- Cámaras web: *camera linksys inurl:main.cgi 700*
- Archivos robots.txt: "robots.txt" "disallow:" *filetype:txt*
- Búsqueda de versión y tipo de servidor web IIS: *site: ejemplo.com intitle:index.of "IIS/\*"*

Los subdominios es una extensión del dominio principal y su función es facilitar el acceso al contenido dentro de un sitio web.

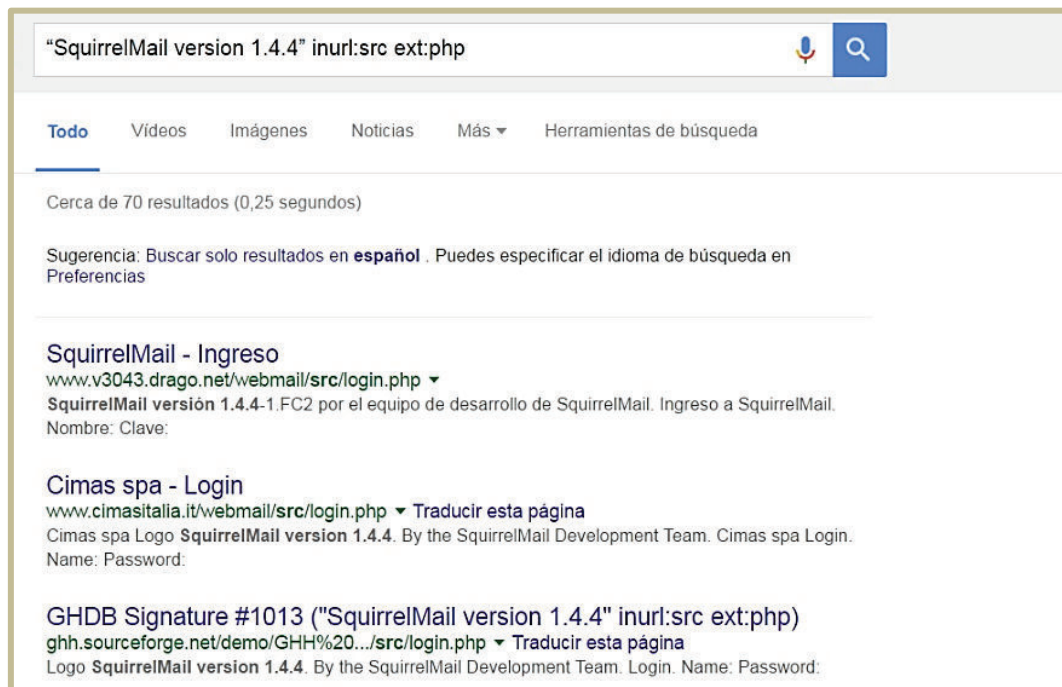
La búsqueda de subdominios es importante, ya que estos pueden estar mal configurados, expuestos o vulnerables. Un ejemplo sería una interfaz de administración o un panel de configuración.

En la figura 3.1 se muestra una búsqueda avanzada utilizando google *dorks*<sup>30</sup> para buscar en este caso un gestor de correo con su versión y su página de inicio de sesión. Los resultados obtenidos se aprecian a continuación.

---

<sup>30</sup> *Dorks* son búsquedas avanzadas utilizadas para extraer información valiosa desde Google.

Se observa en la figura varias páginas que coinciden con la búsqueda.



**Figura 3.1 Búsqueda avanzada en Google**

### 3.1.2. FINGERPRINT DEL SERVIDOR WEB (OTG-INFO-002)

Encontrar la versión y tipo de servidor web que aloja la aplicación es el objetivo de esta prueba, con esto se podrán buscar vulnerabilidades y *exploits* conocidos.

Para esta prueba se usará la herramienta `httprint` y `gregthatcher.com`.

En la figura 3.2 se aprecia como el comando `httprint [1]` obtiene información sobre el tipo y versión del servidor web, de la siguiente manera:

**`httprint -h dirección-IP -s signatures.txt`**

**-h:** Para especificar la dirección IP, URL o un rango de IP.

**-s `signatures.txt`:** Archivo que contiene las firmas para realizar el *fingerprint*.

Se nota que la dirección IP del servidor fue escondida por razones de seguridad, para mantener el anonimato del sitio que está siendo analizado.



```

root@bt:~/pentest/enumeration/www/httpprint/linux# ./httpprint -h [redacted] -s signatures.txt
httpprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httpprint/
httpprint@net-square.com

Finger Printing on http:// [redacted] /
Finger Printing Completed on http:// [redacted] /
-----
Host:
Derived Signature:
Apache
9E431BC86ED3C295811C9DC5811C9DC5050C5D32505FCFE84276E4BB811C9DC5
0D7645B5811C9DC5811C9DC5CD37187C11DDC7D7811C9DC5811C9DC58A91CF57
FCCC535B6ED3C295FCCC535B811C9DC5E2CE6927050C5D336ED3C295811C9DC5
6ED3C295E2CE6926811C9DC56ED3C2956ED3C2956ED3C2956ED3C295E2CE6923
E2CE69236ED3C295811C9DC5E2CE6927E2CE6923

Banner Reported: Apache
Banner Deduced: Apache/2.0.x
Score: 130
Confidence: 78.31
-----
Scores:
Apache/2.0.x: 130 78.31
Apache/1.3.[4-24]: 122 62.83
Apache/1.3.[1-3]: 122 62.83
Apache/1.3.27: 121 61.05
Apache/1.3.26: 120 59.31

```

Figura 3.2 Fingerprint del servidor web con netcat [1]

En la figura 3.3 se aprecia el fingerprint del servidor web con la ayuda de la herramienta web gregthatcher.com, simplemente colocando la URL de la página web, de resultados se obtiene el tipo y versión de servidor web, se recuerda que la URL ha sido escondida por cuestiones de privacidad.

### Find out which Web Server Software a website is running

Enter the domain name of the website.

http://

says it is running: Apache/2.2.3 (CentOS)

Page Title:

Additionally, it mentioned the following:

Connection : close;  
Accept-Ranges : bytes;  
Content-Length : 146;  
Content-Type : text/html;  
Date : Fri, 17 Mar 2017 01:33:36 GMT;

Figura 3.3 Fingerprint con gregthatcher.com

### 3.1.3. REVISIÓN DE META-ARCHIVOS POR FUGAS DE INFORMACIÓN (OTG-INFO-003)

Esta prueba describe como visualizar el contenido del archivo robots.txt<sup>31</sup>, con esto se puede encontrar información acerca de directorios o rutas a carpetas de la aplicación. También se podrá crear una lista de directorios que no son indexados por arañas, *robots* o *crawlers*.

Se puede tener el siguiente contenido en el archivo robots.txt

- **User-agent: \*: Robots**<sup>32</sup> de los motores de búsqueda que deberían hacer caso de las reglas, en este caso todos los robots.
- **Disallow: /templates:** Niega el acceso a los archivos almacenados en el directorio templates
- **Allow: /images:** Permite el acceso a los archivos almacenados en el directorio images
- **Sitemap: http://static.ejemplo.com/sitemap/sitemap.xml:** Incluye información sobre el mapa del sitio en formato xml<sup>33</sup>.

En esta prueba se utiliza un navegador web y la herramienta wget, con el propósito de encontrar archivos que contengan información relevante para un ataque. En la figura 3.4 se observa el contenido de un archivo robots.txt utilizando un navegador de la siguiente forma: **http://ejemplo.com/robots.txt**

```
User-agent: *
Disallow: /search
Allow: /search/about
Disallow: /sdch
Disallow: /groups
Disallow: /index.html?
Disallow: /?
Allow: /?hl=
```

Figura 3.4 Archivo robots.txt

<sup>31</sup> robots.txt es un método para evitar que *bots* indexen información de un sitio web a los resultados de búsqueda.

<sup>32</sup> *Robot* web, su uso más conocido es el *spidering*.

<sup>33</sup> XML: *Extensible Markup Language* es un lenguaje de etiquetado, su función principal es describir datos.

La figura 3.5 demuestra como se usa la herramienta wget para descargar el archivo robots.txt, luego se visualiza el contenido del archivo con cualquier comando head, cat, vim, tail, etc, de la siguiente manera.

**wget http://sitio.ejemplo.com/robots.txt:** Descarga el archivo robots.txt de la página seleccionada.

```

root@lulb0x:/usr/share/wordlists/ByteReaper_Lists# wget http://[redacted]/robots.txt
s.txt
cat: robots.txt: No such file or directory
--2016-07-01 11:10:48-- http://[redacted]/robots.txt
Connecting to [redacted] 80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 41 [text/plain]
Saving to: 'robots.txt'

robots.txt           100%[=====]           41  --.-KB/s
2016-07-01 11:10:48 (7.06 MB/s) - 'robots.txt' saved [41/41]

```

Figura 3.5 Descarga del archivo robots.txt con wget

### 3.1.4. ENUMERAR APLICACIONES EN EL SERVIDOR WEB (OTG-INFO-004)

Esta prueba tiene por objetivo enumerar los programas y servicios que corren en el servidor web con sus respectivas versiones, es posible también obtener información del sistema operativo. Para esta prueba se usa el comando nmap de la siguiente manera:

**nmap -T4 --source-port 80 -sS --send-ip -n --data-length 25 --mtu 24 -PN -f -sV dirección IP/URL**

**-T4:** T[0-5] Temporizador para observar los resultados, entre más alto, más rápido.

**--source-port 80:** Evasión de firewall, se hace pensar que el puerto origen es el 80.

**-sS:** Análisis TCP SYN<sup>34</sup>.

**--send-ip:** Enviar escaneo con paquetes IP.

**-n:** No hacer resolución DNS<sup>35</sup>.

**--data-length 25:** Añade datos aleatorios a los paquetes enviados, 25 bytes.

<sup>34</sup> SYN es un bit de control dentro del segmento TCP.

<sup>35</sup> DNS, *Domain Name System*, su función principal es la resolución de nombres de dominio.

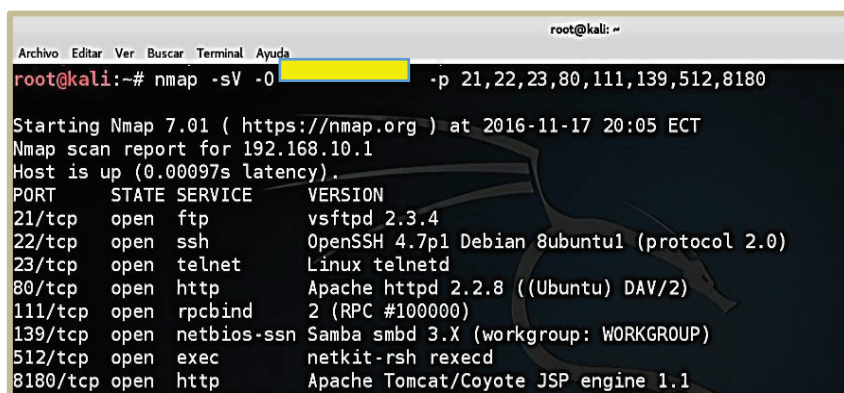
**--mtu 24:** Especificando la unidad máxima de transferencia<sup>36</sup> en 24 bytes.

**-PN:** Indicando al escaneo que no haga ping.

**-f:** Fragmenta los paquetes.

**-sV:** Obtener información del servicio y su versión.

La figura 3.6 muestra la enumeración de aplicaciones con el comando nmap [1], [35].



```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# nmap -sV -0 [redacted] -p 21,22,23,80,111,139,512,8180

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-17 20:05 ECT
Nmap scan report for 192.168.10.1
Host is up (0.00097s latency).
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
  
```

Figura 3.6 Enumerando servicios con nmap

### 3.1.5. REVISAR COMENTARIOS EN LA PAGINA WEB Y METADATOS POR FUGAS DE INFORMACIÓN (OTG-INFO-005)

Es muy común que los programadores dejen información detallada en forma de comentarios y metadatos en el código fuente. El objetivo de esta prueba es revisar dichos comentarios y metadatos para encontrar cualquier información sensible.

Para esta prueba se hace uso de la herramienta en línea [desenmacara.me](http://desenmacara.me) para revisar los metadatos de la página web y para encontrar comentarios se visualiza el código fuente de la página web con la ayuda del navegador.

En la figura 3.7 se observan los comentarios contenidos en el código fuente de una página web, para visualizar este código se presionan las teclas *control + u*, en este caso se puede observar en la parte resaltada un comentario en el código fuente el cual indica el nombre de usuario y contraseña para registrarse en el sitio web.

<sup>36</sup> Unidad Máxima de Transmisión (MTU) define el tamaño más grande de los paquetes que una interfaz puede transmitir sin necesidad de fragmentar.

```

38
39 </fieldset>
40
41 </form>
42 <!--  -->
43
44 <p>Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project</p>
45 <p><!-- default username is 'admin' with password 'password'--> </p>
46 </div> <!-- end align div -->
47
48 <br />
49
50
51

```

Figura 3.7 Comentarios en el código de una página web

La figura 3.8 muestra los resultados con la herramienta web desenmascara.me, simplemente colocando la URL de objetivo. Como se aprecia la información encontrada puede ser:

- Tipo de servidor web: Apache, NGINX, IIS, etc.
- Gestor de contenido (CMS): Joomla, WordPress, Drupal, etc.
- *Framework* de la Aplicación: PHP, ASP:NET.
- Dirección IP: Dirección IP pública del servidor web.

Metadato:	Valor
Metadato:	HTML5, HTTPServer[Apache]
Metadato:	IP[redacted]
Metadato:	JQuery[1.8.3]
Metadato:	Lightbox, Meta-Author[
Metadato:	Meta-Geo[0.241699, -78.486328, 0.241699;-78.486328,
Metadato:	MetaGenerator[WordPress 3.5.1]
Metadato:	Modernizr, Open-Graph-Protocol[blog]
Metadato:	Script[text/javascript]
Metadato:	Title[
Metadato:	WordPress[3.5.1, redacted]
Metadato:	x-pingback[http://redacted.xmlrpc.php]

Figura 3.8 Revisión de metadatos con desenmascara.me

### 3.1.6. IDENTIFICAR LOS PUNTOS DE ENTRADA DE LA APLICACIÓN (OTG-INFO-006)

Esta prueba tiene como objetivo entender cómo se forman las respuestas y solicitudes en la aplicación, identificando los métodos GET<sup>37</sup> y POST<sup>38</sup> y las variables que intervienen en el proceso de intercambio de información.

Para realizar esta prueba se usa la herramienta Burp Suite incluida en Kali Rolling 2016.2, sirve para intercepta e inspeccionar el tráfico de res.

En este caso se observa una solicitud con el método POST en el cual se puede evidenciar que las credenciales de inicio de sesión de algún sitio en particular viajan en texto claro. Otra información que se puede encontrar con esta herramienta son: parámetros y variables en la URL e incluso cookies que contienen información de inicio de sesión. Entre las información más importante encontrada, se tiene lo siguiente:

- Nombre de usuario: admin.
- Contraseña: password.
- Cookie de sesión: PHPSESSID.
- Dirección IP pública del servidor web.

La figura 3.9 presenta cómo está formada una solicitud de inicio de sesión.

```
POST /dwa/login.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-[REDACTED] zip, deflate
Referer: http://[REDACTED]/dwa/login.php
Cookie: security=high; PHPSESSID=7b97c5a82443bd3d9dcb423aa5752cda
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: [REDACTED]
username=admin&password=password&login=login
```

**Figura 3.9 Solicitud POST analizada con Burp Suite**

<sup>37</sup> Método HTTP que solicita datos de un recurso especificado.

<sup>38</sup> Método HTTP que envía los datos a procesar a un recurso especificado.

### 3.1.7. MAPEAR RUTAS DE EJECUCIÓN A TRAVÉS DE LA APLICACIÓN (OTG-INFO-007)

Mapear la aplicación para comprender mejor su estructura y flujo de trabajo es necesario para una buena prueba de penetración.

Para esta se utilizan las herramientas OWASP ZAP y Burp Suite, el propósito es encontrar archivos y directorios sensibles dentro de la aplicación, con el fin de encontrar si existe fuga de información, este método se conoce como web *spidering*. También se puede crear un mapa de la aplicación o un árbol de directorios y de esta forma comprender de mejor manera el comportamiento de las misma.

OWASP ZAP funciona de la misma forma que Burp Suite, es una herramienta incluida en Kali Rolling 2016.2 la cual funciona como proxy, interceptando el tráfico que se intercambia con la aplicación web, de manera que puede ser analizado o modificado. Entre la información más importante que se puede encontrar con esta prueba se tiene:

- Árbol de directorios
- Directorios sensibles
- Archivos sensibles
- Parámetros y variables en las URL
- Direcciones administrativas
- Mapa de sitio
- Interfaces de inicio de sesión
- Metadatos

La figura 3.10 y 3.11 muestran el mapa de un sitio web después de haber aplicado el proceso de *spidering*, con OWASP ZAP y Burp Suite respectivamente.

Como resultados se muestra, en la fiura 3.10 un árbol de directorio, uno de los cuales podría contener información sensible. El la figura 3.11 se puede observar un resultado similar en otro sitio web.

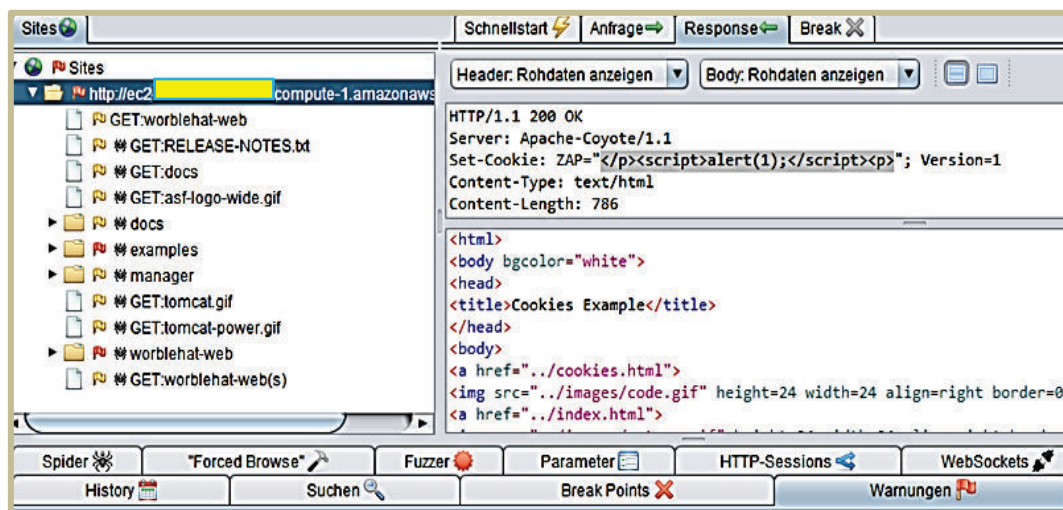


Figura 3.10 Spidering con OWASP ZAP

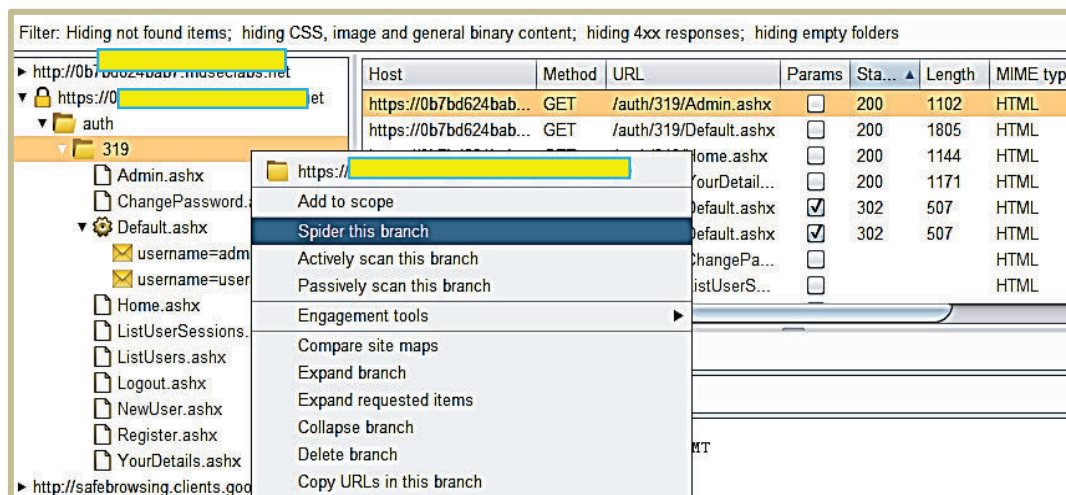


Figura 3.11 Spidering con Burp Suite

### 3.1.8. FINGERPRINT EL FRAMEWORK DE LA APLICACIÓN WEB (OTG-INFO-008)

Definir el tipo de *framework* web que utiliza la aplicación con el objetivo de buscar vulnerabilidades, este es el propósito de esta prueba.

Para la realización de esta prueba se utiliza el comando `whatweb` incluido en Kali Rolling 2016.2 de la siguiente manera:

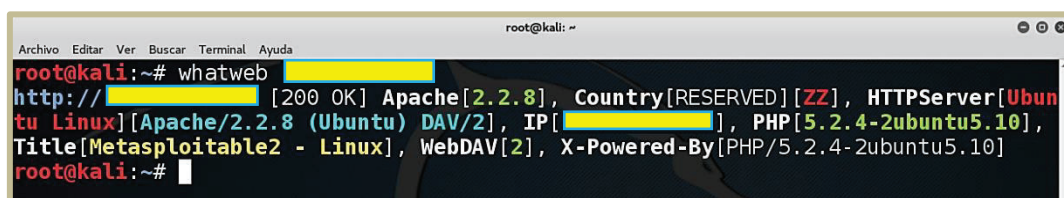
`whatweb http://pagina.ejemplo.com`



El campo X-Powered-By, muestra la versión de PHP<sup>39</sup> del servidor remoto, la cual representa el framework de la aplicación web, esta vulnerabilidad se conoce como revelación de información, en este caso se tiene PHP 5.2.4. Además se puede encontrar información como:

- Versión y tipo de servidor web
- Sistema operativo
- IP pública del servidor web
- CMS

La figura 3.12 demuestra el resultado de fingerprint del framework de una aplicación web.



```

root@kali:~# whatweb [redacted]
http://[redacted] [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], IP[redacted], PHP[5.2.4-2ubuntu5.10], Title[Metasploitable2 - Linux], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]
root@kali:~#

```

Figura 3.12 Fingerprinting del framework de una aplicación web

### 3.1.9. FINGERPRINT A LA APLICACIÓN WEB (OTG-INFO-009)

Identificar la versión y tipo de aplicación web es necesario para buscar vulnerabilidades conocidas y el *exploit*<sup>40</sup> apropiado para usar durante la prueba de penetración.

En esta prueba lo importante para la búsqueda de vulnerabilidades conocidas es determinar el gestor de contenido (CMS), para ello se ocupa el *plugin* Wappalyzer de Firefox y la herramienta whatweb que ya se explicó su uso en la sección 3.1.8.

Wappalyzer despliega la información obtenida en el portal o aplicación web en la barra de direcciones en forma de íconos, si se requiere visualizar de mejor manera estos resultados se debe pulsar sobre en dichos íconos.

<sup>39</sup> PHP es un lenguaje de programación del lado del servidor, es una herramienta para hacer páginas web dinámicas e interactivas.

<sup>40</sup> *Exploit* pequeño programa usado para aprovechar una vulnerabilidad de seguridad de un sistema de información.

Una de las variables que se encuentran en esta prueba es el CMS con el cual ha sido construida la aplicación web, en este caso un WordPress<sup>41</sup> 4.5.2.

Ademas, se puede encontrar información importante como:

- CMS
- Framework de la aplicación
- Sistema operativo
- *Cookies*
- Lenguaje de programación
- *Framework* Javascript
- Tipo y versión del servidor web

En la figura 3.13 se aprecia el *fingerprinting* en la aplicación web, para determinar el tipo de CMS que se está utilizando.

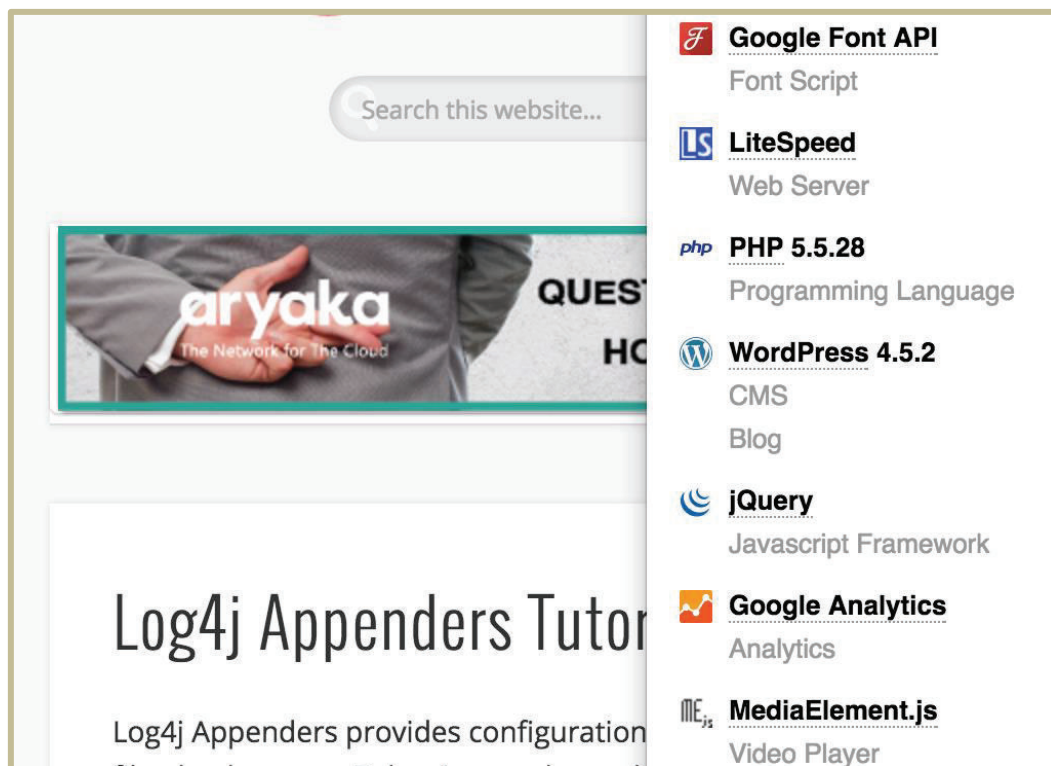


Figura 3.13 Fingerprint de una aplicación con wappalyzer

<sup>41</sup> WordPress, gestor de contenido, sirve para crea páginas web.

## 3.2. PRUEBAS DE GESTIÓN DE LA CONFIGURACIÓN Y LA IMPLEMENTACIÓN

Los errores de configuración pueden comprometer a la aplicación, así como una aplicación no segura puede comprometer al servidor.

Para evaluar la configuración e implementación, se realizarán las siguientes pruebas:

### 3.2.1. PRUEBA DE CONFIGURACIÓN DE RED/INFRAESTRUCTURA (OTG-CONFIG-001)

En esta prueba se necesita conocer la infraestructura que soporta a la aplicación y verificar que tan segura se encuentra. Lo que se debe analizar es lo siguiente [1]:

- Determinar qué elementos de seguridad protegen la infraestructura, entender como interactúan con la aplicación web y como afectan a su seguridad.
- Revisar sistemas de autenticación si la aplicación tiene implementado uno.
- Revisar configuración de los elementos de la infraestructura.

En la figura 3.14 se aprecia un diagrama de infraestructura que soporta una aplicación web.

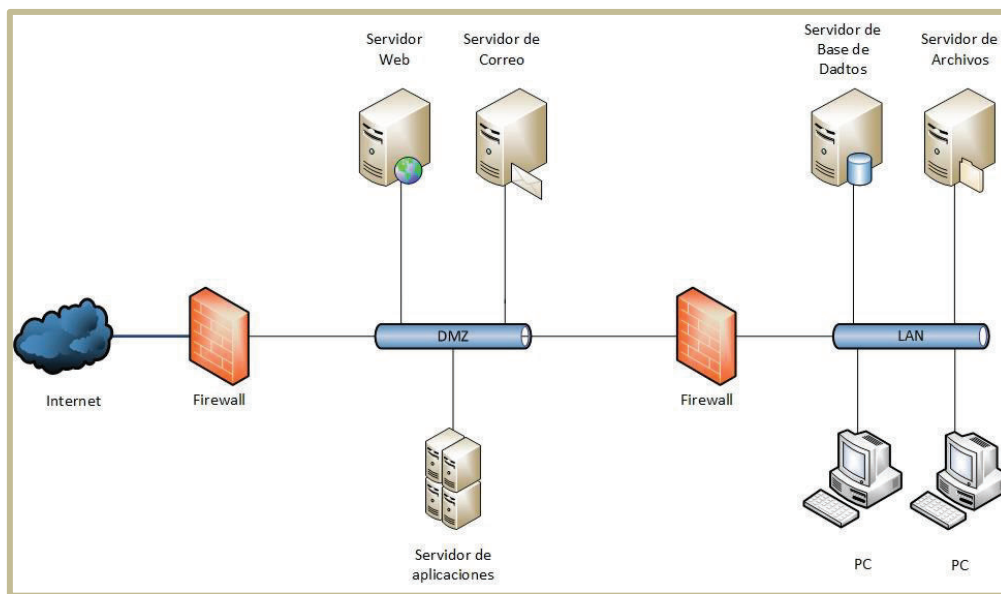


Figura 3.14 Diagrama de infraestructura de red

Con el presente diagrama de red se puede concluir:

- La organización posee un firewall interno.
- La organización posee un firewall externo para la salida a Internet.
- Se ha creado una zona desmilitarizada (DMZ).

### **3.2.2. PRUEBA DE CONFIGURACIÓN DE LA PLATAFORMA DE LA APLICACIÓN (OTG-CONFIG-002)**

En esta prueba lo que se busca es conocer si las instalaciones que se han hecho han sido personalizadas o si se han hecho instalaciones por defecto. Por ejemplo, conocer que módulos están activos en el servidor y si estos son los necesarios para que la aplicación funcione de manera adecuada.

Cabe indicar que para esta prueba no es necesaria la dirección IP de la víctima, ya que al tratarse de una prueba de caja blanca tenemos acceso al servidor y por ende se puede revisar su configuración.

Dependiendo de la distribución Linux la forma de listar los módulos<sup>42</sup> activos en el servidor web se tienen los siguientes comandos:

- `apache2 -L`
- `apachectl -M`
- `apache2ctl -t -D DUMP_MODULES`
- `httpd -M`
- `/usr/local/apache22/bin/httpd -M`

El resultado obtenido es un listado de los módulos que han sido compilados dentro del servidor web.

La figura 3.15 muestra una lista de los módulos que han sido activados en un servidor web Apache.

---

<sup>42</sup> Un Módulo en Apache sirve para agrupar funcionamientos dentro del servidor, ya que no todas las instalaciones requieren las mismas funcionalidades.

```

root@webserver:~# apache2ctl -t -D DUMP_MODULES
Loaded Modules:
  core_module (static)
  log_config_module (static)
  logio_module (static)
  mpm_prefork_module (static)
  http_module (static)
  so_module (static)
  alias_module (shared)
  auth_basic_module (shared)

```

Figura 3.15 Módulos activos en un servidor Apache

Al tratarse de un sistema operativo Windows Server la manera de listar los módulos/features es la siguiente:

**C:\Windows\System32\ServerManagerCmd.exe -q > C:\Logs\IIS.log** para Windows Server 2008

**Get-WindowsFeature > C:\Logs\IIS.log** para Windows Server 2012

En la figura 3.16 se observan de una manera gráfica los módulos/features instalados en un servidor web IIS de Microsoft.

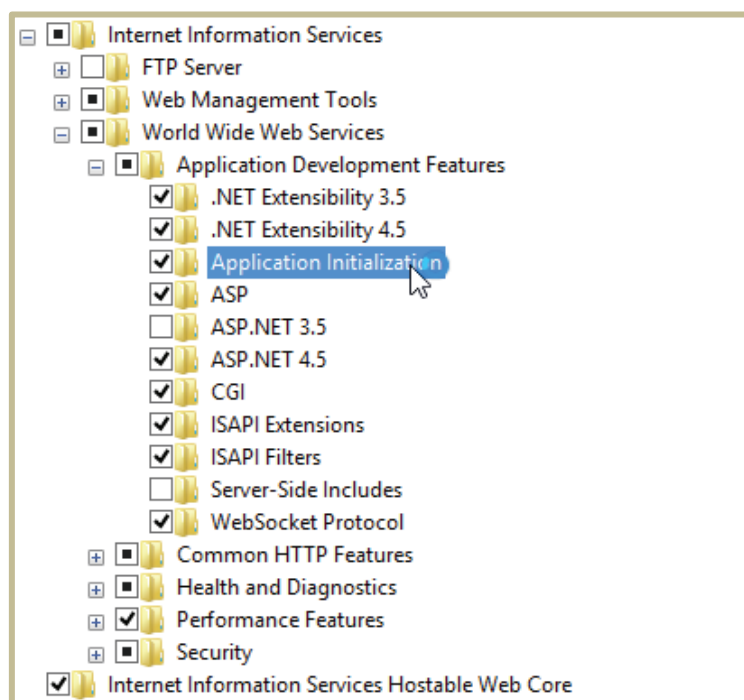


Figura 3.16 Módulos/features activos en un servidor IIS

### 3.2.3. ARCHIVOS DE BACKUP Y NO REFERENCIADOS CON INFORMACIÓN SENSIBLE (OTG-CONFIG-004)

Existen archivos que pueden revelar información confidencial que puede ser utilizada para realizar ataques a la aplicación. Por ejemplo, rutas de archivos absolutas o archivos que contienen información de credenciales de bases de datos.

Los archivos antiguos y copias de respaldo pueden contener vulnerabilidades que se han corregido en versiones más recientes; por ejemplo el archivo *viewdoc.old.jsp* puede contener una vulnerabilidad de *path traversal* que ha sido corregida en *viewdoc.jsp* pero todavía puede ser explotada por cualquiera que encuentre la versión antigua [1].

Los registros pueden contener información importante sobre las actividades de los usuarios. Por ejemplo, números de tarjetas de crédito, identificadores de usuario, contraseñas.

El objetivo de esta prueba es verificar que no existan archivos que puedan revelar información sensible o confidencial, que pueda afectar al desempeño de la aplicación o sea perjudicial para los usuarios de la misma.

### 3.2.4. ENUMERAR INTERFACES DE ADMINISTRACIÓN DE APLICACIONES Y DE INFRAESTRUCTURA (OTG-CONFIG-005)

Esta prueba tiene por objetivo encontrar interfaces de administrador, esta puede estar presente en la aplicación o en el servidor de la aplicación. Estas interfaces permiten a usuarios privilegiados realicen ciertas actividades que los usuarios no autorizados o estándar no pueden realizar.

Para realizar esta prueba se hace uso de un navegador web de la siguiente manera:

**<http://sitio.ejemplo.com/administrator>** para Joomla

**<http://sitio.ejemplo.com/wp-admin>** Para WordPress

<http://sitio.ejemplo.com/user> Para Drupal

En la figura 3.17 se expone una interfaz de administrador de un sitio basado en WordPress.



Figura 3.17 Interfaz de administrador

### 3.2.5. PRUEBA DE MÉTODOS HTTP (OTG-CONFIG-006)

Ya que HTTP ofrece una serie de métodos que son utilizados para realizar acciones en el servidor web, este debe estar correctamente configurado, caso contrario estos métodos pueden ser utilizados con propósitos perjudiciales para la aplicación.

En esta prueba se identifican los métodos que el servidor web maneja.

Para identificar los métodos configurados en el servidor web se utiliza la herramienta nmap con un script de la siguiente manera:

```
nmap -sV --script=http-methods dirección IP/URL -p 80
```

**-sV:** Obtener información del servicio y su versión

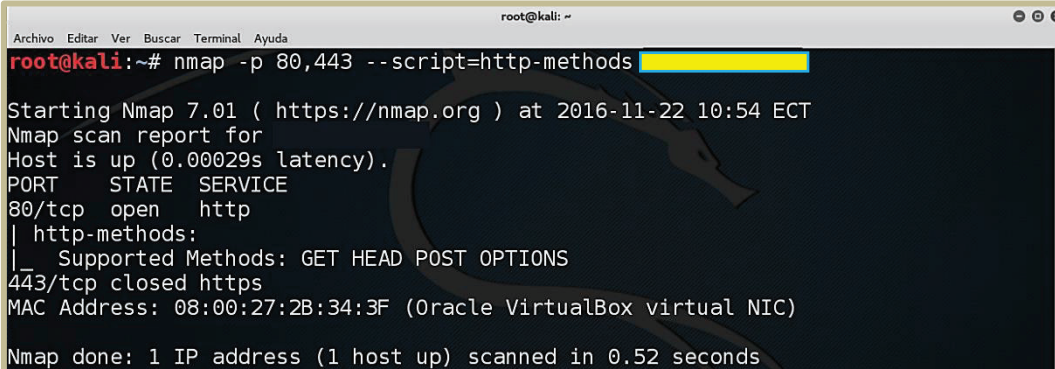
**--script=http-methods:** Script nmap para identificar métodos HTTP

**-p 80:** Escaneo del puerto 80

La información encontrada en la presente prueba es la siguiente:

- Métodos HTTP configurados: GET, HEAD, POST, OPTIONS
- Sistema operativo
- Versión y tipo de servidor web
- Framework de la aplicación

En la figura 3.18 se visualizan los métodos que soporta el servidor web.



```

root@kali: ~# nmap -p 80,443 --script=http-methods
Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-22 10:54 ECT
Nmap scan report for
Host is up (0.00029s latency).
PORT      STATE SERVICE
80/tcp    open  http
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
443/tcp    closed https
MAC Address: 08:00:27:2B:34:3F (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
  
```

**Figura 3.18 Métodos HTTP que soporta un servidor web**

### 3.2.6. PRUEBA DE SEGURIDAD DE TRANSPORTE ESTRICTO HTTP - HSTS (OTG-CONFIG-007)

La seguridad de transporte estricto de HTTP (HSTS) es un mecanismo que los sitios web comunican a los navegadores para que todo el tráfico intercambiado se envíe siempre a través de HTTPS<sup>43</sup>, esto ayudará a proteger la información de las solicitudes que viajen sin estar cifradas. El objetivo de esta prueba es verificar que el sitio web este utilizando este mecanismo de seguridad. Este encabezado tiene dos directivas:

- Max-age: Indica el número de segundos para que el navegador convierta automáticamente todas las solicitudes HTTP a HTTPS.

<sup>43</sup> *Hypertext Transfer Protocol Secure* (Protocolo seguro de transferencia de hipertexto), HTTPS, realiza la transferencia segura de datos de Hipertexto.



- **IncludeSubDomains**: Para indicar que todos los subdominios<sup>44</sup> deben usar HTTPS.

Para esta prueba se utilizan las herramientas curl y el analizador web de Qualys Inc.

El comando curl se utiliza de la siguiente manera:

```
curl -s -D http://sitio.ejemplo.com | grep Strict
```

**-s**: Modo silencioso.

**-D**: Se utiliza para almacenar los encabezados HTTP de un sitio web.

**| grep Strict**: Busca la palabra *Strict* dentro del encabezado almacenado.

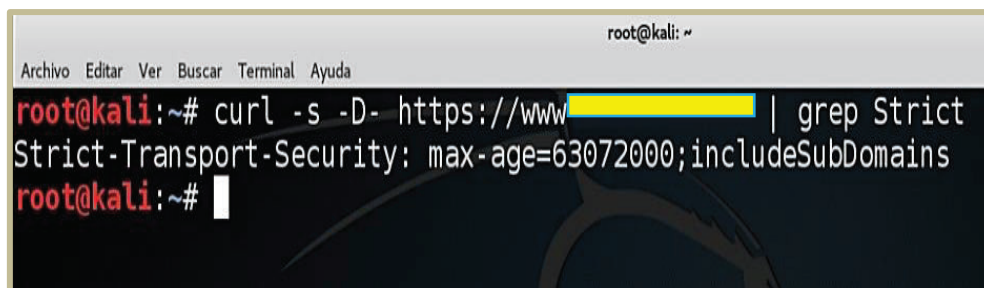
Entre los resultados podemos tener:

**max-age=<expire-time>**, el tiempo, en segundos, que el navegador debe recordar que este sitio sólo se puede acceder mediante HTTPS.

**IncludeSubDomains(Opcional)**, si se especifica este parámetro, se aplica también a todos los subdominios del sitio.

En el presente ejemplo se puede ver que el tiempo de expiración es 63072000 segundos (2 años), e incluye a todos los subdominios del sitio web.

La imagen 3.19 demuestra la implementación de HSTS en un servidor web.



```
root@kali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@kali:~# curl -s -D- https://www[redacted] | grep Strict  
Strict-Transport-Security: max-age=63072000;includeSubDomains  
root@kali:~#
```

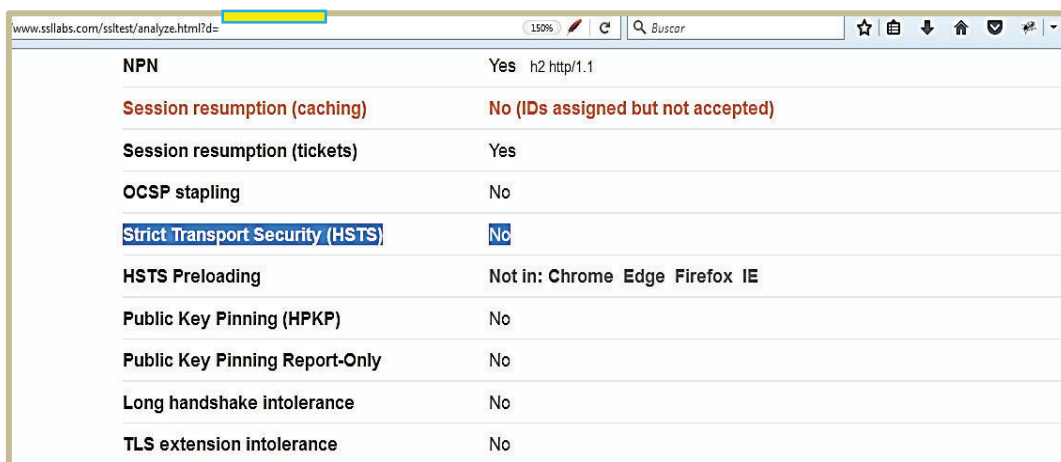
**Figura 3.19 Implementación de HSTS**

---

<sup>44</sup> Un subdominio es un subgrupo del nombre de dominio el cual es definido con fines administrativos u organizativos.

Con el analizador web de Qualys Inc, solo se necesita ingresar la URL del sitio objeto del análisis y verificar dentro del informe final si se ha implementado o no este sistema.

La figura 3.20 muestra el informe sobre HSTS de Qualys Inc. Se aprecia resaltado en azul que en el servidor tomado como ejemplo no se encuentra implementado este sistema de seguridad.



NPN	Yes	h2 http/1.1
Session resumption (caching)	No	(IDs assigned but not accepted)
Session resumption (tickets)	Yes	
OCSP stapling	No	
<b>Strict Transport Security (HSTS)</b>	<b>No</b>	
HSTS Preloading	Not in:	Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No	
Public Key Pinning Report-Only	No	
Long handshake intolerance	No	
TLS extension intolerance	No	

Figura 3.20 Análisis de HSTS con Qualys Inc.

### 3.2.7. PRUEBA DE POLÍTICA DE DOMINIO CRUZADO RIA (OTG-CONFIG-008)

*Rich Internet Applications* (RIA), adoptó los archivos de políticas `crossdomain.xml` de Adobe para permitir el acceso de dominio cruzado al consumo de datos y servicios mediante tecnologías como Java, Oracle, Adobe Flash. Esto quiere decir que un dominio puede conceder acceso remoto a sus servicios desde un dominio diferente.

Una mala configuración de este archivo puede generar ataques de *Cross-site Request Forgery* y permitir que personas no autorizadas accedan a datos privados predestinados al usuario.

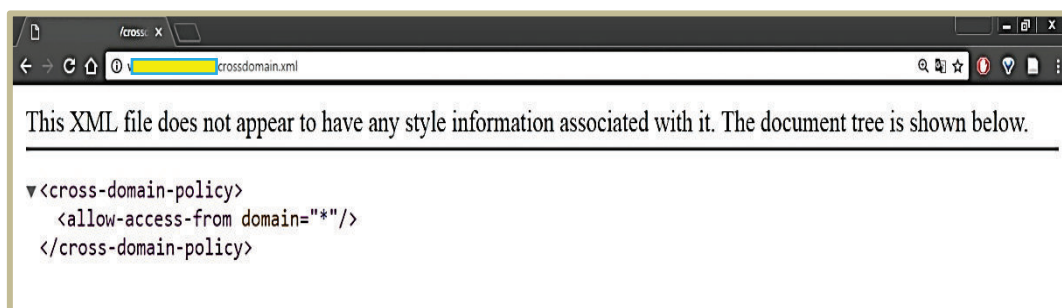
Para realizar esta prueba se hace uso de un navegadore web de la siguiente manera: **<http://www.ejemplo.com/crossdomain.xml>**. Los resultados esperados pueden ser:

**allow-access-from domain="\*"**: Concede a un dominio solicitante la lectura de datos del dominio de destino. Para cada solicitud a la que se da permiso, se requiere un nuevo elemento allow-access-from. En este caso se permite el acceso a todos los dominios (\*).

**site-control permitted-cross-domain-policies="all"**: Establece una meta-política<sup>45</sup> para el dominio actual, en este caso todos los archivos de políticas de este dominio de destino está permitido.

Para el ejemplo de observa que concede permiso de acceso desde todos los dominios.

En la figura 3.21 se detalla el contenido de un archivo crossdomain.xml.



**Figura 3.21 Contenido del archivo crossdomain.xml**

### 3.3. PRUEBAS DE AUTORIZACIÓN

En esta sección las pruebas tratarán de encontrar alguna forma de saltar el proceso de autorización, encontrar la forma de escalar privilegios o rutas transversales que permitan llegar a archivos que contengan información sensible y que solo está disponible para cierto tipo de usuarios.

#### 3.3.1. PRUEBA DE DIRECTORIO/PATH TRAVERSAL (OTG-AUTHZ-001)

Esta vulnerabilidad ocurre cuando no existe suficiente seguridad en los procesos de autorización de usuarios, con esto se puede acceder a cualquier archivo o información que se encuentra fuera de la carpeta raíz de la web.

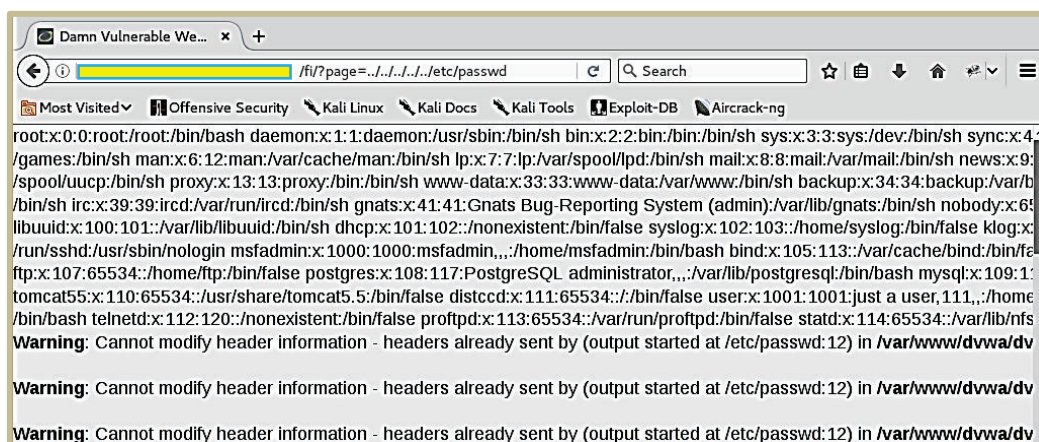
<sup>45</sup> Una meta política especifica archivos de políticas de dominio aceptables.

Se lo conoce como el ataque punto-punto-slash (../), ya que con esta secuencia o sus variaciones puede ser posible acceder a directorios o archivos almacenados en el sistema de archivos del servidor web.

Para esta prueba se hace uso de un navegador de la siguiente manera:

**http://sitio.ejemplo.com/dir1/video/0?itemid=../..../etc/passwd**

En la figura 3.22 se muestra el resultado de un ataque de directorio traversal donde se accedió al archivo `/etc/passwd`<sup>46</sup>.



**Figura 3.22 Ataque de path traversal**

También se usa una herramienta automatizada para realizar la misma prueba, esta viene incluida en Kali Rolling 2016.2, se llama *dotdotpwn* y su uso es de la siguiente manera:

**Dotdotpwn -m HTTP -u http://**

**sitio.ejemplo.com/dir1/video/0?itemid=TRAVERSAL**

**-m:** Módulo, puede ser HTTP, FTP, Payload

**-u:** Indica la URL a examinar, el parámetro *TRAVERSAL* indica que en esa sección empieza a realizar las diferentes variantes que existe para realizar el ataque de path traversal.

<sup>46</sup> El archivo `passwd` es una base de datos basada en texto de información sobre usuarios que pueden iniciar sesión en el sistema.

Como resultado del ejemplo vemos que se encontró la presencia de la vulnerabilidad.

La figura 3.23 muestra el accionar de la herramienta, en un servidor FTP.

```
[+] FTP Server's Current Path: /
[+] Local Path to download files: /home/nitr0us/dotdotpwn-v2.0/retrieved_files
[+] Press any key to continue

[+] Testing ...
[*] CD ../../../../ | GET boot.ini <- VULNERABLE!
[*] CD ../../../../windows/system32/drivers/etc/ | GET hosts <- VULNERABLE!
[*] CD ../../../../ | GET boot.ini <- VULNERABLE!
[*] CD ../../../../windows/system32/drivers/etc/ | GET hosts <- VULNERABLE!
[*] CD ../../../../ | GET boot.ini <- VULNERABLE!
[*] CD ../../../../windows/system32/drivers/etc/ | GET hosts <- VULNERABLE!
[*] CD ../../../../ | GET boot.ini <- VULNERABLE!
[*] CD ../../../../windows/system32/drivers/etc/ | GET hosts <- VULNERABLE!
[*] CD ../../../../ | GET boot.ini <- VULNERABLE!
[*] CD ../../../../windows/system32/drivers/etc/ | GET hosts <- VULNERABLE!
[*] CD ../../../../ | GET boot.ini <- VULNERABLE!
[*] CD ../../../../windows/system32/drivers/etc/ | GET hosts <- VULNERABLE!
[*] CD ../../../../ | GET boot.ini <- VULNERABLE!
[*] CD ../../../../windows/system32/drivers/etc/ | GET hosts <- VULNERABLE!
[*] CD ../../../../ | GET boot.ini <- VULNERABLE!
[*] CD ../../../../windows/system32/drivers/etc/ | GET hosts <- VULNERABLE!
[*] CD ../../../../ | GET boot.ini <- VULNERABLE!
[*] CD ../../../../windows/system32/drivers/etc/ | GET hosts <- VULNERABLE!
[+] Fuzz testing finished
[+] Total Traversals found: 16
```

Figura 3.23 Path traversal con dotdotpwn

### 3.3.2. PRUEBA DE ESCALAMIENTO DE PRIVILEGIOS (OTG-AUTHZ-003)

Esta vulnerabilidad permite ganar privilegios dentro de un sistema, con esto le permite al atacante realizar más actividades de las que tiene permitido hacer.

En Windows el atacante trata de obtener privilegios de administrador, mientras que en sistemas Unix busca obtener privilegios de root<sup>47</sup>.

El escalamiento de privilegios puede ser horizontal o vertical. El escalamiento vertical se produce cuando en un sistema existen diferentes niveles de privilegios y un usuario alcanza un nivel superior al cual ha sido asignado, el escalamiento horizontal en cambio se genera cuando se accede a recursos de usuarios con el mismo nivel de privilegios. Para esta prueba se pueden utilizar las herramientas OWASP ZAP o Burp Suite, ambas incluidas en Kali Rolling 2016.2, a este proceso se conoce como *tampering*, este consiste en manipular las variables que se encuentran en las peticiones HTTP para lograr alcanzar privilegios diferentes.

<sup>47</sup> En sistemas operativos Unix, es el superusuario.

La figura 3.24 muestra un ejemplo de escalamiento de privilegios.

```

HTTP/1.1 200 OK
Server: Netscape-Enterprise/6.0
Date: Wed, 1 Apr 2006 13:51:20 GMT
Set-Cookie: USER=aW78ryrGrTWs4MnOd32Fs51yDqp; path=/; domain=www.
Set-Cookie: SESSION=k+KmKeHXTgDi1J5fT7Zz; path=/; domain= www.
Cache-Control: no-cache
Pragma: No-cache
Content-length: 247
Content-Type: text/html
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Connection: close

<form name="autoriz" method="POST" action = "visual.jsp">
<input type="hidden" name="profile" value="SysAdmin">
<body onload="document.forms.autoriz.submit()">

```

**Figura 3.24 Escalamiento de privilegios con OWASP ZAP**

El escalamiento de privilegios surge si al modificar el valor de la variable *profile* a *SysAdmin* este usuario obtiene privilegios de Administrador [1].

### 3.3.3. PRUEBA DE REFERENCIA DIRECTA INSEGURA A OBJETOS (OTG-AUTHZ-004)

Esta vulnerabilidad tiene lugar cuando la aplicación provee acceso directo a objetos modificando los parámetros proporcionados por los usuarios. Cuando el ataque es exitoso el atacante logra sobrepasar el proceso de autorización y acceder a recursos del sistema, como archivos de configuración o archivos de las bases de datos.

El objetivo de esta prueba es tratar de obtener acceso a archivos restringidos o funciones adicionales en la aplicación, modificando los parámetros utilizados en la comunicación con la misma. Para explicar este ataque se utiliza la siguiente URL, la cual es una solicitud común:

**<http://app.dominion.com/accessPage?menuitem=12>**

En este caso, el valor del parámetro *menuitem* se utiliza para indicar a la aplicación qué elemento de menú (y, por lo tanto, qué funcionalidad de aplicación) el usuario

está intentando acceder. Se supone que el usuario debe estar restringido y por lo tanto tiene enlaces disponibles sólo para acceder a los elementos de menú 1, 2 y 3. Mediante la modificación del valor del parámetro *menuitem* es posible omitir la autorización y acceder a la funcionalidad de la aplicación adicional [1].

En la figura 3.25 se muestra la URL modificando el parámetro *menuitem*, se puede observar un mensaje de error, comprobando en este caso que no se obtiene acceso a funcionalidades diferentes a las autorizadas.



**Figura 3.25 Modificación de parámetro, prueba referencia directa insegura a objetos**

### **3.4. PRUEBAS DE GESTIÓN DE SESIONES**

La gestión de sesiones es un punto muy importante a tratar cuando de aplicaciones web se refiere. Las sesiones son el mecanismo que controla la interacción entre la aplicación y el usuario. Este control se produce desde el momento de la autenticación del usuario, hasta cuando el usuario ha decidido salir de la aplicación.

HTTP es un protocolo sin estado, esto quiere decir que no almacena ningún dato de usuario en las peticiones.

El propósito de estas pruebas es verificar cómo la aplicación gestiona las sesiones con los usuarios.

#### **3.4.1. PRUEBA DE FALSIFICACIÓN DE PETICIONES EN SITIOS CRUZADOS - CSRF (OTG-SESS-005)**

Este ataque conocido como CSRF tiene como finalidad obligar al usuario mismo a realizar acciones no deseadas en la aplicación en la que se encuentra autenticado.

Este tipo de ataque se dirige únicamente al cambio de estado y no al robo de información.

Esta prueba de seguridad no se puede realizar en el presente trabajo, ya que para ello es necesario sistemas de autenticación, método que no está implementado en las aplicaciones objetos del estudio, pero se toma en cuenta y se explica este tipo de ataque, ya que pertenece al *Top Ten OWASP*[1].

En la sección 1.3.3 se indica el proceder de este tipo de ataque

La figura 3.26 muestra cómo se produce el ataque de CSRF, el proceso se explica a continuación.

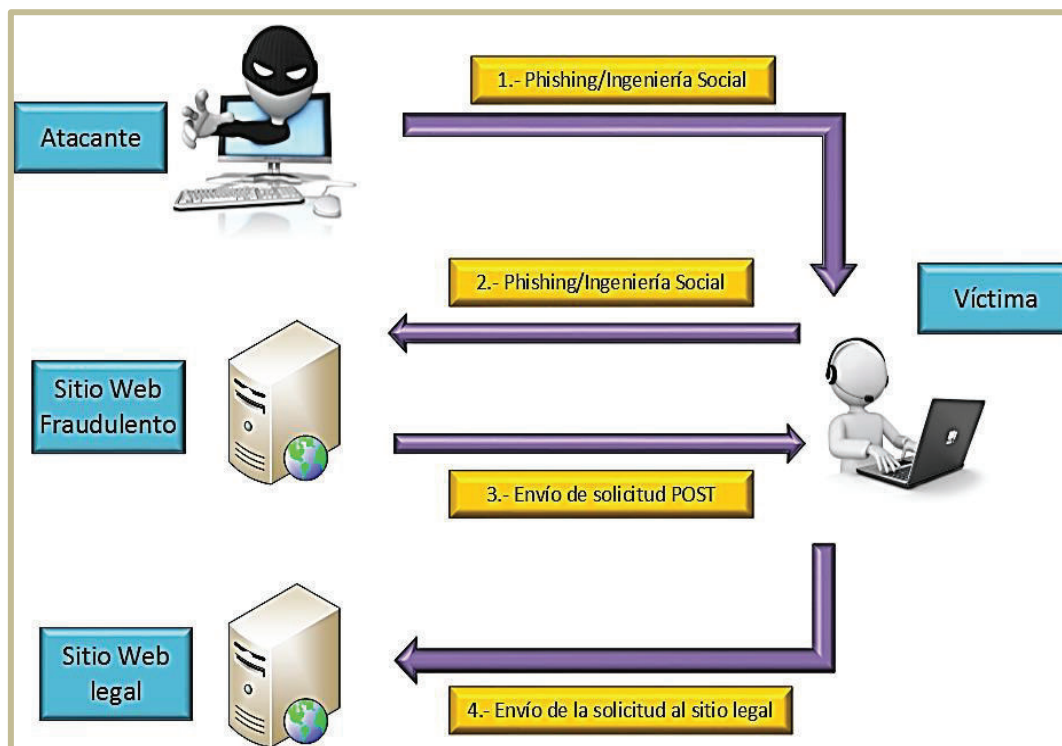


Figura 3.26 Cross site request forgery [21]

### 3.5. PRUEBAS DE VALIDACIÓN DE ENTRADA

Este grupo de pruebas tiene como objetivo verificar una de las vulnerabilidades más comunes en la seguridad de las aplicaciones web, la falta de validación correcta de las entradas que proceden del usuario antes de utilizarlas.



Esta debilidad conduce a las principales vulnerabilidades conocidas; XSS, inyección SQL, denegación de servicio, inclusión de archivos, inyección de comandos, inyección de código, etc.

### 3.5.1. PRUEBA DE CROSS SITE SCRIPTING REFLEJADO (OTG-INPVAL-001)

*Cross Site Scripting* reflejado (*Reflected - XSS*) es una de las vulnerabilidades más frecuentes, y también se conoce como XSS no persistente. Cuando se aprovecha de esta vulnerabilidad se pueden instalar keyloggers, robar cookies de las víctimas, cambiar el destino de los enlaces.

Este ataque se genera cuando se inyecta código ejecutable en el navegador, no es persistente, esto quiere decir que no se almacenan datos dentro de la aplicación y afecta al usuario que abre el enlace malintencionado o una página web de terceros.

Generalmente el código que inyecta el atacante está escrito en lenguaje Javascript<sup>48</sup>, pero puede escribirse en ActionScript<sup>49</sup> o VBScript<sup>50</sup> y está incluido como parte de los parámetros HTTP.

Esta prueba se la realizó de dos maneras, la primera forma con una herramienta para que haga el trabajo de forma automatizada llamada *xsser* [1] y la segunda de manera manual, usando simplemente el navegador web.

En la figura 3.27 se muestra el funcionamiento de la herramienta *xsser* y los resultados obtenidos con la misma.

Esta herramienta prueba de manera automatizada todas las variantes que existen para la inyección de este tipo de código. Se puede observar en la figura como la herramienta prueba las distintas formas y variantes de inyección de código, y va clasificando cada ataque como sospechoso, vulnerable, fallidos o errores.

En el presente ejemplo se observa que las inyecciones realizadas fueron fallidas.

---

<sup>48</sup> JavaScript es un lenguaje ligero orientado a objetos, sirve para crear efectos atractivos en páginas web.

<sup>49</sup> Lenguaje de programación de la plataforma Adobe Flash. sirve para construir animaciones de todo tipo.

<sup>50</sup> VBScript (*Microsoft Visual Basic Scripting Edition*)



La forma de verificar esta vulnerabilidad es parecida a la del XSS reflejado como se explica en la sección 3.5.1 y se produce en aquellas aplicaciones que permiten guardar algún tipo de dato al usuario, un ejemplo son los registros de visitas.

Para este ataque es necesario inyectar código HTML en sitios que permitan hacerlo. XSS almacenado toma información hostil, la almacena en un fichero, una base de datos, u otro sistema de almacenamiento, y luego en una etapa posterior, muestra dicha información sin filtrado alguno. Esto es extremadamente peligroso en sistemas de administración de contenidos (CMS), blogs, o foros, donde un gran número de usuarios accederá a la información introducida por otros usuarios [1].

La figura 3.29 muestra como el ataque de XSS almacenado afecta a un diario de visitas en una aplicación web, produciendo un mensaje de error.

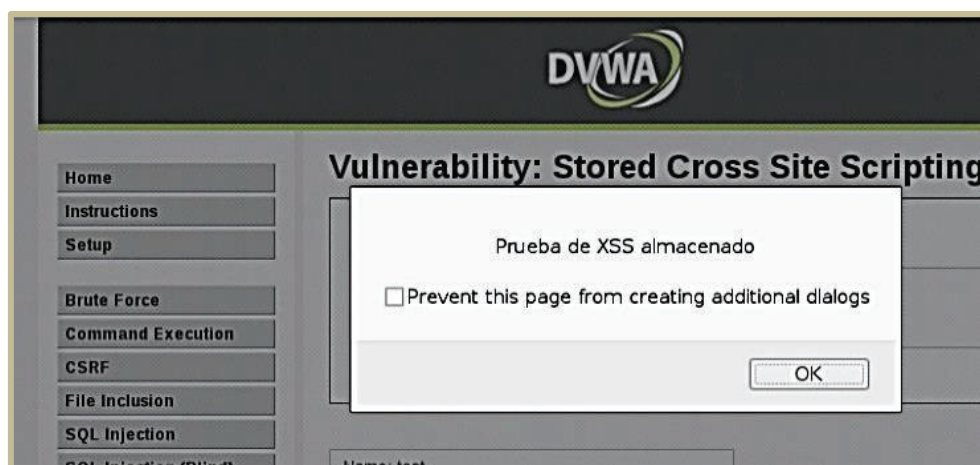


Figura 3.29 XSS almacenado

### 3.5.3. PRUEBA DE MANIPULACIÓN HTTP (OTG-INPVAL-003)

HTTP maneja una serie de métodos, los más comunes que se utilizan son GET y POST para realizar las peticiones, pero también pueden estar especificados otros métodos para obtener algo de información del servidor, como el método HEAD.

Pero las especificaciones de HTTP incluyen otros métodos, los cuales son utilizados para hacer pruebas y para el desarrollo de aplicaciones web, por lo tanto el objetivo de esta prueba es analizar el comportamiento de la aplicación cuando se utilizan

estos métodos diferentes, entre los cuales se tiene: OPTIONS, PUT, DELETE, TRACE, CONNECT, etc.

Para esta prueba se pueden utilizar las herramientas netcat o telnet de igual forma, para el presente ejemplo se usa el comando netcat para realizar una solicitud de la siguiente manera:

**nc direcciónIP/URL 80**

**TRACE / HTTP/1.1**

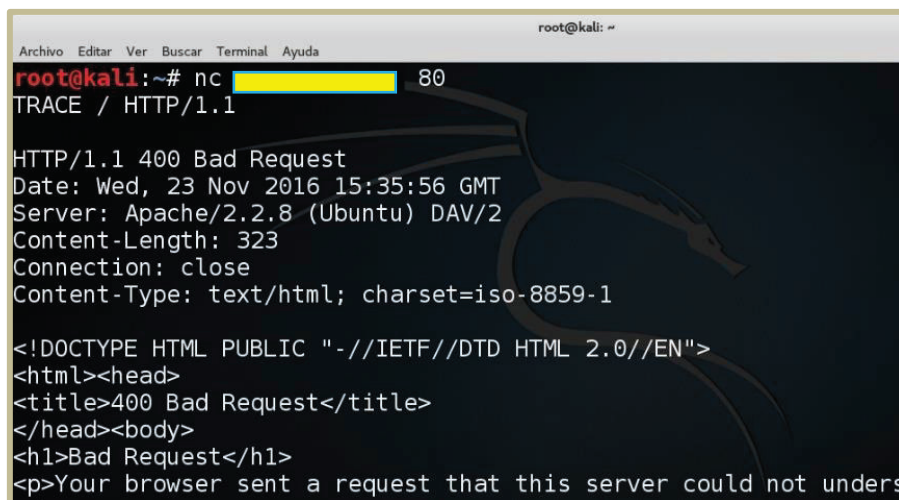
**80:** Puerto 80

**TRACE:** Método HTTP no implementado comúnmente.

**/:** Solicita el archivo raíz del sitio.

En la figura 3.30 se visualiza cómo responde un servidor web cuando se realiza una solicitud con el método TRACE. Entre los resultados obtenidos se puede encontrar:

- Sistema operativo
- Código de estado HTTP
- Versión y tipo de servidor web
- *Framework* de la aplicación



```
root@kali: ~# nc [redacted] 80
TRACE / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Wed, 23 Nov 2016 15:35:56 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Content-Length: 323
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not unders
```

Figura 3.30 Manipulación HTTP

### 3.5.4. PRUEBA DE INYECCIÓN SQL (OTG-INPVAL-005)

La inyección SQL consiste en la inserción de una consulta SQL total o parcial, a través de los datos de entrada desde el cliente hasta el servidor.

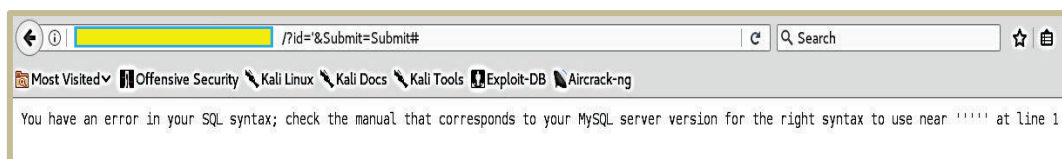
Si el ataque es exitoso, el atacante puede leer, modificar, hacer operaciones con la información contenida en la base de datos.

Por lo explicado anteriormente esta prueba tiene como objetivo verificar si la aplicación es vulnerable a la inyección SQL.

Para verificar esta vulnerabilidad lo primero que se hizo es encontrar páginas web con la búsqueda avanzada **site: ejemplo.com "php?id="**, los resultados deben tener el siguiente formato: **?id=xxx**, donde **?id=** es un ejemplo de vector de ataque, ya que la inyección SQL se puede dar sobre cualquier parámetro o variable que sea manipulada por la aplicación y xxx es un número, con esto se genera una solicitud de sintaxis incorrecta agregando un carater especial (**?id=xxx'**), si se produce el error nos indica que la aplicación tiene un error de configuración y que la vulnerabilidad puede estar presente.

Para el presente ejemplo se utiliza únicamente un navegador web.

La figura 3.31 presenta un error por una consulta SQL con mala sintaxis.



**Figura 3.31 Error en la base de datos**

Una vez comprobado el error se procede a realizar la inyección de código SQL de la siguiente manera:

**`http://sitio.ejemplo.com/item?id=1' or 1=1#`**

**1' or 1=1#** crea una declaración siempre verdadera para obtener la mayoría de los datos de la base de datos o forzar una declaración verdadera.

En la figura 3.32 se aprecia el resultado de la inyección SQL exitosa, donde se muestra información como nombres y apellidos de personas que han hecho uso de la aplicación web.



**Figura 3.32 Inyección SQL**

Esta prueba se puede realizar también de manera automatizada, utilizando la herramienta incluida en Kali Rolling 2016.2 llamada SQLMap [1], [47] de la siguiente manera:

**sqlmap -u "http://sitio.ejemplo.com/articulo?id=23"**

**-u:** Especifica la URL con parámetros susceptibles a inyección SQL, de esta manera la herramienta prueba todas las variantes de inyección que existen en su base de datos.

Cabe indicar que la URL debe estar escrita dentro de comillas, caso contrario la prueba tendrá un fallo.

La figura 3.33 muestra el proceso de inyección SQL con sqlmap

```

root@bt:~/pentest/web/scanners/sqlmap# ./sqlmap.py -u "https://[redacted]/index.jsp"

sqlmap/0.9 - automatic SQL injection and database takeover tool
http://sqlmap.sourceforge.net

[*] starting at: 12:36:44

[12:36:44] [INFO] using '/pentest/web/scanners/sqlmap/output/192.168.20.128/session' as session file
[12:36:44] [INFO] testing connection to the target url
[12:36:45] [INFO] testing if the url is stable, wait a few seconds
[12:36:46] [INFO] url is stable
[12:36:46] [INFO] testing if POST parameter 'word' is dynamic
[12:36:46] [WARNING] POST parameter 'word' is not dynamic
[12:36:49] [INFO] heuristic test shows that POST parameter 'word' might be injectable (possible DBMS: MySQL)
[12:36:49] [INFO] testing sql injection on POST parameter 'word'
[12:36:49] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:37:07] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[12:37:11] [INFO] POST parameter 'word' is 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause' injectable
[12:37:11] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[12:37:14] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
[12:37:16] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[12:37:39] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
POST parameter 'word' is vulnerable. Do you want to keep testing the others? [y/N] N
sqlmap identified the following injection points with a total of 32 HTTP(s) requests:
---
Place: POST
Parameter: word
  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
  Payload: word=test AND (SELECT 1870 FROM(SELECT COUNT(*),CONCAT(CHAR(58,109,121,117,58),(SELECT (CASE WHEN (1870=1870)
4,120,58),FLOOR(RAND(0)*2))x FROM information_schema.tables GROUP BY x)a)
---

```

Figura 3.33 Inyección SQL con sqlmap

### 3.5.5. PRUEBA DE INCLUSIÓN LOCAL DE ARCHIVOS (OTG-INPVAL-012)

Esta prueba tiene como objetivo verificar que no se puedan incluir archivos que se encuentran localmente en el servidor web.

Este ataque conocido como LFI (*Local File Inclusion*), busca visualizar archivos que están presentes localmente en el servidor, explotando procedimientos de inclusión vulnerables que están implementados en la aplicación.

Por ejemplo, cuando una página recibe como entrada la ruta de un archivo a incluirse y esta entrada no ha sido correctamente verificada, permite la escalada de directorios con el ataque punto-punto-slash.

Para encontrar página que puedan presentar esta vulnerabilidad se usa un método similar al explicado en la sección 3.5.4, páginas con parámetros que puedan ser modificados, y son vectores de ataque.

Una vez encontrada la página se procede a modificar la URL de la siguiente manera:

**<http://sitio.ejemplo.com/item?id=../../../../etc/hosts>**

Dependiendo de la gravedad de la vulnerabilidad esta puede conducir a otros ataques como XSS, DoS, revelación de información.

La figura 3.34 muestra el contenido del archivo `/etc/hosts`<sup>51</sup> únicamente cambiando los parámetros en la URL. La realización de la prueba es similar a la explicada en la sección 3.3.1 prueba de directorio/*path traversal*.

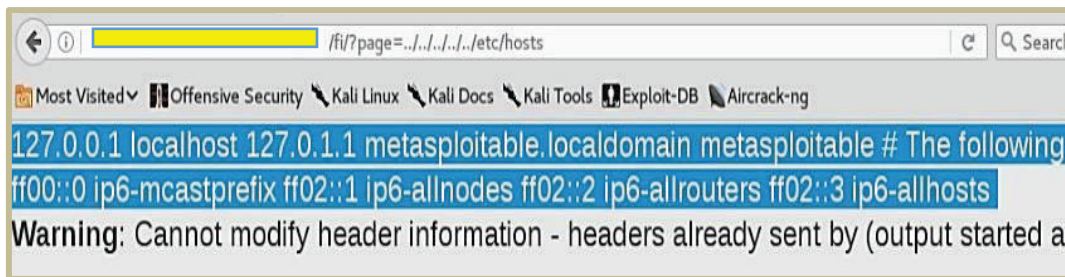


Figura 3.34 LFI con un navegador web

### 3.5.6. PRUEBA DE INYECCIÓN DE COMANDOS (OTG-INPVAL-013)

Esta prueba tiene por objetivo tratar de inyectar códigos que utiliza el sistema operativo para mostrar información adicional a la que la aplicación fue diseñada para mostrar.

La inyección de comandos se hace a través de la interfaz web de la aplicación.

En la figura 3.35 se observa cómo se inyecta el comando `pwd`<sup>52</sup> en una aplicación web que tiene por finalidad realizar un ping<sup>53</sup> a un host, de la siguiente manera:

En el cuadro de entrada de datos se ingresan los siguientes parámetros.

#### **direcciónIP | pwd**

**direcciónIP:** Dirección ip a la cual se va hacer el ping.

**comando:** Inyecta el nuevo comando a realizarse, en este caso el comando `pwd` que muestra el directorio actual de trabajo.

<sup>51</sup> Este es un archivo de texto plano, asocia direcciones IP con nombres de host.

<sup>52</sup> Pwd (*print working directory*) imprime el nombre del directorio actual de trabajo.

<sup>53</sup> Ping (*packet internet groper*) es una utilidad que comprueba el estado de la comunicación de un host local con uno o varios equipos remotos de una red.





Figura 3.35 Inyección de comando

Esta prueba se puede realizar de manera automatizada, haciendo uso de la herramienta *commix* de la siguiente forma:

```
commix --url="http://sitio.ejemplo.com/dir/0?itemid=INJECT_HERE"
```

**--url:** Indica la URL donde se quiere realizar el ataque.

**INJECT\_HERE:** Le indica a la herramienta que en esa parte de la URL debe inyectar los comandos de manera automática.

Cabe indicar que la URL debe estar escrita dentro de comillas, caso contrario la prueba tendrá un fallo.

La figura 3.36 muestra la interfaz y el ataque realizado con la herramienta *commix*, obteniendo como resultado una inyección de comando exitosa, la cual obtuvo una interfaz shell para realizar cualquier actividad dentro de la aplicación.

### 3.6. MANEJO DE ERRORES

En esta sección de la prueba de penetración se explica cómo la aplicación maneja los errores cuando se genera una petición de una página que no existe o una petición errónea.

```

root@localhost:~/commix# python commix.py --url="http://[redacted]/cmdinj/vulnerab
le.php?cmd=INJECT_HERE"

v0.2b-NonGit }

+--
Automated All-in-One OS Command Injection and Exploitation Tool
Copyright (c) 2015 Anastasios Stasinopoulos (@ancst)
+--

(*) Checking connection to the target URL... [ SUCCEED ]
(*) Setting the (GET) 'cmd' parameter for tests.
(*) Testing the classic injection technique... [ SUCCEED ]
(!) The (GET) 'cmd' parameter is vulnerable to Results-based Command Injection.
    (+) Type : Results-based Command Injection
    (+) Technique : Classic Injection Technique
    (+) Payload : echo PPYLUH${(87+14)}$(echo PPYLUH)PPYLUH

(?) Do you want a Pseudo-Terminal shell? [Y/n/q] > y

Pseudo-Terminal (type '?' for shell options)
Shell > id

u

Shell > █

```

Figura 3.36 Inyección de comandos con commix [1]

### 3.6.1. ANÁLISIS DE CÓDIGOS DE ERROR (OTG-ERR-001)

Esta prueba tiene por objetivo analizar los errores mostrados por el servidor web al solicitar una página inexistente. Si estos mensajes de error no son personalizados se puede revelar información sobre el servidor y su versión.

Para esta prueba se utilizan dos herramientas, la primera es un navegador web y la segunda es el comando telnet.

Como resultados de esta prueba se puede obtener lo siguiente:

- Sistema Operativo
- Versión y tipo de servidor web
- *Framework* de la aplicación

Para solicitar una página inexistente en el servidor basta con cambiar el nombre de una página válida, de la siguiente manera:

<http://sitio.ejemplo.com/index.php> Página válida

<http://sitio.ejemplo.com/index234.php> Página inexistente

La figura 3.37 muestra un mensaje de error de una página no encontrada, donde se aprecia información sobre el servidor. La información determinada en el ejemplos es, un servidor Web Apache versión 2.2.8, en un sistema operativo Ubuntu.

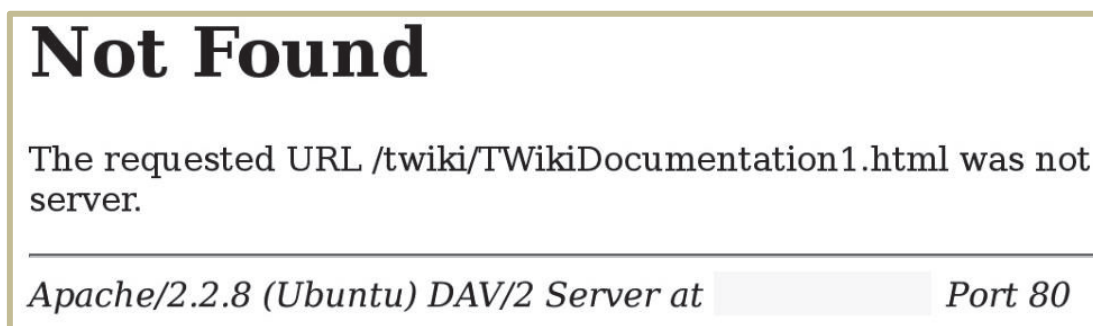


Figura 3.37 Mensaje de error no personalizado

El uso de telnet para realizar la presente prueba es el siguiente:

```
telnet http://sitio.ejemplo.com 80
```

```
GET /iindex1234.html HTTP/1.1
```

De esta manera al solicitador la página inexistente iindex1234.html devolverá por consola el error, con su respectivo encabezado, revelando o no información sobre el servidor web. En este caso se obtuvo la versión y tipo de servidor web y el sistema operativo sobre el cual esta implementado el mismo. La figura 3.38 muestra el resultado de la prueba utilizando la herramienta telnet.

```
root@kali:~# telnet [redacted] 80
Trying [redacted] ..
Connected to [redacted].
Escape character is '^]'.
GET /iindex1.html HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Mon, 20 Mar 2017 16:18:21 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
```

Figura 3.38 Mensaje de error generado con telnet

### 3.7. CRIPTOGRAFÍA

Esta sección de pruebas verifica si los datos transmitidos entre el usuario y la aplicación se transportan de manera segura.

#### 3.7.1. PRUEBA DE CIFRADO TLS/SSL DÉBIL Y PROTECCIÓN INSUFICIENTE DE CAPA DE TRANSPORTE (OTG-CRYPST-001)

Esta prueba tiene por objetivo verificar si la información que se envía entre el usuario y la aplicación viaja de manera segura o en texto plano.

Esta falla de seguridad podría llegar a ser perjudicial, ya que si se transmite información sensible como contraseñas o cuentas bancarias en texto plano, existe el riesgo de captura y fuga de información.

También se analiza que tan fuerte es el cifrado TLS/SSL y sobre la validez del certificado de seguridad.

Para esta prueba se utiliza la herramienta nmap y también se revisa de forma manual la seguridad del sitio web. Para verificar si los servicios usan TLS/SSL se hace un escaneo con nmap de la siguiente manera:

```
nmap --script=ssl-cert,ssl-enum-ciphers -p 443,465,993,995 dirección IP/URL -oN crypst-001-nmap.txt
```

**script ssl-cert:** Script para revisar el certificado SSL de un servidor web

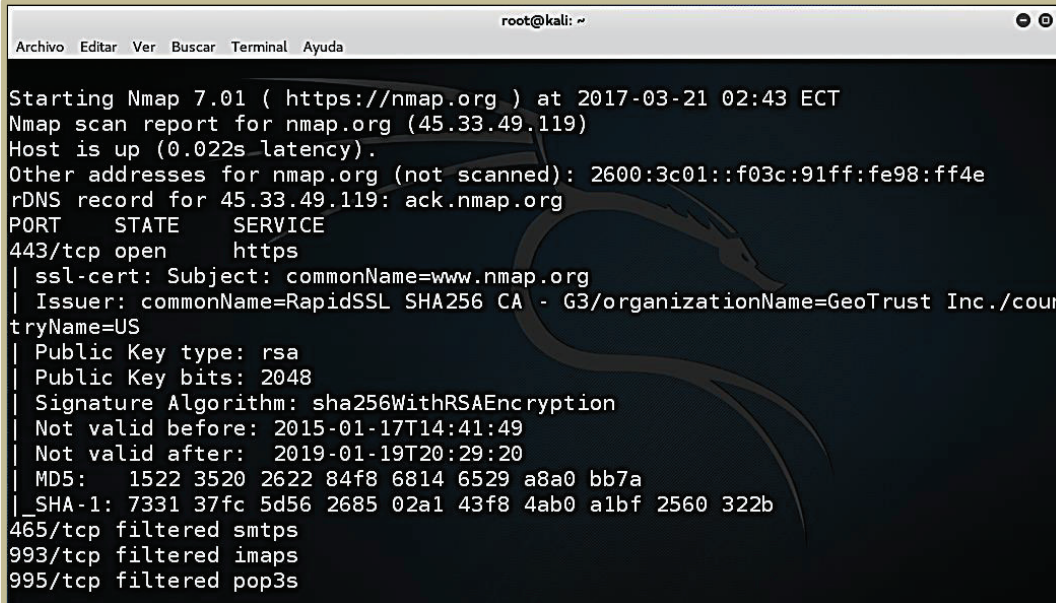
**script ssl-enum-ciphers:** Script para revisar si el servidor acepta o rechaza el cifrado SSL/TLS

**-p 443,465,993,995:** Puertos para el escaneo.

**-oN crypst-001-nmap.txt:** Guardar el resultado en un archivo de texto

El resultado del escaneo proporciona si estos servicios se encuentran activos en el servidor web.

La figura 3.39 muestra el resultado de la prueba utilizando nmap.



```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda

Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-21 02:43 ECT
Nmap scan report for nmap.org (45.33.49.119)
Host is up (0.022s latency).
Other addresses for nmap.org (not scanned): 2600:3c01::f03c:91ff:fe98:ff4e
rDNS record for 45.33.49.119: ack.nmap.org
PORT      STATE      SERVICE
443/tcp   open      https
| ssl-cert: Subject: commonName=www.nmap.org
| Issuer: commonName=RapidSSL SHA256 CA - G3/organizationName=GeoTrust Inc./countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2015-01-17T14:41:49
| Not valid after: 2019-01-19T20:29:20
| MD5: 1522 3520 2622 84f8 6814 6529 a8a0 bb7a
|_SHA-1: 7331 37fc 5d56 2685 02a1 43f8 4ab0 a1bf 2560 322b
465/tcp   filtered  smtps
993/tcp   filtered  imaps
995/tcp   filtered  pop3s

```

Figura 3.39 Verificación SSL/TLS con nmap

La segunda forma de verificar si estos mecanismos están implementados es revisar manualmente el certificado del sitio web. En la parte de detalles técnicos, dentro de la información de la página web se observa si estos mecanismos se encuentran implementados. Utilizando mozilla Firefox se puede acceder a la información de la página de la siguiente manera:

### Menú herramientas – Información de la página – Pestaña seguridad

En la figura 3.40 se presenta información sobre un sitio web que si tiene implementado TLS.

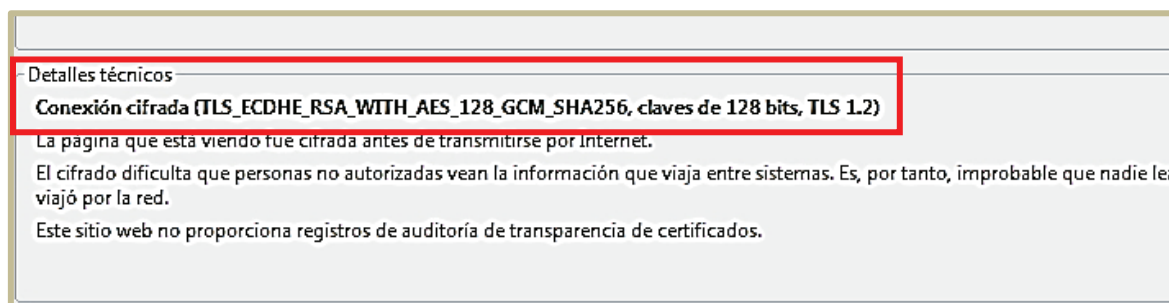


Figura 3.40 Información de seguridad de un sitio web

### 3.7.2. PRUEBA DE INFORMACIÓN SENSIBLE ENVIADA POR CANALES SIN ENCRIPTAR (OTG-CRYPT-003)

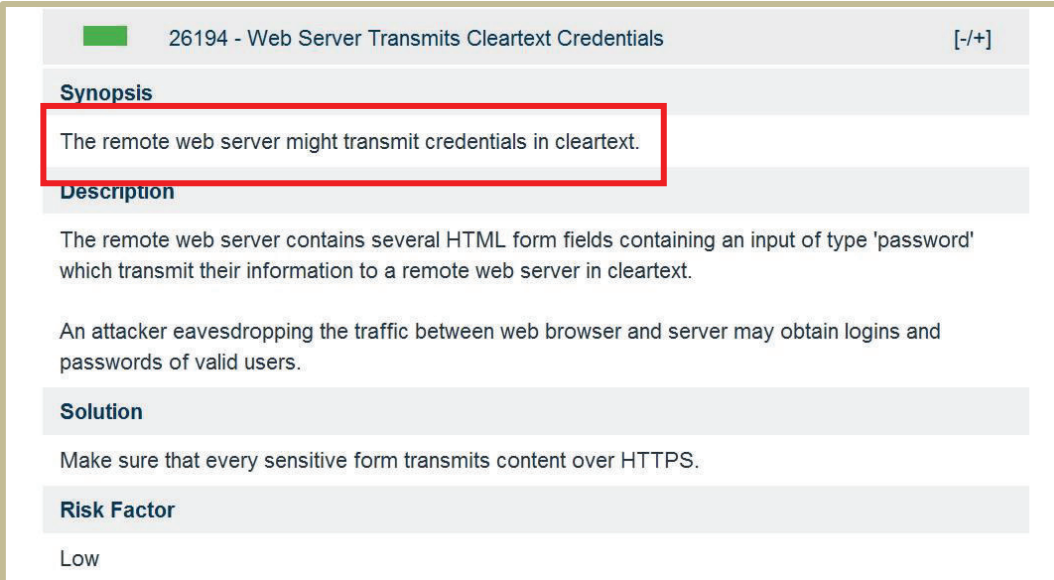
Varios tipos de información deben ser transportados de manera segura y no deben enviarse en texto claro porque tienen un contenido sensible.

El propósito de esta prueba es verificar si información usada para la autenticación, credenciales, cookies se transmiten de forma segura.

Para esta prueba se utiliza 2 herramientas, el escáner de vulnerabilidades Nessus [31], [32] y el *sniffer* Wireshark [1], [14].

En la figura 3.41 se aprecia el resultado del escáner Nessus [31], [32] el cual indica que las credenciales y toda la información que transmite el servidor web, viaja en texto claro.

Para este tipo de análisis se usa Nessus con un perfil de escaneo *Web Application Test*.



The image shows a screenshot of a Nessus scan result. At the top, there is a green bar with the text '26194 - Web Server Transmits Cleartext Credentials' and a '[+/-]' icon. Below this, the 'Synopsis' section is highlighted with a red box and contains the text: 'The remote web server might transmit credentials in cleartext.' The 'Description' section follows, stating: 'The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.' The 'Solution' section says: 'Make sure that every sensitive form transmits content over HTTPS.' The 'Risk Factor' section is labeled 'Low'.

Figura 3.41 Credenciales en texto claro con Nessus [31], [32]

Para visualizar el resultado con la segunda herramienta es necesario hacer una captura de tráfico y analizar sus respectivos campos.

En la gráfica se puede apreciar que existen datos que viajan a través de SSL , por lo que se concluye que la información intercambiada con el servidor web no viaja en texto claro.

La figura 3.42 muestra el análisis de tráfico con la herramienta wireshark.

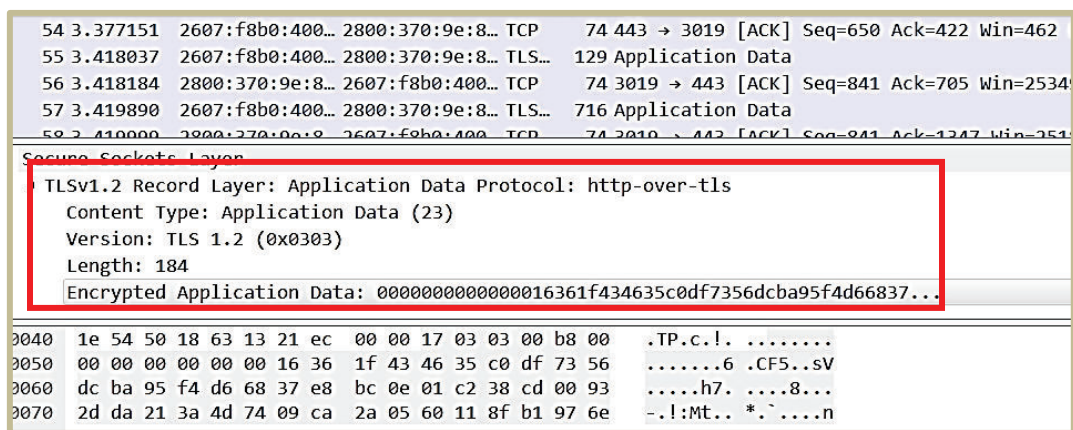


Figura 3.42 Tráfico encriptado visto con wireshark

### 3.8. OBJETIVOS DE LAS PRUEBAS DE SEGURIDAD Y HERRAMIENTAS A UTILIZAR PARA ALCANZAR LOS MISMOS [1]

La tabla 3.1 muestra una lista resumen de pruebas a realizar, con el objetivo de cada prueba de seguridad y las herramientas que se utilizarán para su respectiva implementación.

CATEGORÍA	CODIGO PRUEBA	NOMBRE DE LA PRUEBA	OBJETIVO DE LA PRUEBA	HERRAMIENTAS UTILIZADAS [1]
Recopilación de Información	OTG-INFO-001	Descubrimiento con motores de búsqueda y reconocimiento por fugas de información	Entender qué información de diseño y configuración sensibles de la aplicación u organización se exponen en el Internet	Google [1], [112], mozilla firefox[1]
	OTG-INFO-002	Fingerprint del servidor web	Encuentrar versión y tipo de servidor web en ejecución para determinar las vulnerabilidades conocidas	httprint [1], [92], wappalyzer[103]

CATEGORÍA	CÓDIGO PRUEBA	NOMBRE DE LA PRUEBA	OBJETIVO DE LA PRUEBA	HERRAMIENTAS UTILIZADAS
Recopilación de Información	OTG-INFO-003	Revisión de meta-archivos por fugas de información	Revisar si existe fuga de información de directorios o rutas de la aplicación web. Crear lista de directorios que deben ser evitados por Spiders, Robots o Crawler	wget [1], [96], owasp zap [1], [89]
	OTG-INFO-004	Enumerar aplicaciones en el servidor web	Enumerar las aplicaciones que existen en el servidor web	nmap [1], [35], nessus [31], [32]
	OTG-INFO-005	Revisar comentarios en la página web y metadatos por fugas de información	Revisar comentarios y metadatos de la página web para comprender mejor la aplicación y encontrar fugas de información	mozilla Firefox [1], desenmascara.me [109]
	OTG-INFO-006	Identificar los puntos de entrada de la aplicación	Comprender cómo se forman las solicitudes y las respuestas típicas de la aplicación	burp suite [1], [88]
	OTG-INFO-007	Mapear rutas de ejecución a través de la aplicación	Mapear la aplicación objetivo y comprender su flujo de trabajo	burp suite [1], [88], owasp zap [1], [89]
	OTG-INFO-008	Fingerprint del framework de la aplicación web	Definir el tipo de framework web utilizado para tener una mejor comprensión de la metodología de pruebas de seguridad	whatweb [1], [93]
	OTG-INFO-009	Fingerprint a la aplicación web	Identificar la aplicación web y la versión para determinar las vulnerabilidades conocidas. Identificar el tipo de CMS	builtwith.com [108], whatweb [1], [93]
Gestión de la Configuración y la Implementación	OTG-CONFIG-001	Prueba de configuración de red/infraestructura	Revisar la infraestructura de red para determinar que tan segura se encuentra la aplicación web	N/A
	OTG-CONFIG-002	Prueba de configuración de la plataforma de la aplicación	Revisar si la instalación del servidor web es por defecto. Revisar si el servidor web utiliza uniacamente las funcionalidades necesarias.	N/A



CATEGORÍA	CÓDIGO PRUEBA	NOMBRE DE LA PRUEBA	OBJETIVO DE LA PRUEBA	HERRAMIENTAS UTILIZADAS
Gestión de la Configuración y la Implementación	OTG-CONFIG-004	Archivos de backup y no referenciados con información sensible	Verificar si existen archivos de respaldo con información sensible. Verificar el almacenamiento de los logs	N/A
	OTG-CONFIG-005	Enumerar interfaces de administración de aplicaciones y de infraestructura	Revisar si existen interfaces de administración para usuarios privilegiados.	mozilla firefox [1], owasp zap [1], [89]
	OTG-CONFIG-006	Prueba de métodos HTTP	Determinar si están habilitados metodos HTTP que puedan ser usados para propósitos maliciosos	nmap [1], [35]
	OTG-CONFIG-007	Prueba de seguridad de transporte estricto HTTP - HSTS	Verificar si el mecanismo de seguridad HTTP Strict Transport Security (HSTS) está implementado	curl [1], [95], ssl test server [1], [110]
	OTG-CONFIG-008	Prueba de política de dominio cruzado RIA	Verificar la política de dominio cruado	mozilla firefox [1]
Autorización	OTG-AUTHZ-001	Prueba de directorio/ <i>path traversal</i>	Verificar si se puede acceder a archivos sensibles	dotdotpwn [1], [99], mozilla firefox [1]
	OTG-AUTHZ-003	Prueba de scalamiento de privilegios	Verficar si se puede escalar privilegios o roles, tanto vertical como horizontalmente	N/A
	OTG-AUTHZ-004	Prueba de referencia directa insegura a objetos	Determinar si es posible acceder a recursos modificando parámetros en la URL	mozilla firefox [1]
Gestión de Sesiones	OTG-SESS-005	Prueba de falsificación de peticiones en sitios cruzados CSRF	Verificar si es posible realizar un ataque de CSRF	N/A
Validación de Datos de Entrada	OTG-INPVAL-001	Prueba de <i>Cross Site Scripting</i> reflejado	Verficar si se puede realizar un ataque de XSS	xsser [1], [100], mozilla firefox [1]
	OTG-INPVAL-002	Prueba de <i>Cross Site Scripting</i> almacenado	Verficar si se puede realizar un ataque de XSS almacenado	N/A

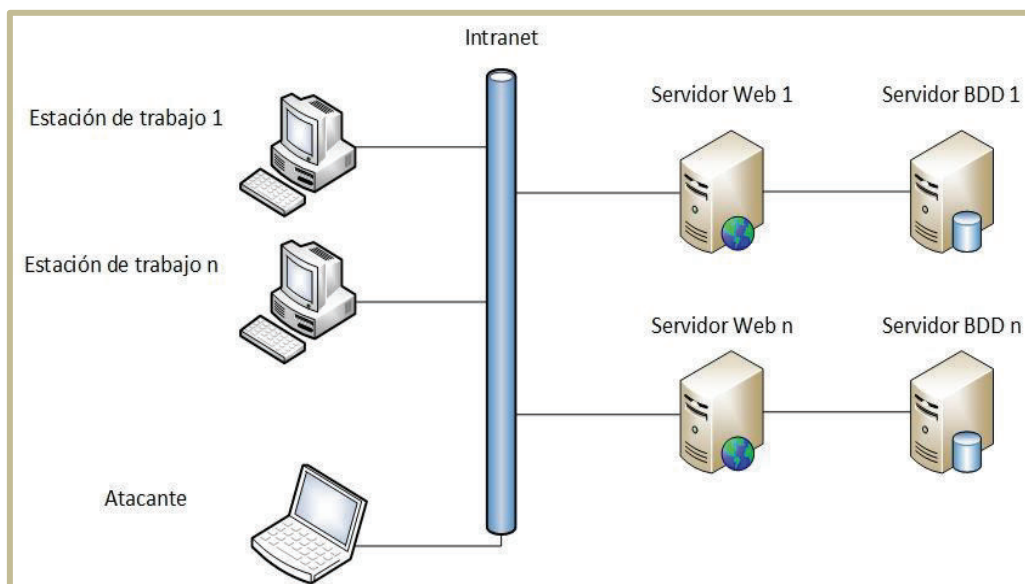
CATEGORÍA	CÓDIGO PRUEBA	NOMBRE DE LA PRUEBA	OBJETIVO DE LA PRUEBA	HERRAMIENTAS UTILIZADAS
Validación de Datos de Entrada	OTG-INPVAL-003	Prueba de manipulación de métodos HTTP	Revisar el resultado de las peticiones con métodos HTTP no comunes	telnet [1], [91]
	OTG-INPVAL-005	Prueba de inyección SQL	Revisar si es posible realizar inyección SQL	mozilla firefox [1], sqlmap [1] [47]
	OTG-INPVAL-012	Prueba de inclusión local de archivos	Verificar si se puede incluir archivos que están presentes en el servidor web	dotdotpwn [1], [99], mozilla firefox [1]
	OTG-INPVAL-013	Prueba de inyección de comandos	Revisar si es posible la inyección de comandos	commix [1], [111]
Manejo de Errores	OTG-ERR-001	Análisis de códigos de error	Determinar si los mensajes de error en las páginas web revelan información	telnet [1], [91], mozilla firefox [1]
Criptografía	OTG-CRYPST-001	Prueba de cifrado ssl/tls débil y protección insuficiente de capa de transporte	Revisar la fortaleza de los protocolos SSL/TLS	sslyze [1], [97], ssl test server [1][110]
	OTG-CRYPST-003	Prueba de información sensible enviada por canales sin encriptar	Verificar si la información viaja en canales sin encriptar	nessus [31], [32], wireshark [1], [14]

**Tabla 3.1 Objetivos y herramientas utilizadas**

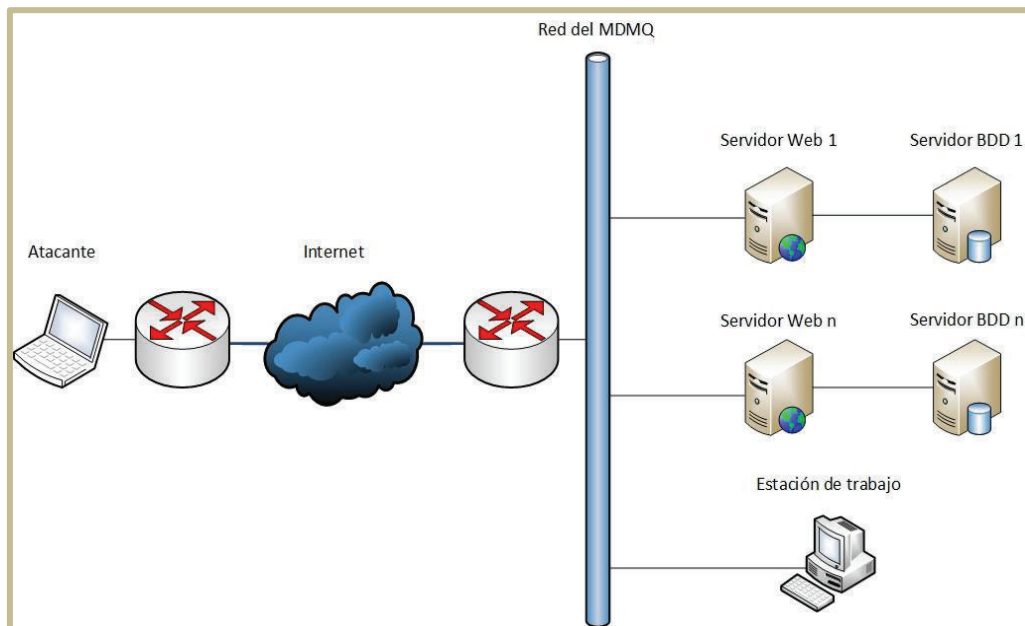
### 3.9. DISEÑO DEL AMBIENTE DE PRUEBAS

A continuación, se detalla el hardware y software que se utilizará para el ambiente de pruebas de penetración. En la figura 3.42 se muestra el diagrama de red, de cómo se realizarán las pruebas de seguridad desde la red de la organización.

La figura 3.43 muestra el esquema de red utilizado para realizar las pruebas desde fuera de la organización, específicamente las pruebas de la sección 3.1.1, concernientes a búsqueda de información con motores de búsqueda.



**Figura 3.42 Esquema de las pruebas de penetración desde dentro de la organización**



**Figura 3.42 Esquema de pruebas desde fuera de la organización**

Las especificaciones de hardware y software son únicamente del atacante ya que los servidores objetivos de las pruebas de seguridad son los servidores reales que alojan los portales o aplicaciones web que presta el MDMQ. La tabla 3.2 muestra los detalles de software y hardware utilizado para el ambiente de pruebas.

PRUEBAS DE HACKING ETICO - EQUIPOS			
#	TIPO	DESCRIPCIÓN	
		HARDWARE	SOFTWARE
1	Computador portátil	<b>Procesador:</b> Intel Core i5-2410M <b>RAM:</b> 2 DIMM hasta 8 GB (2 x 4 GB) <b>Tarjeta Gráfica:</b> Intel HD 3000 <b>Pantalla:</b> HD de 14,0 pulgadas <b>Disco Duro:</b> 750 GB (7200 RPM) <b>Unidad Óptica:</b> DVD+/RW <b>Tarjeta de red:</b> Intel Centrino Wireless-N 1030 <b>Tarjeta de red:</b> Atheros PCI-E Fast Ethernet <b>Bluetooth:</b> 3.0 +HS estándar	<b>Sistema Operativo</b> Kali Rolling 2016.2

Tabla 3.2 Descripción de hardware y software del equipo atacante

## **CAPÍTULO 4**

### **RESULTADOS**

En este capítulo se documentan y analizan los resultados de las pruebas de seguridad que se realizaron en las aplicaciones web, basadas en la Guía de Pruebas OWASP 4.0 [1].

En las secciones 4.1 y 4.2 se demuestran los resultados de la pruebas de penetración en el Portal del MDMQ y en el Sitio de Pago de Impuestos por Internet respectivamente.

A continuación en las secciones 4.3 y 4.4 se presenta el análisis de resultados para ambos objetivos de estudio.

Por cuestiones de seguridad algunos datos van a ser anonimizados. Por ejemplo, las direcciones IP y las URLs.

#### **4.1. RESULTADO DE PRUEBAS PARA EL PORTAL WEB DEL MDMQ**

En esta sección se muestran los resultados de haber aplicado la prueba de penetración basada en la Guía OWASP, para el portal web del MDMQ.

##### **4.1.1. RESULTADO DE PRUEBAS: RECOPIACIÓN DE INFORMACIÓN**

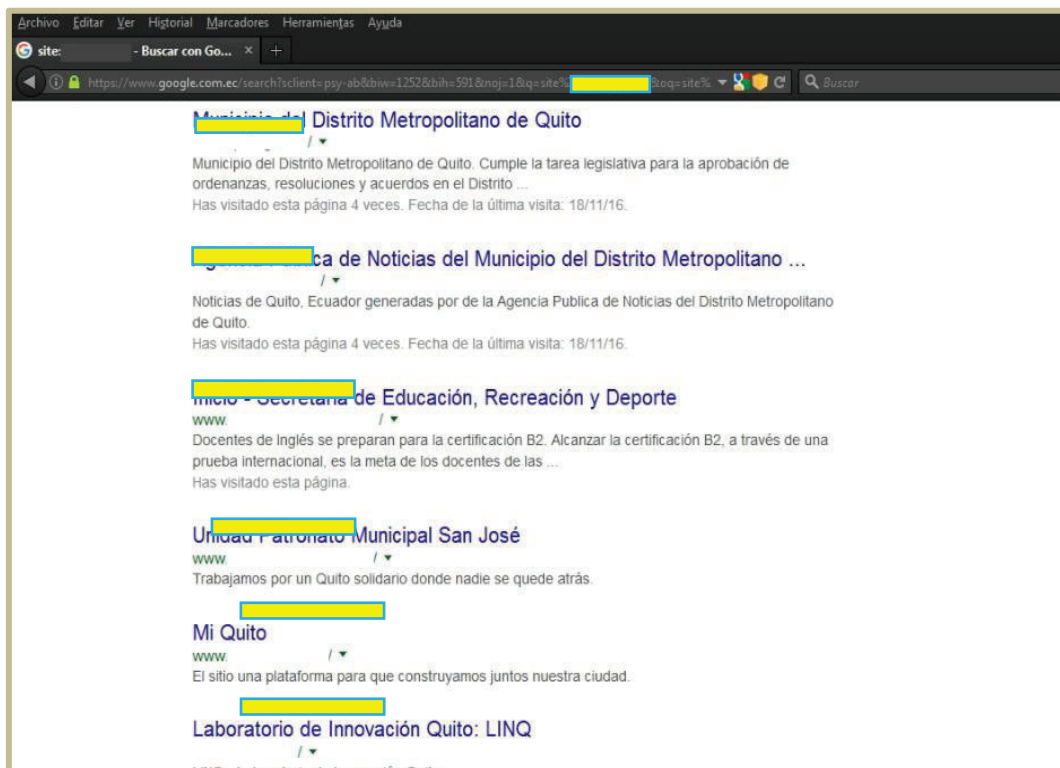
###### **4.1.1.1. Descubrimiento con motores de búsqueda y reconocimiento por fugas de información (OTG-INFO-001)**

Para esta prueba se utilizó búsquedas avanzadas con el motor de búsqueda Google, con el fin de encontrar información que ha sido publicada sin querer y que contenga datos sensibles.

- Búsqueda de Subdominios:

En la figura 4.1 se aprecia el resultado de buscar subdominios del objetivo. Para eso se utilizó la siguiente búsqueda avanzada:

**site:** ejemplo.com



**Figura 4.1 Búsqueda de subdominios**

Resultados de la búsqueda:

Se encontró subdominios del objetivo principal, estos pueden ser vulnerables o mal configurados.

- Búsqueda de interfaces de administración

En las figuras 4.2, 4.3 y 4.4 se muestra el resultado de la búsqueda de una interfaz de administración, para Joomla, WordPress y Drupal respectivamente.

Resultado de la primera búsqueda:

Figura 4.2 interfaz de administración para Joomla encontrada.

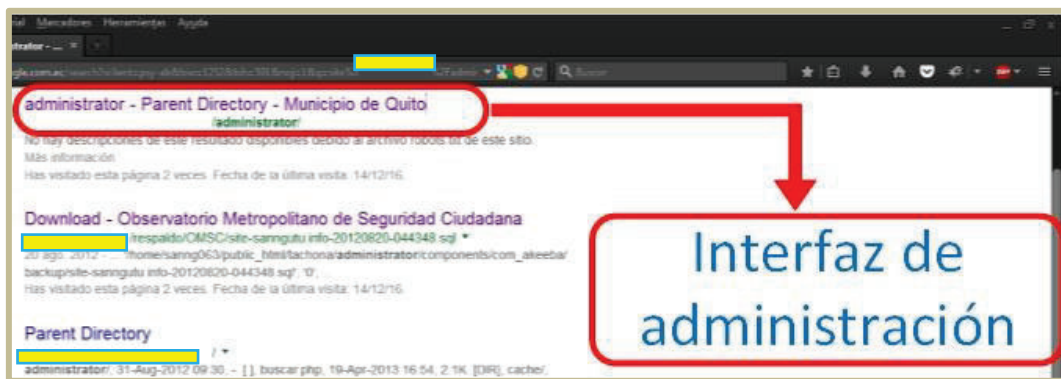


Figura 4.2 Búsqueda de interfaz de administración Joomla

Figura 4.3 búsqueda de interfaz de administración para Wordpress.

Resultado de la segunda búsqueda: La consulta no produjo resultados.

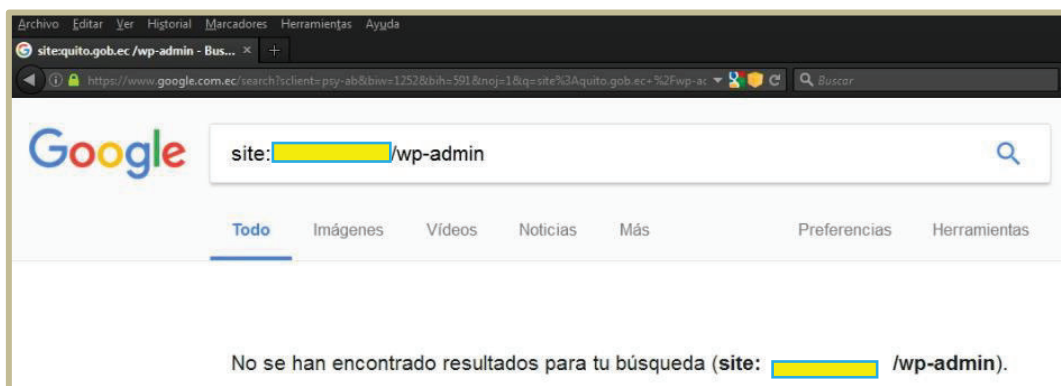


Figura 4.3 Búsqueda de interfaz de administración Wordpress

Figura 4.4 búsqueda de interfaz de administración para Drupal.

Resultado de la tercera búsqueda: La consulta no produjo resultados del objetivo.



Figura 4.4 Búsqueda de interfaz de administración Drupal

- Búsqueda de páginas con parámetros susceptibles a XSS o SQLi.

En la figura 4.5 se muestra el resultado para buscar páginas susceptibles a XSS e inyección SQL dentro del dominio.



**Figura 4.5 Búsqueda de páginas propensas a XSS e inyección SQL**

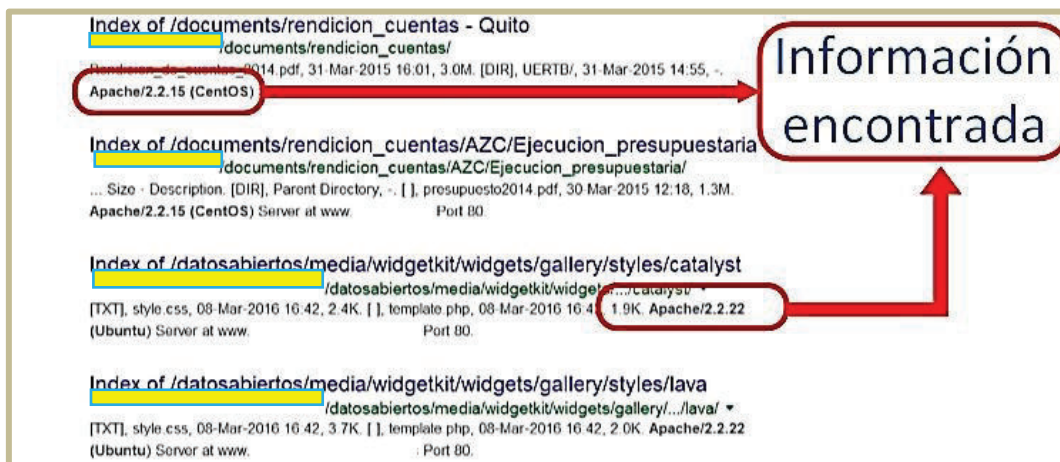
Resultados de la búsqueda: Se encontraron páginas dentro el objetivo con parámetros en la URL del tipo (**php?id=**) los cuales pueden ser vectores de ataque de XSS o inyección SQL.

- Búsqueda de tipo y versión de servidor web.

La figura 4.6 muestra el resultado de búsqueda de versión y tipo de servidor web.

Información obtenida:

- Versión y tipo de servidor web: Apache 2.2.15, Apache 2.2.22
- Sistema Operativo: CentOS, Ubuntu



**Figura 4.6 Búsqueda de la versión y tipo de Servidor Web**



#### 4.1.1.2. Fingerprint del servidor web (OTG-INFO-002)

En la figura 4.7 se observa el resultado de la prueba con httprint.

Entre la información encontrada considerada más relevante, se tiene la siguiente:

- Tipo de servidor web: Apache
- Versión del servidor web: 2.4.6
- Sistema operativo: *Red Hat Enterprise Linux* (RHEL)

```

root@kali:~# httprint -h http://[redacted] -s /usr/share/httprint/signatures.txt
httprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httprint/
httprint@net-square.com

Finger Printing on http://[redacted]
Finger Printing Completed on http://[redacted]
-----
Host: [redacted]
Derived Signature:
Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16
811C9DC56ED3C295811C9DC5811C9DC5811C9DC5505FCFE84276E4BB811C9DC5
0D7645B5811C9DC5811C9DC5CD37187C811C9DC5811C9DC5811C9DC5811C9DC5
6ED3C2956ED3C2956ED3C295811C9DC5E2CE6927811C9DC56ED3C295811C9DC5
6ED3C2956ED3C2952A200B4C6ED3C2956ED3C2956ED3C295E2CE6923
E2CE6923811C9DC57A40A2E4E2CE6927E2CE6923

Banner Reported: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16
Banner Deduced: Apache/2.0.x
Score: 90
Confidence: 54.22
-----

```

Figura 4.7 Fingerprint del servidor web con httprint

En la figura 4.8 se obtiene el mismo resultado que el comando httprint, pero esta vez utilizando la herramienta web para fingerprint gregthatcher.com.

Find out which Web Server Software a website is running

Enter the domain name of the website.

http:// [redacted]

Submit

says it is running: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16

Page Title: Municipio del Distrito Metropolitano de Quito

Additionally, it mentioned the following:

Pragma : no-cache;  
 Connection : close;  
 Transfer-Encoding : chunked;  
 Cache-Control : no-cache;  
 Content-Type : text/html;  
 charset=utf-8;  
 Date : Fri, 21 Oct 2016 14:28:57 GMT;  
 P3P : CP="NOI ADM DEV PSAI COM NAV OUR OTRo STP IND DEM";  
 Set-Cookie : 136b65862bda7837e1c7dfad8247bd04=mqg0oI2(truncated);  
 X-Powered-By : PHP/5.4.16

Figura 4.8 Fingerprint del servidor web con gregthatcher.com

#### 4.1.1.3. Revisión de meta-archivos por fugas de información (OTG-INFO-003)

En esta se hacen uso de las herramienta wget y un navegador web, con el propósito de encontrar archivos que contengan información relevante para un ataque.

La información más importante encontrada en esta prueba es la siguiente:

- CMS: Joomla.
- Dirección IP pública del servidor web.
- Interfaz de administración
- Meta-archivos
- Directorios excluidos para indexar por motores de búsqueda
- Protocolo de exclusión robots.txt

En la figura 4.9 muestra la forma de descargar el archivo robots.txt con el comando wget y luego se visualiza su contenido con el comando tail.

```

root@kali:~# wget http://[redacted]/robots.txt
--2017-03-20 18:55:04-- http://[redacted]/robots.txt
Resolviendo [redacted] ([redacted])...
Conectando con [redacted] ([redacted])[redacted]:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 865 [text/plain]
Grabando a: "robots.txt.1"

robots.txt.1 100%[=====>] 865 --.-KB/s in 0s

2017-03-20 18:55:15 (32.8 MB/s) - "robots.txt.1" guardado [865/865]

root@kali:~# tail -n20 robots.txt
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Disallow: /administrator/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /images/

```

Figura 4.9 Descarga y visualización de robots.txt con wget y tail respectivamente

En la figura 4.10 se aprecia el mismo resultado de la prueba anterior, pero esta vez utilizando el navegador web.

```
# http://www.sxw.org.uk/computing/robots/check.html
User-agent: *
Disallow: /administrator/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /images/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /libraries/
Disallow: /logs/
Disallow: /media/
Disallow: /modules/
Disallow: /plugins/
Disallow: /templates/
```

Figura 4.10 Visualización de robots.txt con el navegador web

#### 4.1.1.4. Enumerar aplicaciones en el servidor web (OTG-INFO-004)

La figura 4.11 muestra los resultados de la prueba con ayuda del comando nmap. Entre la información más importante se tiene la siguiente:

- Puertos descubiertos: 20, 21, 22, 80, 443, 2000, 3306, 6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 6009, 6025, 6059.
- Puertos abiertos: 21, 80, 2000, 3306.
- Puertos cerrados: 20, 22, 443, 6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 6009, 6025, 6059.
- Sistema operativo: Unix (RHEL).
- Servicios y su versión.

```
Not shown: 982 filtered ports
PORT      STATE SERVICE      VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp          vsftpd 3.0.2
22/tcp    closed ssh
80/tcp    open  http         Apache httpd 2.4.6 ((Red Hat Enterprise Linux) PHP/5.4.16)
443/tcp   closed https
2000/tcp  open  cisco-scp?
3306/tcp  open  mysql        MySQL 5.5.44-MariaDB
6000/tcp  closed X11
6001/tcp  closed X11:1
6002/tcp  closed X11:2
6003/tcp  closed X11:3
6004/tcp  closed X11:4
6005/tcp  closed X11:5
6006/tcp  closed X11:6
6007/tcp  closed X11:7
6009/tcp  closed X11:9
6025/tcp  closed x11
6059/tcp  closed X11:59
Service Info: OS: Unix
```

Figura 4.11 Enumerando aplicaciones con nmap [1], [35]

#### 4.1.1.5. Revisar comentarios en la página web y metadatos por fugas de información (OTG-INFO-005)

Para esta prueba se utiliza la herramienta en línea desenmascara.me para revisar los metadatos de la página web y para encontrar comentarios se visualiza el código fuente de la página web con la ayuda del navegador. La figura 4.12 muestra el resultado de la prueba con la ayuda de la herramienta en línea desenmascara.me.

Resultados obtenidos:

- CMS: Joomla
- Fingerprint del framework de la aplicación: PHP/5.4.16
- Dirección IP pública del servidor web

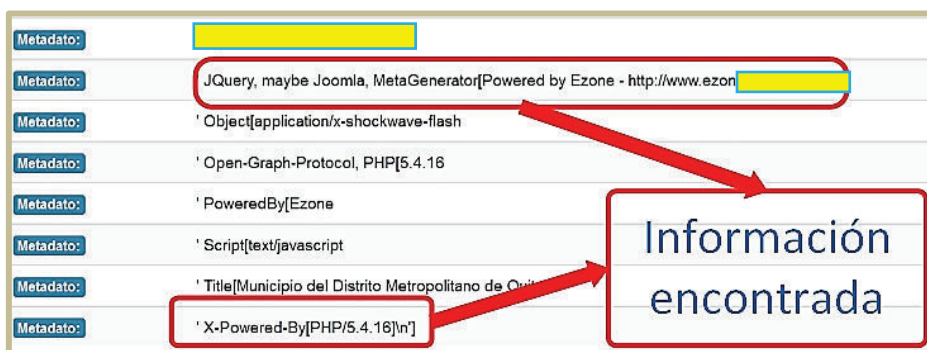


Figura 4.12 Metadatos con desenmascara.me

En la figura 4.13 se observa el código fuente de la página en búsqueda de comentarios que revelen información. Resultados obtenidos: No se encuentran comentarios con información importante en el código de la página web.

```

<div id="menu" class="clear">
  <div class="moduletable m_menu">
<!--[if lte IE 7]>
<link href="/modules/mod_maximenuck/themes/css3megamenu/css/ie7.css" rel="stylesheet
<![endif]--><!-- debut Maximenu CK, par cedric keiflin -->
<div class="maximenuckh" id="mainmenu" style="z-index:10;">
  <div class="maxiroundedleft"></div>
<div class="maxiroundedcenter">
  <ul class="menu m_menu maximenuck" style="">
    <li class="maximenuck item101 current active first levell " :
</li><li class="maximenuck item109 parent levell " style="z-index : 11999;"><a class:

```

Figura 4.13 Revisión de comentarios en el código fuente de la página web

#### 4.1.1.6. Identificar los puntos de entrada de la aplicación (OTG-INFO-006)

En la figura 4.14 se muestra la estructura de una solicitud con el método GET.

La información que se encontró es la siguiente: Cookie: `_ga`

```
GET / HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: _ga=GA1.3.420818313.1480606043
```

Figura 4.14 Solicitud con el método GET

#### 4.1.1.7. Mapear rutas de ejecución a través de la aplicación (OTG-INFO-007)

Entre la información más importante encontrada durante esta prueba se tiene lo siguiente:

- Directorio *Administrator*.
- Con Burp Suite se visualiza el archivo `robots.txt`.

La figura 4.15 muestra el resultado del *spidering* con la herramienta Burp Suite.

The screenshot shows the Burp Suite interface during a spidering operation. On the left, a directory tree is visible with several folders and files. Two items are highlighted with red circles and red arrows pointing to callouts: 'administrator' (pointing to a callout labeled 'Directorio Administrator') and 'robots.txt' (pointing to a callout labeled 'Archivo robots.txt'). On the right, the 'Raw' tab of the 'robots.txt' file is displayed, showing a list of disallowed paths (Disallow) such as /administrator/, /cache/, /cli/, /components/, /images/, /includes/, /installation/, /language/, /libraries/, /logs/, /media/, /modules/, /plugins/, /templates/, and /tmp/.

Figura 4.15 Spidering con Burp Suite[1]

En la figura 4.16 se observar un resultado similar, realizado esta vez con ZAP de OWASP.

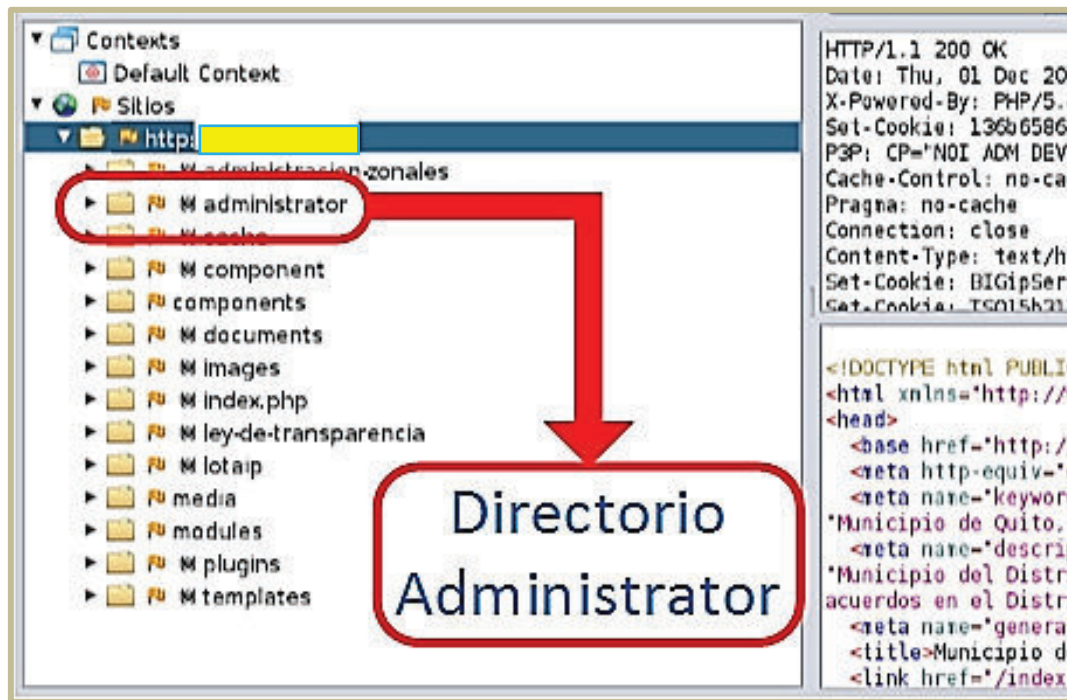


Figura 4.16 Spidering con ZAP[1]

#### 4.1.1.8. Fingerprint el framework de la aplicación web (OTG-INFO-008)

Conocer el *framework* de una aplicación es una forma de fuga de información, con esto se podría buscar en Internet vulnerabilidades conocidas.

En la información encontrada con esta prueba se tiene:

- X-Powered-By: PHP/5.4.16
- Sistema operativo: RHEL
- CMS: Joomla
- *Framework* Javascript
- *Cookies*
- Tipo y versión de servidor web: Apache 2.4.6

En la figura 4.17 se aprecia el resultado de esta prueba utilizando la herramienta whatweb.

```

root@kali:~# whatweb http://[redacted]
http://[redacted] [200 OK] Adobe-Flash, Apache[2.4.6], Cookies[136b65862bda7837e1c7dfad8247bd04],
ntry[RESERVED][ZZ], Email[serviciosciudadanos@quito.gob.ec], Google-API[ajax/libs/jquery/1.8/jquery
.js,ajax/libs/jqueryui/1.8/jquery], Google-Analytics[UniversalUA-58165136-1], HTTPServer[Red Hat
x][Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16], IP[redacted], JQuery, maybe Joomla, Met
erator[Powered by Ezone - http://www.ezone.com.ec], Object[application/x-shockwave-flash], Open-Gra
rotocol, OpenSearch[http://[redacted]/index.php/component/search/?format=opensearch], PHP[5.4.16]
weredBy[Ezone], Script[text/javascript], Title[Municipio del Distrito Metropolitano de Quito], Unco
Headers[x-content-encoded-by], X-Powered-By[PHP/5.4.16]
root@kali:~#

```




Figura 4.17 Fingerprint del framework de la aplicación

#### 4.1.1.9. Fingerprint a la aplicación web (OTG-INFO-009)

Otra de las variables importantes para la búsqueda de vulnerabilidades conocidas es el gestor de contenido (CMS), para ello se utiliza el plugin Wappalyzer de Firefox y la herramienta whatweb.

Entre la información la información más relevante se tiene:

- CMS: Joomla 2.5
- *Framework* de la aplicación: PHP/5.4.16
- Sistema operativo: RHEL
- Tipo y versión del servidor web: Apache 2.4.6

En la figura 4.18 se muestra el resultado con Firebug de Firefox.



Figura 4.18 Fingerprint a la aplicación web con wappalyzer

La figura 4.19 demuestra que se obtuvo la misma información con la herramienta whatweb.

```

root@kali:~# whatweb http:// [redacted]
http:// [redacted] [200 OK] Adobe-Flash, Apache[2.4.6], Cookies[136b65862bda7837e1c7dfad8247bd04],
ntry[RESERVED][ZZ], Email[serviciosciudadanos@quito.gob.ec], Google-API[ajax/libs/jquery/1.8/jquery
.js,ajax/libs/jqueryui/1.8/jquery], Google-Analytics[Universal][UA-58105136-1], HTTPServer[Red Hat
x][Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16], IP[ [redacted] ], JQuery, maybe Joomla, Met
erator[Powered by Ezone - http://www.ezone.com.ec], Object[application/x-shockwave-flash], Open-Gra
rotocol, OpenSearch[http:// [redacted] /index.php/component/search/?format=opensearch], PHP[5.4.16]
weredBy[Ezone], Script[text/javascript], Title[Municipio del Distrito Metropolitano de Quito], Unco
Headers[x-content-encoded-by], X-Powered-By[PHP/5.4.16]
root@kali:~# █

```

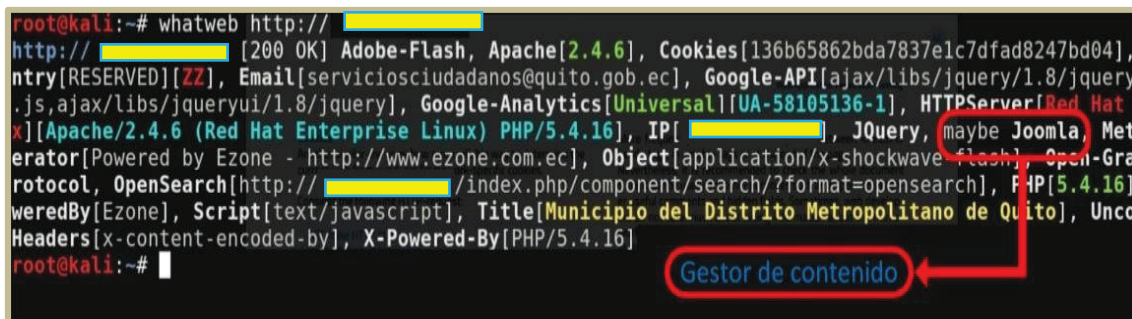


Figura 4.19 Fingerprint a la aplicación web con whatweb

## 4.1.2. RESULTADO DE PRUEBAS: GESTIÓN DE LA CONFIGURACIÓN Y LA IMPLEMENTACIÓN

### 4.1.2.1. Prueba de configuración de red/infraestructura (OTG-CONFIG-001)

Por cuestiones del compromiso de confidencialidad y disponibilidad de información no se tuvo acceso a un diagrama de red detallado.

Por este motivo no se puede hacer un análisis más detallado sobre la infraestructura de seguridad que soporta a la aplicación web.

En la figura 4.20 se puede distinguir lo siguiente:

**CLOUD:** Servicio de almacenamiento y aplicaciones en la nube, por ejemplo trabajo colaborativo y servicios al cliente.

**RTM:** Red de transporte interna que sirve de comunicación entre dependencias del MDQM que se encuentran ubicadas en el Centro Histórico de Quito.

**ENLACE DE DATOS:** Enlaces de datos de tipo WAN para comunicarse con las dependencias que se encuentran geográficamente alejadas, por ejemplo las Administraciones Zonales.

**INTERNET:** Enlace de salida al Internet.



En la figura 4.20 se aprecia un diagrama de red general sobre la infraestructura de red del MDMQ, obtenido del departamento de Redes y Telecomunicaciones del MDMQ.

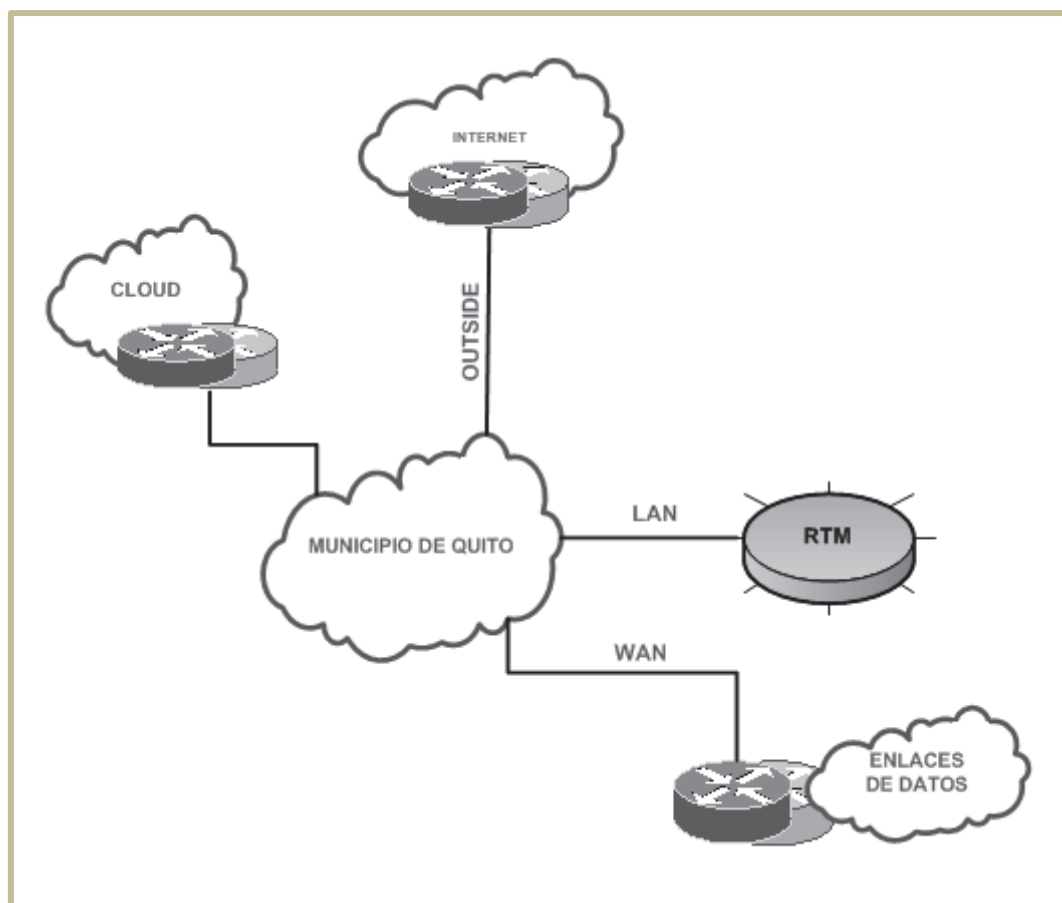


Figura 4.20 Diagrama de red<sup>54</sup>

#### 4.1.2.2. Prueba de configuración de la plataforma de la aplicación (OTG-CONFIG-002)

En la tabla 4.1 se listan ciertos módulos que han sido configurados en el servidor web para el funcionamiento de la aplicación web.

Módulo	Tipo
core_module	Static

<sup>54</sup> Diseño general de la red de datos del MDMQ. (Fuente: Dirección Metropolitana de Informática, Departamento de Redes y Telecomunicaciones)

<b>Módulo</b>	<b>Tipo</b>
so_module	Static
http_module	Static
alias_module	Shared
allowmethods_module	Shared
auth_basic_module	Shared
auth_digest_module	Shared
authn_anon_module	Shared
authz_host_module	Shared
authz_owner_module	Shared
authz_user_module	Shared
autoindex_module	Shared
cache_module	Shared
expires_module	Shared
ext_filter_module	Shared
headers_module	Shared
include_module	Shared
log_config_module	Shared
logio_module	Shared
negotiation_module	Shared
remoteip_module	Shared
status_module	Shared
unixd_module	Shared
userdir_module	Shared
version_module	Shared
vhost_alias_module	Shared
proxy_module	Shared
proxy_ajp_module	Shared
proxy_balancer_module	Shared
proxy_connect_module	Shared
proxy_ftp_module	Shared
proxy_http_module	Shared
proxy_scgi_module	Shared
systemd_module	Shared
cgi_module	Shared
php5_module	Shared

**Tabla 4.1 Módulos del servidor web**

#### 4.1.2.3. Archivos de backup y no referenciados con información sensible (OTG-CONFIG-004)

Por cuestiones de seguridad la única información que se proporcionó por parte del Departamento de Producción de la DMI sobre los registros del sistema es la ubicación dónde estos se encuentran guardados, si es el lugar por defecto o si es en otra ubicación.

La persona encargada de la administración de servidores UNIX y Windows Server aseguró que los registros se guardan en un destino personalizado dentro del servidor web.

#### 4.1.2.4. Enumerar interfaces de administración de aplicaciones y de infraestructura (OTG-CONFIG-005)

Las interfaces de administración proporcionan una entrada con muchos privilegios para poder modificar el sitio web o la aplicación, actividades que no pueden hacer usuarios normales o estándar.

La información más relevante de esta prueba es la siguiente:

- Interfaz de administración de un sitio basado en Joomla

En la figura 4.21 se muestra la interfaz de administración mediante el navegador web.



Figura 4.21 Interfaz de administración Joomla

#### 4.1.2.5. Prueba de métodos HTTP (OTG-CONFIG-006)

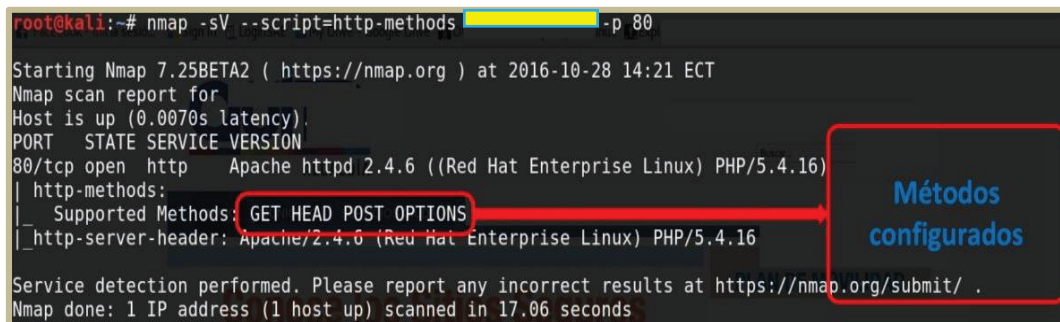
Los métodos definen acciones que se hacen sobre un recurso determinado, y solo ciertos métodos están configurados en los servidores web.

Para identificar los métodos configurados se utiliza la herramienta nmap con un script.

La información encontrada en la presente prueba es la siguiente:

- Métodos HTTP configurados: GET, HEAD, POST, OPTIONS
- Sistema operativo: RHEL
- Estado de los servicios
- Versión y tipo de servidor web: Apache 2.4.6
- *Framework* de la aplicación: PHP/5.4.16

En la figura 4.22 se muestra el resultado de la prueba para identificar los métodos configurados en el servidor web.



```

root@kali:~# nmap -sV --script=http-methods [redacted] -p 80
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-10-28 14:21 ECT
Nmap scan report for [redacted]
Host is up (0.0070s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.6 ((Red Hat Enterprise Linux) PHP/5.4.16)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.06 seconds
  
```

Figura 4.22 Métodos configurados en el servidor web

#### 4.1.2.6. Prueba de seguridad de transporte estricto HTTP - HSTS (OTG-CONFIG-007)

El uso de HSTS es una medida de seguridad, la cual indica al navegador web realice una comunicación con el servidor web utilizando una conexión HTTP segura.

En la figura 4.23 se observa el resultado obtenido con la herramienta curl, al tratar de verificar si este mecanismo de seguridad ha sido implementado.

Resultado de la prueba: como el comando *grep* no encontró coincidencias dentro de la cabecera HTTP, este no muestra nada en pantalla, esto quiere decir que el sistema HSTS no está implementado.

```

root@kali:~# curl -s -D- http://[redacted] | grep Strict
root@kali:~#
  
```

Figura 4.23 Implementación de HSTS

Otra manera de verificar el uso de este mecanismo es con el reporte en línea que genera *SSL Server Test* [1]. En la figura 4.24 se muestra información sobre la no implementación de HSTS en el servidor web.

Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
<b>Strict Transport Security (HSTS)</b>	<b>No</b>
HSTS Preloading	Not in: Chrome Edge Firefox IE

Figura 4.24 Resultado de SSL Server Test

#### 4.1.2.7. Prueba de política de dominio cruzado RIA (OTG-CONFIG-008)

En la figura 4.25 se observa el resultado de la prueba, para esto se usa un navegador web de. Los resultados son los siguientes:

- *allow-access-from* domain: \*, esto quiere decir que se puede acceder al contenido desde cualquier dominio.

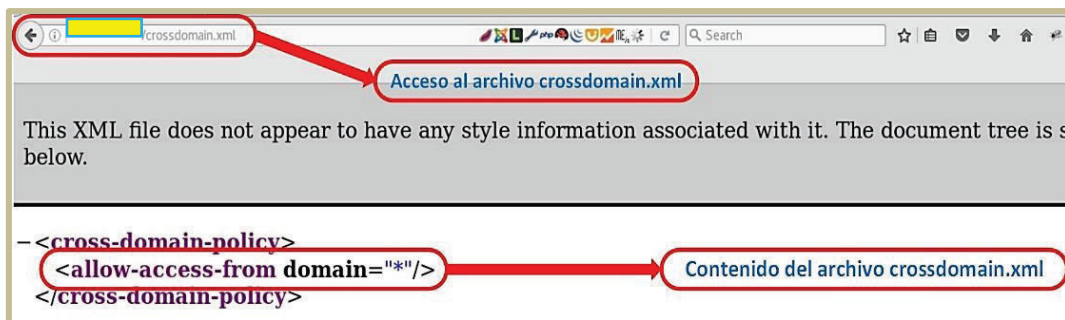


Figura 4.25 Archivo crossdomain.xml

### 4.1.3. RESULTADO DE PRUEBAS: AUTORIZACIÓN

#### 4.1.3.1. Prueba de directorio/path traversal (OTG-AUTHZ-001)

Resultados obtenidos: En la figura 4.26 se observa que la herramienta dotdotpwn ha determinado que la página web es vulnerable al ataque de *path traversal*.

En la figura 4.26 se presenta el resultado de la prueba realizada de forma automatizada.

```

/./allvideoshare/video/0?Itemid=TRAVERSAL:80/./etc/passwd <- VULNERABLE!
/./allvideoshare/video/0?Itemid=TRAVERSAL:80/./../etc/passwd <- VULNERABLE!
/./allvideoshare/video/0?Itemid=TRAVERSAL:80/./../..etc/passwd <- VULNERABLE!
/./allvideoshare/video/0?Itemid=TRAVERSAL:80/./../..../etc/passwd <- VULNERABLE!
/./allvideoshare/video/0?Itemid=TRAVERSAL:80/./../..../..etc/passwd <- VULNERABLE!
/./allvideoshare/video/0?Itemid=TRAVERSAL:80/./../..../..../etc/passwd <- VULNERABLE!
/./allvideoshare/video/0?Itemid=TRAVERSAL:80/./../..../..../..etc/passwd <- VULNERABLE!
/index.php/component/allvideoshare/video/0?Itemid=TRAVERSAL:80/..%5Cetc%5Cpasswd <- VULNERABLE!

```

Figura 4.26 Directorio traversal con dotdotpwn

A continuación se realiza la prueba de manera manual, utilizando un navegador web.

Resultados obtenidos: La prueba no obtuvo resultados.

La figura 4.27 muestra el resultado de la prueba de manera manual.

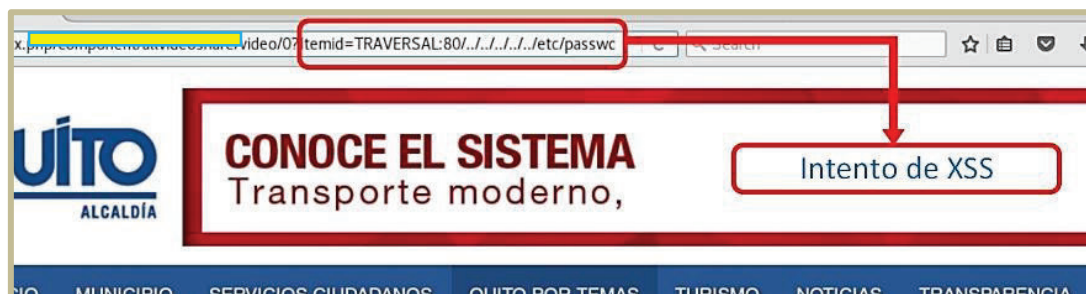


Figura 4.27 Directorio traversal de forma manual

#### 4.1.3.2. Prueba de escalamiento de privilegios (OTG-AUTHZ-003)

No se pudo aplicar esta prueba, ya que no existe ningún formulario de registro o login, ni parámetros que se puedan alterar para poder obtener privilegios de nivel superior.

#### 4.1.3.3. Prueba de referencia directa insegura a objetos (OTG-AUTHZ-004)

En la figura 4.28 muestra una página web con parámetro id (id original 118), el cual va a ser modificado para observar si se puede obtener un archivo diferente. En la figura 4.29 se presenta el resultado cuando se cambia el parámetro id (id nuevo 133) por uno diferente.

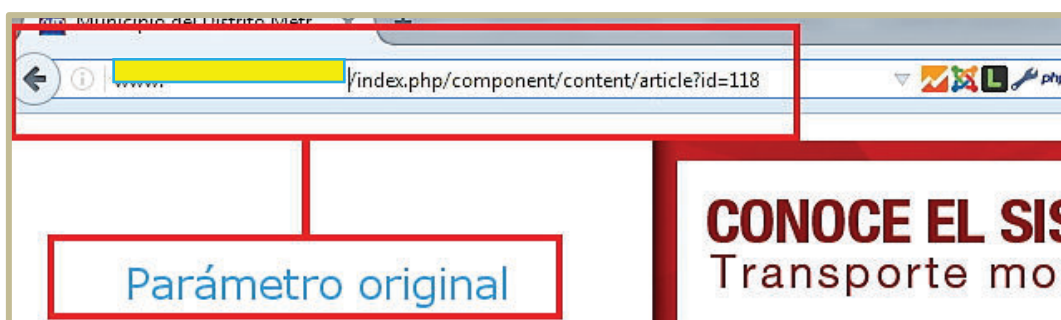


Figura 4.28 Página sin cambio de parámetro id



Figura 4.29 Página con el parámetro id modificado

Resultado obtenido: Como resultado se obtuvo mensaje de error que la página solicitada no existe, no se puede acceder a funcionalidades ni privilegios especiales al modificar el parámetro de la URL.

#### 4.1.4. RESULTADO DE PRUEBAS: GESTIÓN DE SESIONES

##### 4.1.4.1. Prueba de falsificación de peticiones en sitios cruzados - CSRF (OTG-SESS-005)

Esta prueba no se aplica a este servidor web, ya que para realizarla es necesario un sistema de autenticación, y en este mecanismo no está implementado ya que solo es un portal de información estática informativa.

#### 4.1.5. RESULTADO DE PRUEBAS: VALIDACIÓN DE ENTRADA

##### 4.1.5.1. Prueba de Cross Site Scripting reflejado (OTG-INPVAL-001)

La figura 4.30 muestra los resultados de la prueba de manera automatizada.

Resultado obtenido:

La herramienta ha probado todas las variantes para realizar ataques de XSS, dando como resultado únicamente fallos.

```

Vulnerables Failed Errors Crawling
/component/content/article?id="/">
/component/content/article?id="/">626930c93fb7098d48b0339fc6c4e123
/component/content/article?id="/<BODY onload!#$%&()*~+-_.,:;?@[/\|`^`=e46669d1b4541b339d9d99689687ad19
/component/content/article?id="/</TITLE>89ffa340ccd75409a160a89cb32f8e41
/component/content/article?id="/;!--"<5d5567f58416d314c643c4e8d152b784>=&{()}"
/component/content/article?id="/<IMG SRC=c7b6d9182b7d3125f3e02d8f7ffc7ae7>
/component/content/article?id="/<IMG SRC="36c740f584f0b46449afc021d718e547">
/component/content/article?id="/<IMG SRC=`9d256f88a2f2cbf2374625ff381d5c71`>
/component/content/article?id="/<IMG """">47d43cd8b53e3765589dcbcbf1755d6a">
/component/content/article?id="/<DIV STYLE="behaviour:url(635fd60465b188f8ba460ab6f85b734f);">
/component/content/article?id="/<IMG SRC=" &#14; 955aad3c2b0b0fa83c48c3009114b094">
/component/content/article?id="/;7218a316b06dfb6570c26dabef72626//
/component/content/article?id="/<IMG SRC=`ad20707e39821c3286f5688d47355dfb`
/component/content/article?id="/<BODY BACKGROUND="998ef469a0173a1cf46bd02d3076567c"> Failed injections
/component/content/article?id="/<INPUT TYPE="IMAGE" SRC="6b39468086c3383f7b1e15f15397c8z3">
/component/content/article?id="/<IMG DYN SRC="8d24259dd20b9ea708306dfda5ebf59">
/component/content/article?id="/<BODY ONLOAD=b64b07e385eeadc8356cd15a88c40802>
/component/content/article?id="/<IMG LOWSRC="748b2c65091adb56963b270c3a289c0d">
/component/content/article?id="/<BR SIZE="&(b59366fbc1d92ee06d0329bada9158b5)">
/component/content/article?id="/<BG SOUND SRC="b863393b6de4a72b2535a3af623bee44">
/component/content/article?id="/<LINK REL="stylesheet" HREF="3024ccce288bca59867b6596323f6cc2">
/component/content/article?id="/<IMG SRC=vscripct:1c5978a2b9b4beeb807bffe969a2bafb>
/component/content/article?id="/<IMG SRC="mocha:[401dcbfd1d5bd1b4e68b62667d966750]">
/component/content/article?id="/<IMG SRC="livescript:[8300af74253d950b6ae7f324ceaad12a]">

```

Figura 4.30 XSS con xsser [1]



A continuación se realiza la prueba de manera manual, únicamente utilizando un navegador web.

En la figura 4.31 se observa el resultado de la prueba.

Resultado obtenido:

La prueba manual de XSS no produjo resultados, lo que se visualiza en pantalla es un mensaje de error.

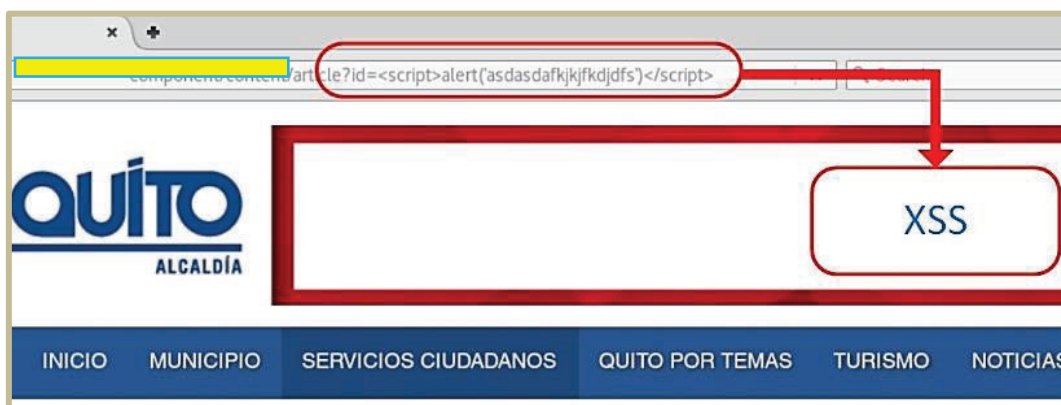


Figura 4.31 XSS con el navegador

#### 4.1.5.2. Prueba de Cross Site Scripting almacenado (OTG-INPVAL-002)

Esta prueba no es aplicable para este sitio web, ya que para ello se necesita que se guarde alguna información del usuario, por ejemplo un registro de visitas.

Ya que este sitio web es un portal donde se muestra información y es enlace hacia otros sitios no cuenta con un sistema como el mencionado.

#### 4.1.5.3. Prueba de manipulación de métodos HTTP (OTG-INPVAL-003)

El propósito de esta prueba es verificar como responde el servidor web cuando se utilizan métodos HTTP que no han sido implementados.

Entre la información más relevante que fue encontrada, se tiene:

- Versión y tipo de servidor web: Apache 2.4.6
- Sistema operativo: RHEL

- *Framework*: PHP 5.4.16

La figura 4.32 muestra el resultado de una petición con el método TRACE.

```

root@kali:~# telnet [redacted] 80
Trying [redacted]...
Connected to [redacted].
Escape character is '^['.
TRACE /index.php HTTP/1.1
Host: [redacted]

HTTP/1.1 200 OK
Date: Fri, 25 Nov 2016 17:00:16 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http

31
TRACE /index.php HTTP/1.1
  
```

Figura 4.32 Respuesta al método TRACE

En la figura 4.33 se observa el resultado de una petición con el método PUT.

```

root@kali:~# telnet [redacted] 80
Trying [redacted]...
Connected to [redacted].
Escape character is '^['.
PUT /index.php HTTP/1.1
host: [redacted]

HTTP/1.1 200 OK
Date: Fri, 25 Nov 2016 16:56:29 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16
X-Powered-By: PHP/5.4.16
Set-Cookie: 136b65862bda7837e1c7dfad8247bd04=1evdeh1k5p5in4rd126frlru25; pa
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Cache-Control: no-cache
Pragma: no-cache
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
  
```

Figura 4.33 Respuesta al método PUT

#### 4.1.5.4. Prueba de inyección SQL (OTG-INPVAL-005)

La figura 4.34 muestra el mensaje de error en el navegador cuando se realizó la consulta con la sintaxis incorrecta.

Resultado obtenido: Se obtiene es un error de página inexistente, esto quiero decir que la aplicación no presenta vulnerabilidad hacia ataques de inyección SQL.

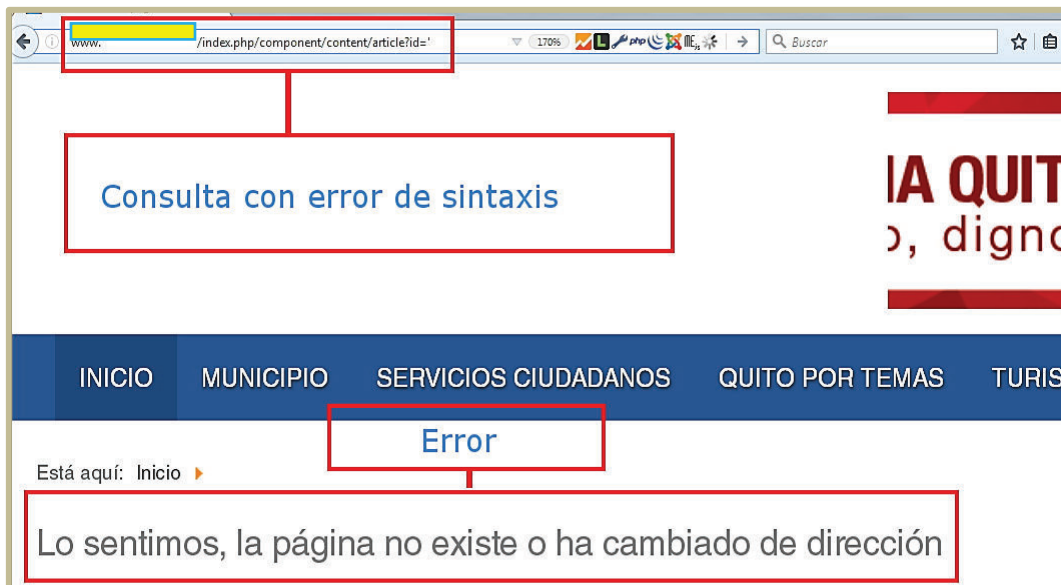


Figura 4.34 Error en la consulta

En la figura 4.35 se presentan los resultados de las pruebas utilizando una herramienta para hacerla de forma automatizada.

Resultado obtenido: La prueba no obtuvo resultados de inyección SQL.

```

root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~
root@kali:~# sqlmap -u "http://[redacted]/component/content/article?id=118"
{1.0.8.2#dev}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
Applicable local, state and federal laws. Developers assume no liability and are not responsible for any
[*] starting at 14:31:16

[14:31:16] [INFO] testing connection to the target URL
[14:31:47] [WARNING] turning off pre-connect mechanism because of connection time out(s)
[14:31:47] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[14:31:47] [WARNING] if the problem persists please check that the provided target URL is valid. In ca
tch '--random-agent' turned on and/or proxy switches ('--ignore-proxy', '--proxy',...)
[14:33:17] [CRITICAL] connection timed out to the target URL

[*] shutting down at 14:33:17

```

Figura 4.35 SQLi con sqlmap [1], [47]

#### 4.1.5.5. Prueba de inclusión local de archivos (OTG-INPVAL-012)

Conocida como LFI (*Local File Inclusion*) por sus siglas en inglés, tiene la misma finalidad que la prueba de Path traversal, ya que se busca incluir u obtener archivos sensibles en el servidor local. La figura 4.36 muestra el ataque LFI de manera automatizada utilizando la herramienta dotdotpwn [1].

Resultado obtenido: La prueba no obtuvo resultados.



```

http:// [redacted] /content/article?id=TRAVERSAL:80/../etc/passwd
http:// [redacted] /content/article?id=TRAVERSAL:80/../..etc/passwd
http:// [redacted] /content/article?id=TRAVERSAL:80/../...etc/passwd
http:// [redacted] /content/article?id=TRAVERSAL:80/../...etc/passwd
http:// [redacted] /content/article?id=TRAVERSAL:80/../...etc/passwd
http:// [redacted] /content/article?id=TRAVERSAL:80/../...etc/passwd
http:// [redacted] /content/article?id=TRAVERSAL:80/..%5Cetc%5Cpasswd
http:// [redacted] /content/article?id=TRAVERSAL:80/..%5C.%5Cetc%5Cpasswd
http:// [redacted] /content/article?id=TRAVERSAL:80/..%5C.%5C.%5Cetc%5Cpasswd
http:// [redacted] /content/article?id=TRAVERSAL:80/..%5C.%5C.%5C.%5Cetc%5Cpasswd
http:// [redacted] /content/article?id=TRAVERSAL:80/..%5C.%5C.%5C.%5C.%5Cetc%5Cpasswd

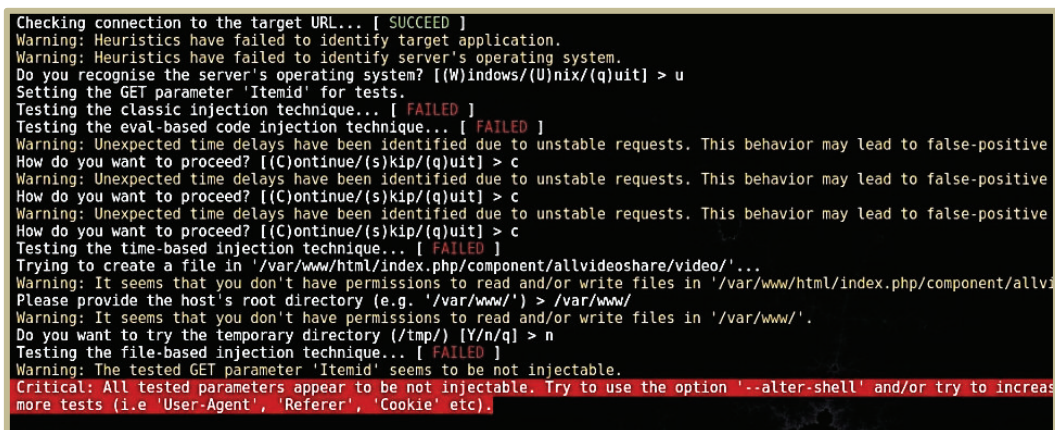
```

Figura 4.36 LFI con dotdotpwn[1]

#### 4.1.5.6. Prueba de inyección de comandos (OTG-INPVAL-013)

En la figura 4.37 se aprecia el resultado que se obtuvo para la prueba de inyección de comandos de manera automatizada con la ayuda de la herramienta *commix*, misma que se incluye en Kali Rolling 2016.2 [2].

Resultado obtenido: La prueba no determina resultados referentes a inyección de comandos.



```

Checking connection to the target URL... [ SUCCEEDED ]
Warning: Heuristics have failed to identify target application.
Warning: Heuristics have failed to identify server's operating system.
Do you recognise the server's operating system? [(W)indows/(U)nix/(q)uit] > u
Setting the GET parameter 'Itemid' for tests.
Testing the classic injection technique... [ FAILED ]
Testing the eval-based code injection technique... [ FAILED ]
Warning: Unexpected time delays have been identified due to unstable requests. This behavior may lead to false-positive
How do you want to proceed? [(C)ontinue/(s)kip/(q)uit] > c
Warning: Unexpected time delays have been identified due to unstable requests. This behavior may lead to false-positive
How do you want to proceed? [(C)ontinue/(s)kip/(q)uit] > c
Warning: Unexpected time delays have been identified due to unstable requests. This behavior may lead to false-positive
How do you want to proceed? [(C)ontinue/(s)kip/(q)uit] > c
Testing the time-based injection technique... [ FAILED ]
Trying to create a file in '/var/www/html/index.php/component/allvideoshare/video/...'
Warning: It seems that you don't have permissions to read and/or write files in '/var/www/html/index.php/component/allv
Please provide the host's root directory (e.g. '/var/www/') > /var/www/
Warning: It seems that you don't have permissions to read and/or write files in '/var/www/'.
Do you want to try the temporary directory (/tmp/) [Y/n/q] > n
Testing the file-based injection technique... [ FAILED ]
Warning: The tested GET parameter 'Itemid' seems to be not injectable.
Critical: All tested parameters appear to be not injectable. Try to use the option '--alter-shell' and/or try to increas
more tests (i.e 'User-Agent', 'Referer', 'Cookie' etc).

```

Figura 4.37 Inyección de comandos con commix [1]

## 4.1.6. RESULTADO DE PRUEBAS: MANEJO DE ERRORES

### 4.1.6.1. Análisis de códigos de error (OTG-ERR-001)

En la figura 4.38 se muestra el resultado obtenido utilizando el navegador web.

Resultado obtenido:

Al revisar el mensaje de error no se encuentra información importante de ningún tipo acerca del servidor web.

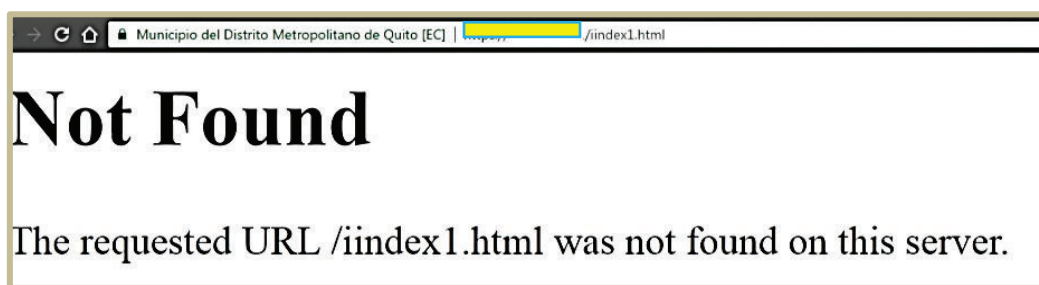


Figura 4.38 Mensaje de error de página inexistente

Por otro lado en la figura 4.39 se observa que si existe información expuesta sobre el servidor cuando se utiliza para esta prueba la herramienta telnet.

Entre la información más relevante se tiene:

- Versión y tipo de servidor web: Apache 2.4.6
- Sistema operativo: RHEL
- *Framework*: PHP 5.4.16

```

root@kali:~# telnet [IP] 80
Trying [IP]...
Connected to [IP].
Escape character is '^'.
GET /iindex1.html HTTP/1.1
host:
HTTP/1.1 404 Not Found
Date: Fri, 25 Nov 2016 10:40:43 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16
Content-Length: 210
Connection: close
Content-Type: text/html; charset=iso-8859-1
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>

```

Figura 4.39 Petición de una página inexistente con telnet

#### 4.1.7. RESULTADO DE PRUEBAS: CRIPTOGRAFÍA

##### 4.1.7.1. Prueba de cifrado SSL/TLS débil y protección insuficiente de capa de transporte (OTG-CRYPST-001)

La figura 4.40 expone los resultados obtenidos con la herramienta nmap, para encontrar los servicios que utiliza SSL/TLS. Para esto se hizo el escaneo con nmap y la ayuda de un *script*.

Entre la información encontrada más importante, se tiene:

- Puertos cerrados: 443, esto quiere decir que no está implementado HTTPS.
- Puertos filtrados: 465, 993, 995, no se puede afirmar si los servicios seguros de smtp, imap y pop3 están activos ya que existe un filtrado de paquetes.

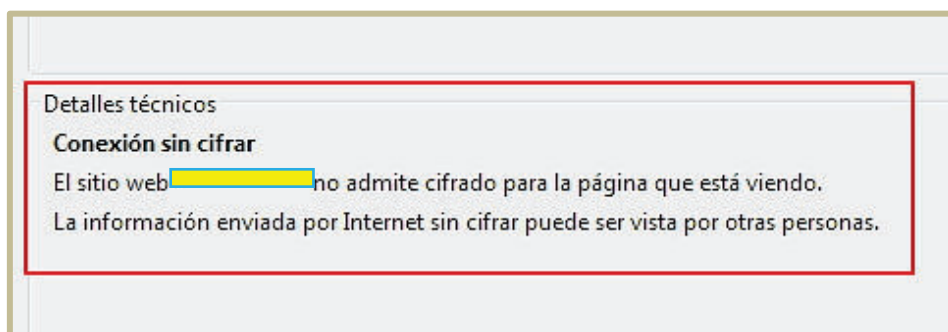
```
#nmap --script=ssl-cert,ssl-enum-ciphers -p 443,465,993,995 -oN [redacted]
# Nmap 7.25BETA2 scan initiated Fri Nov 25 12:20:07 2016
Nmap scan report for
Host is up (0.0049s latency).
PORT      STATE      SERVICE
443/tcp   closed    https
465/tcp   filtered  smtps
993/tcp   filtered  imaps
995/tcp   filtered  pop3s

# Nmap done at Fri Nov 25 12:20:11 2016 -- 1 IP address (1 host up) scanned in 3.85 seconds
```

**Figura 4.40 Servicios que utilizan SSL/TLS**

En la figura 4.41 se aprecia el resultado de revisar manualmente el certificado del sitio web.

Resultado obtenido: La página web no admite cifrado SSL/TLS.



**Figura 4.41 Revisión manual del certificado**

#### 4.1.7.2. Prueba de información sensible enviada por canales sin encriptar (OTG-CRYPT-003)

En la figura 4.42 se muestra el resultado de la prueba con el escáner de vulnerabilidades Nessus [31], [32].

Resultado obtenido:

El escáner Nessus determina que la información que transmite el servidor web viaja en texto claro.

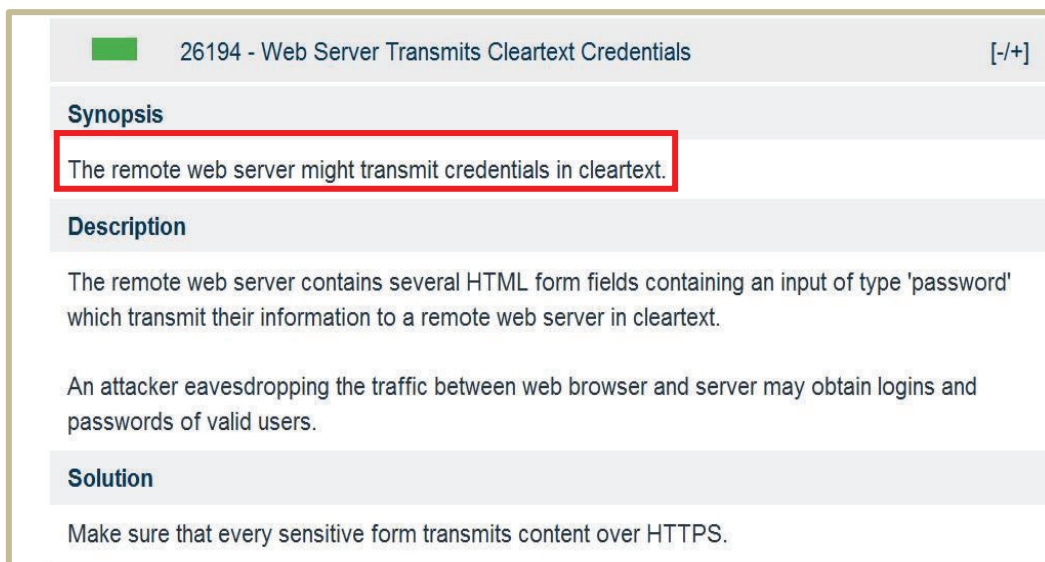


Figura 4.42 Prueba de SSL/TLS con Nessus

## 4.2. RESULTADO DE PRUEBAS PARA EL PORTAL DE PAGO DE IMPUESTOS POR INTERNET

### 4.2.1. RESULTADO DE PRUEBAS: RECOPIACIÓN DE INFORMACIÓN

#### 4.2.1.1. Descubrimiento con motores de búsqueda y reconocimiento por fugas de información (OTG-INFO-001)

En la figura 4.43 se presenta el resultado de esta prueba, cuando se busca subdominios del objetivo. Para eso se utilizan las siguiente búsquedas avanzadas:

- Búsqueda de Subdominios:



**Figura 4.43 Búsqueda de subdominios**

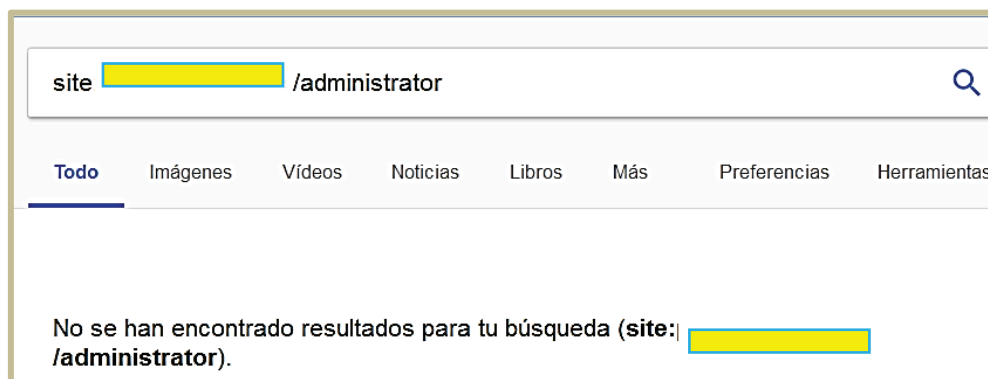
Resultados de la búsqueda: Se encontró subdominios del objetivo principal, estos pueden ser vulnerables o mal configurados.

- Búsqueda de interfaces de administración

En la figuras 4.44, 4.45 y 4.46 se presentan el resultado de la búsqueda de una interfaz de administración, para Joomla, WordPress y Drupal respectivamente.

Figura 4.44 búsqueda de interfaz de administración para Joomla.

Resultado de la primera búsqueda: La consulta no produjo resultados.

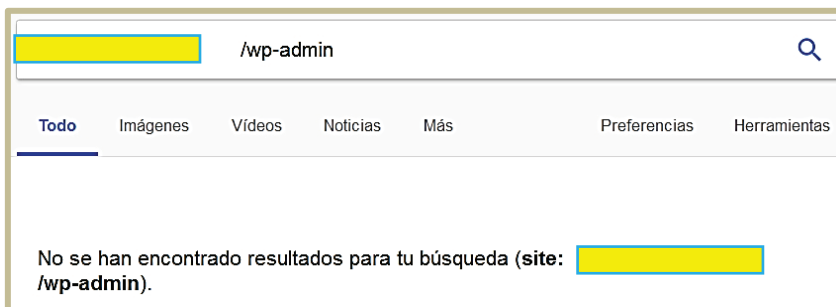


**Figura 4.44 Búsqueda de interfaz de administración Joomla**

Figura 4.45 búsqueda de interfaz de administración para Wordpress.

Resultado de la segunda búsqueda: La consulta no produjo resultados.

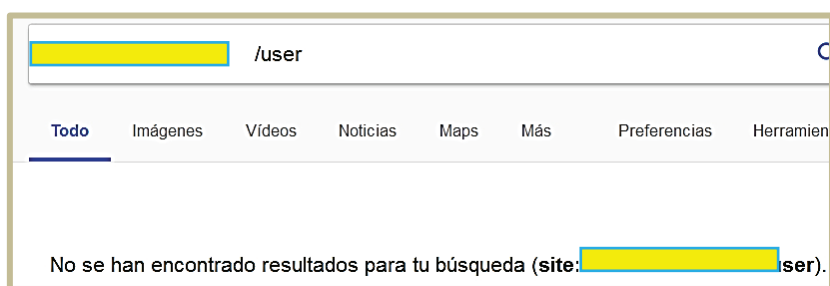




**Figura 4.45 Búsqueda de interfaz de administración Wordpress**

Figura 4.46 búsqueda de interfaz de administración para Drupal.

Resultado de la segunda búsqueda: La consulta no produjo resultados.

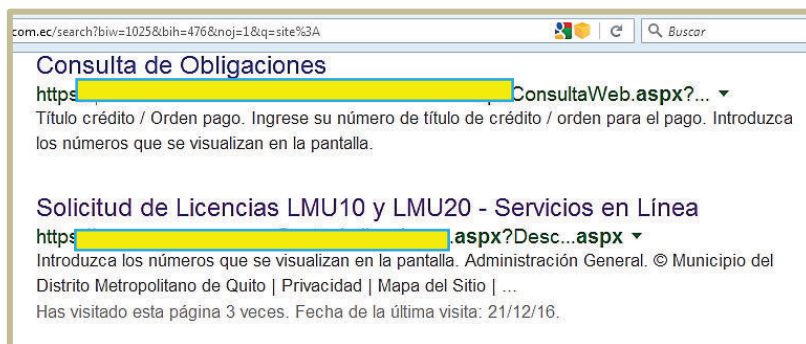


**Figura 4.46 Búsqueda de interfaz de administración Drupal**

- Búsqueda de páginas con parámetros susceptibles a XSS o SQLi.

En la figura 4.47 se muestra el resultado para buscar páginas susceptibles a XSS e inyección SQL dentro del dominio.

Resultados de la búsqueda: Se encontraron páginas con parámetros en la URL (**aspx?id=**) los cuales pueden ser susceptibles a ataques de XSS o inyección SQL.



**Figura 4.47 Búsqueda de páginas propensas a XSS e inyección SQL**

- Búsqueda de tipo y versión de servidor web.

En la figura 4.48 se muestra el resultado de buscar la versión y tipo de servidor web.

Resultado de la prueba: No se obtuvieron resultados.

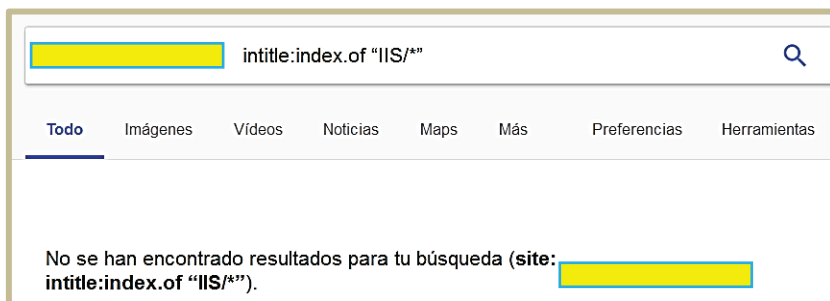


Figura 4.48 Búsqueda de la versión y tipo de Servidor Web

#### 4.2.1.2. Fingerprint del servidor web (OTG-INFO-002)

Para esta prueba se usará la herramienta httpprint y wappalyzer de Firefox, en la figura 4.49 se aprecia el resultado de la prueba con la ayuda de httpprint.

Entre la información encontrada, considerada más relevante está:

- Tipo de servidor web: IIS
- Versión del servidor web: 7.5
- Sistema operativo: Microsoft Windows Server

```

root@kali:~# httpprint -h http://[redacted] -s /usr/share/httpprint/signatures.txt
httpprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httpprint/
httpprint@net-square.com

Finger Printing on http://[redacted]:80/
Finger Printing Completed on http://[redacted]:80/
-----
Host:
Derived Signature:
Microsoft-IIS/7.5
FACD41D36ED3C295811C9DC5811C9DC5811C9DC594DF1BD04276E4BB811C9DC5
0D7645B5811C9DC52A200B4CCD37187C11DDC7D78398721E811C9DC5811C9DC5
E2CE6926E2CE6923E2CE6923811C9DC5E2CE69272576B769E2CE6926FACD41D3
6ED3C295E1CE67B1811C9DC5E2CE6923E2CE6923E2CE6920E2CE6920E2CE6923
E2CE6923811C9DC5A732F670E2CE6927E2CE6920

Banner Reported: Microsoft-IIS/7.5
Banner Deduced: Microsoft-IIS/6.0
Score: 134
Confidence: 80.72
  
```

Figura 4.49 Fingerprint del servidor web con httpprint

En la figura 4.50 se observa el mismo resultado, pero esta vez utilizando el plugin wappalyzer de Firefox.

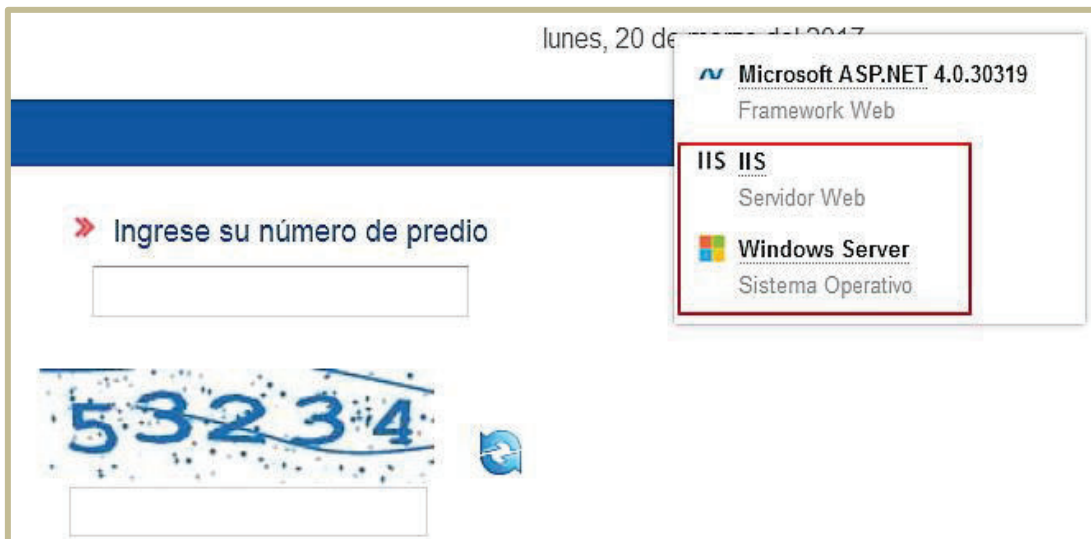


Figura 4.50 Fingerprint del servidor con wappalyzer

#### 4.2.1.3. Revisión de meta-archivos por fugas de información (OTG-INFO-003)

Resultado obtenido: La prueba no produjo resultados, no existe el archivo robots.txt en la ubicación por defecto.

En la figura 4.51 muestra la forma de descargar el archivo robots.txt con el comando wget.

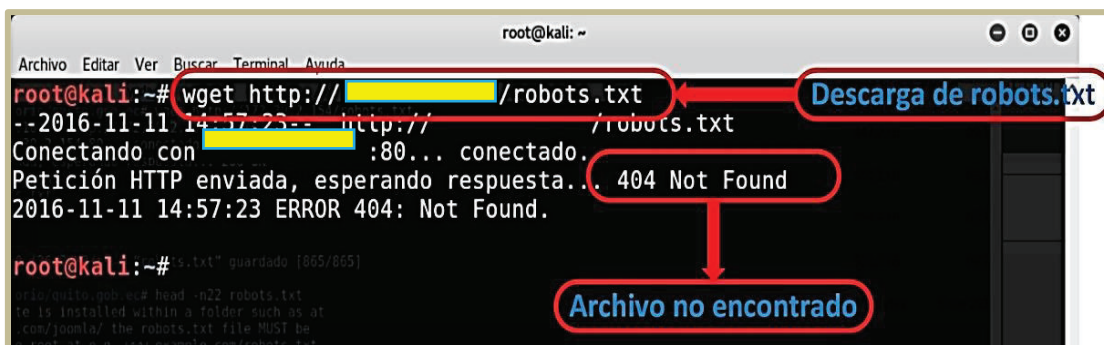


Figura 4.51 Descarga de robots.txt con wget

En la figura 4.52 se observa el mismo resultado de la prueba anterior, pero esta vez utilizando ZAP de OWASP.

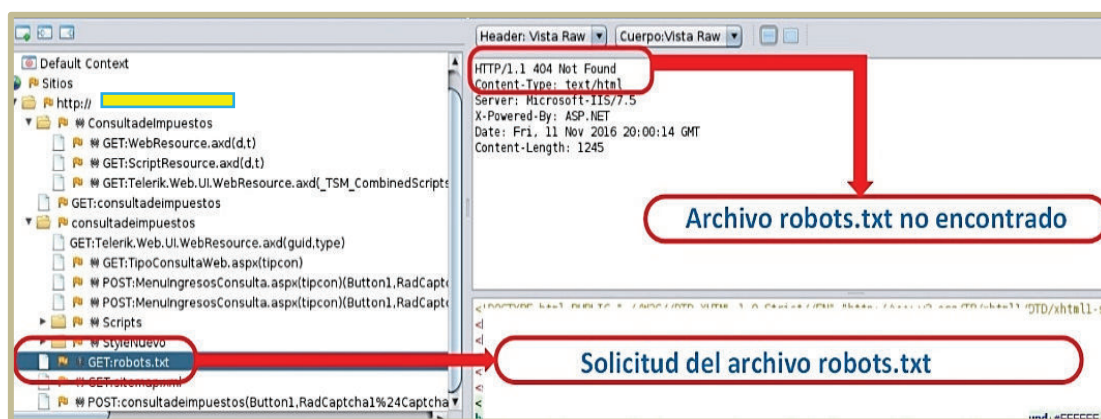


Figura 4.52 Visualización de robots.txt con ZAP

#### 4.2.1.4. Enumerar aplicaciones en el servidor web (OTG-INFO-004)

La figura 4.53 se aprecia el resultado de la prueba realizada con el comando nmap.

Entre la información más importante se tiene lo siguiente:

- Puertos abiertos: 80, 135, 139, 443,445, 2000, 3389, 8000, 49152, 49153, 49154, 49155, 49156, 49159, 49160
- Sistema operativo: Microsoft Windows Server 2008 R2
- Servicios y su versión

```
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-11-11 15:44 ECT
Nmap scan report for
Host is up (0.041s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft IIS httpd 7.5
135/tcp   open  msrpc?
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp   open  ssl/http        Microsoft IIS httpd 7.5
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
2000/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server   Microsoft Terminal Service
8080/tcp  open  http            Microsoft IIS httpd 7.5
49152/tcp open  msrpc           Microsoft Windows RPC
49153/tcp open  msrpc           Microsoft Windows RPC
49154/tcp open  msrpc           Microsoft Windows RPC
49155/tcp open  msrpc           Microsoft Windows RPC
49156/tcp open  msrpc           Microsoft Windows RPC
49159/tcp open  msrpc           Microsoft Windows RPC
49160/tcp open  msrpc           Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:wi
```

Figura 4.53 Enumerando aplicaciones con nmap

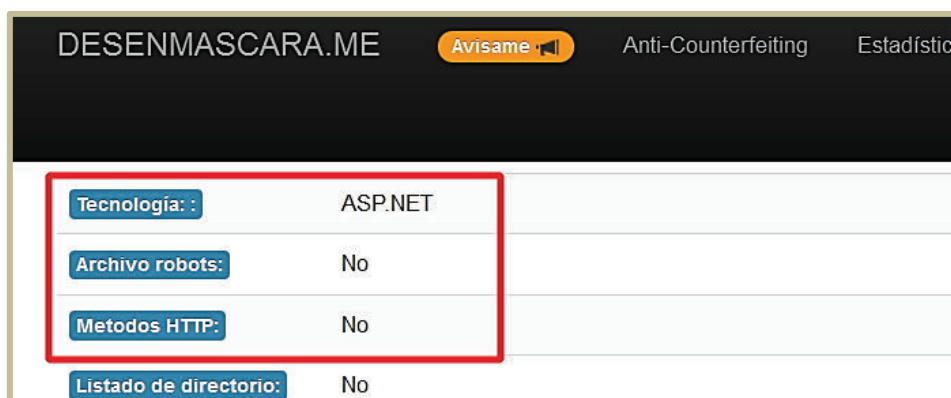
#### 4.2.1.5. Revisar comentarios en la página web y metadatos por fugas de información (OTG-INFO-005)

Para esta esta prueba se hace uso de la herramienta en línea desenmascara.me para revisar los metadatos de la página web y para encontrar comentarios se visualiza el código fuente de la página web con la ayuda del navegador.

En la figura 4.54 se muestra el resultado de metadatos con desenmascara.me.

Resultados obtenidos:

- *Fingerprint* del *framework* de la aplicación: ASP.NET
- Archivo robots.txt: no encontrado



DESENMASCARA.ME	
Tecnología:	ASP.NET
Archivo robots:	No
Métodos HTTP:	No
Listado de directorio:	No

Figura 4.54 Metadatos con desenmascara.me

En la figura 4.55 se observa el código fuente de la página, con la ayuda del navegador web. Resultados obtenidos: No se encuentran comentarios con información importante en el código de la página web.

```
function seleccionTodos() {
//*****
/** CONTROL PARA SELECCIONAR Y DESELECCIONAR TODOS LOS REGISTROS **
//*****
var controles = document.getElementById("tblDatos").getElementsByTagName("input");
var checkcontrol = document.getElementById("tbCabecera").getElementsByTagName("input");

var cont = 0;
var inputs = document.getElementsByName("txtPagoAbo");

for (j = 0; j < controles.length; j++) {
```

Figura 4.55 Revisión de comentarios en el código fuente de la página web

#### 4.2.1.6. Identificar los puntos de entrada de la aplicación (OTG-INFO-006)

En la figura 4.56 se visualiza los parámetros encontrados en una solicitud con el método post. La información más importante que se encontró es la siguiente:

- Parámetros en la URL: idrubro, idrub, desrub, pago, fpago, trans, coopro, pat\_
- Cookies: \_utma, \_utmz, \_ga<sup>55</sup>, ASP.NET\_Sessionid

Type	Name	Value
URL	idrubro	1
URL	idrub	260
URL	desrub	CEM
URL	pago	Pendiente
URL	fpago	
URL	trans	
URL	coopro	0000000
URL	pat	
Cookie	_utma	190538282.1686913000.1479831139.1479831139.1479831139.1
Cookie	_utma	190538282.1686913000.1479831139.1479831139.1479831139.1
Cookie	_utmz	190538282.1479831139.1.1.utmcsr=(direct) utmccn=(direct) utmcmd=(none)
Cookie	_utmz	190538282.1479831139.1.1.utmcsr=(direct) utmccn=(direct) utmcmd=(none)
Cookie	_ga	GA1.3.420818313.1480606043
Cookie	ASP.NET_Sessionid	f00rr2ccpckpi34mo2nkfrq5

Figura 4.56 Solicitud con el método post

#### 4.2.1.7. Mapear rutas de ejecución a través de la aplicación (OTG-INFO-007)

En la figura 4.57 se presenta el resultado del *spidering* con la herramienta Burp Suite.

Resultado obtenido: Mapa del sitio web y árbol de directorios del mismo.

The screenshot shows the Burp Suite interface. On the left, a directory tree is visible under the URL 'https://'. The tree includes folders like 'Consultasobligaciones', 'Scripts', 'StyleNuevo', 'Telerik.Web.UI.WebResource.axd', 'WebResource.axd', 'Images', 'ScriptResource.axd', 'TSbd', 'WebResource.axd', and 'layouts'. On the right, a table lists HTTP requests with columns for Host, Method, URL, Params, Status, and Length. A red box highlights the directory tree, and a red arrow points from it to the 'Request' tab of a selected request. Below the screenshot, the text 'Árbol de directorios' is written in blue.

Figura 4.57 Spidering con Burp Suite

<sup>55</sup> Cookies de Google Analytics, ayuda a los propietarios de sitios web a medir cómo interactúan los usuarios con el sitio web

#### 4.2.1.8. Fingerprint el framework de la aplicación web (OTG-INFO-008)

Conocer el *framework* de una aplicación es una forma de fuga de información, con esto se podría buscar en Internet vulnerabilidades conocidas.

En la información encontrada con esta prueba se tiene:

- X-Powered-By: ASP.NET
- Sistema operativo: Microsoft Windows Servoer
- Tipo y versión de servidor web: IIS 7.5

La figura 4.58 muestra el resultado de esta prueba utilizando la herramienta whatweb.

```

root@kali:~# whatweb http://[redacted]
http://[redacted]/consultadeimpuestos/ [200 OK] ASP.NET[4.0.30319], Cookies[/_
_SessionId], Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/7.5], HttpOnly[AS
essionId], IP[redacted], Microsoft-IIS[7.5], Script[text/javascript,text/vi
], Title[Consulta de Obligaciones], X-Powered-By[ASP.NET]
root@kali:~#
  
```

Figura 4.58 Fingerprint del framework de la aplicación

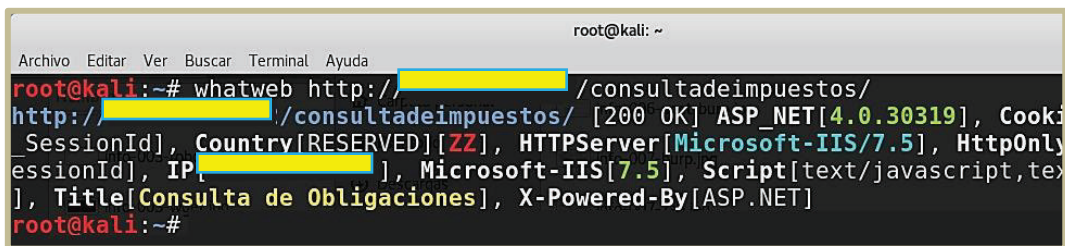
#### 4.2.1.9. Fingerprint a la aplicación web (OTG-INFO-009)

Otra de las variables importantes para la búsqueda de vulnerabilidades conocidas es el gestor de contenido (CMS), para ello se utiliza BuiltWith y la herramienta whatweb.

Entre la información la información más relevante está:

- No se encuentra información acerca del CMS
- *Framework* de la aplicación: ASP.NET
- Sistema operativo: Microsoft Windows Server
- Tipo y versión del servidor web: IIS/7.5
- Dirección IP pública del servidor web

En la figura 4.59 se visualiza el resultado con la ayuda de la herramienta whatweb.



```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# whatweb http://[redacted]/consultadeimpuestos/
http://[redacted]/consultadeimpuestos/ [200 OK] ASP.NET[4.0.30319], Cooki
SessionId], Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/7.5], HttpOnly
essionId], IP,[redacted], Microsoft-IIS[7.5], Script[text/javascript,te
], Title[Consulta de Obligaciones], X-Powered-By[ASP.NET]
root@kali:~#

```

Figura 4.59 Fingerprint a la aplicación web con whatweb

En la figura 4.60 se usa la herramienta en línea BuiltWith.

Resultados obtenidos: No se obtuvo información acerca del CMS.

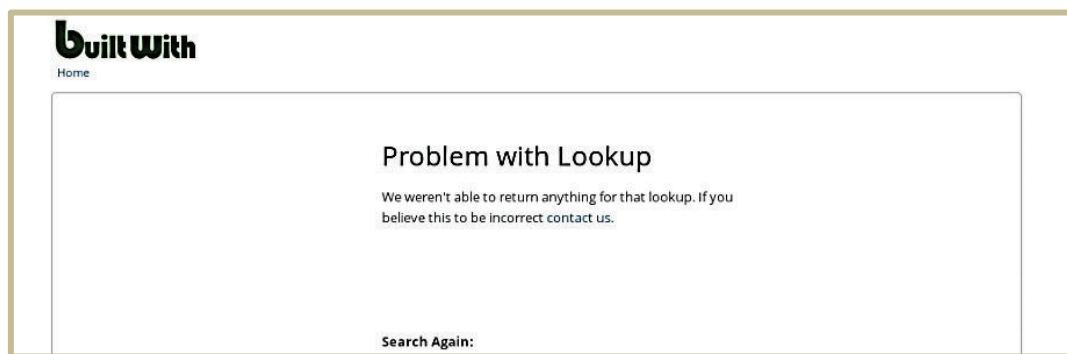


Figura 4.60 Fingerprint a la aplicación web con BuiltWith

## 4.2.2. RESULTADO DE PRUEBAS: GESTIÓN DE LA CONFIGURACIÓN Y LA IMPLEMENTACIÓN

### 4.2.2.1. Prueba de configuración de red/infraestructura (OTG-CONFIG-001)

Los resultados de esta prueba son lo mismos que se detallan en la sección 4.1.2.1.

### 4.2.2.2. Prueba de configuración de la plataforma de la aplicación (OTG-CONFIG-002)

En la tabla 4.2 se listan los *features*<sup>56</sup> instalados en el servidor web.

Features Instalados		
Web Server	Commom HTTP feature	Static Content
		Default Document

<sup>56</sup> Los features son programas que pueden complementar, aumentar o mejorar la funcionalidad del servidor.



Features Instalados		
Web server		Directory Browsing
		HTTP Errors
	Application Development	ASP.NET
		.NET
		ASP
		CGI
		ISAPI Extension
		ISAPI Filters
		Healt and Diagnostic
	Request Monitor	
	Security	Based Authentication
		Windows Authentication
		Request Filtering
	Performance	Static Content Commpression
	Management Tools	
IIS 6 Management Compatibility		IIS 6 Metabase Compatibility
		IIS 6 WMI Compatibility
		IIS 6 Scripting Tools
		IIS 6 Management Console

**Tabla 4.2 Features del servidor web**

**4.2.2.3. Archivos de backup y no referenciados con información sensible (OTG-CONFIG-004)**

El resultado de esta prueba es el mismo que se encuentra explicado en la sección 4.1.2.3.

#### 4.2.2.4. Enumerar interfaces de administración de aplicaciones y de infraestructura (OTG-CONFIG-005)

Las interfaces de administración proporcionan una entrada con muchos privilegios para poder modificar el sitio web o la aplicación, actividades que no pueden hacer usuarios normales o estándar.

En la figura 4.62 se pretende ingresar a una interfaz de administración Joomla.

Resultado obtenido: No se encuentra una interfaz de administración para Joomla.

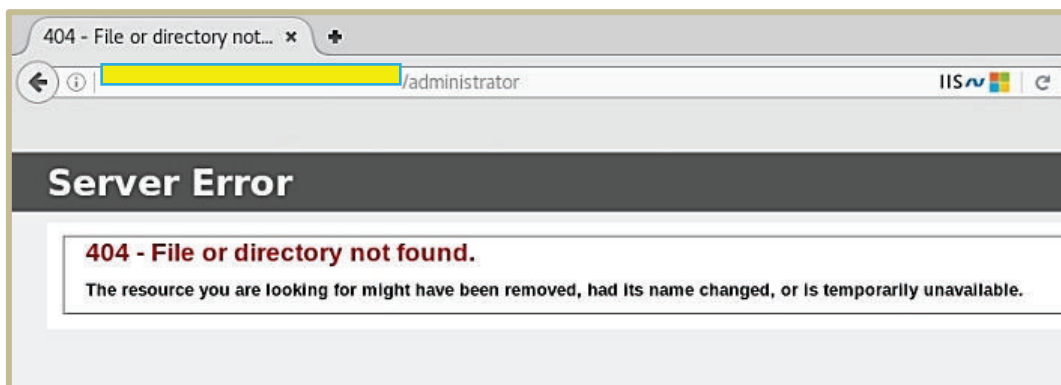


Figura 4.62 Ingreso a interfaz de administración Joomla

En la figura 4.63 se aprecia como ingresar a una interfaz de administración WordPress mediante el navegador.

Resultado obtenido: No se encuentra una interfaz de administración para WordPress.

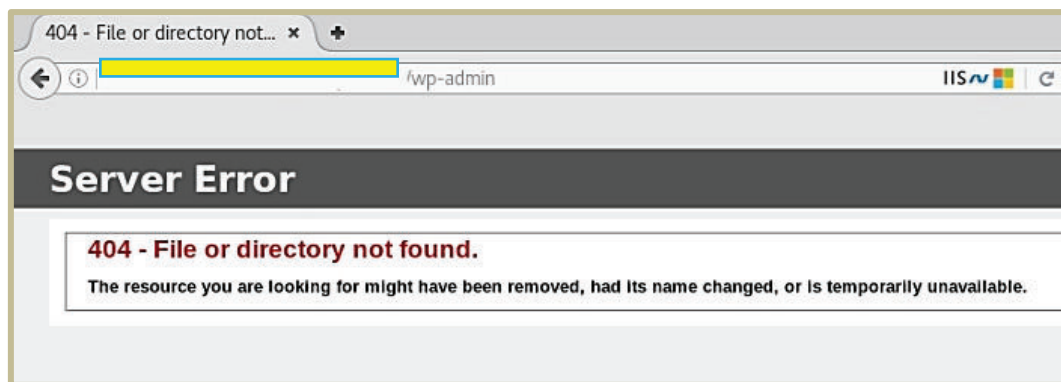


Figura 4.63 Ingreso a interfaz de administración WordPress

En la figura 4.64 se demuestra como ingresar a una interfaz de administración Drupal mediante el navegador.

Resultado obtenido: No se encuentra una interfaz de administración para Drupal.

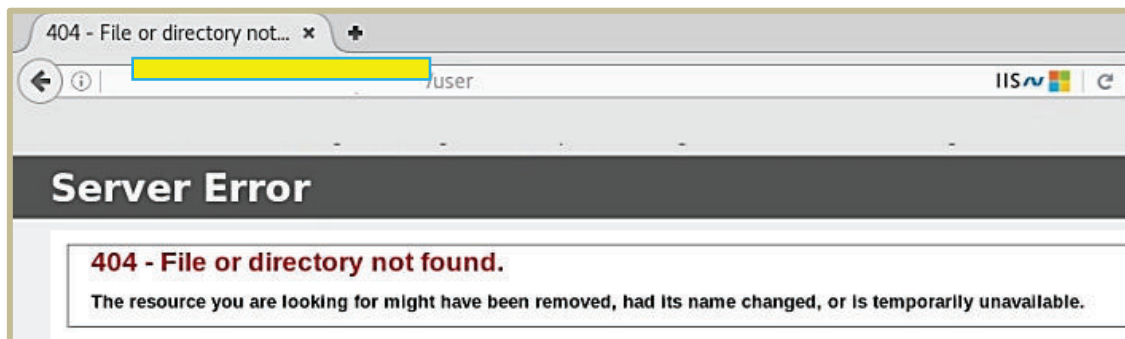


Figura 4.64 Ingreso a interfaz de administración Drupal

#### 4.2.2.5. Prueba de métodos HTTP (OTG-CONFIG-006)

Información encontrada en la presente prueba:

- Métodos HTTP configurados: GET, HEAD, POST, TRACE
- Sistema operativo: Microsoft Windows Server
- Versión y tipo de servidor web: IIS 7.5

En la figura 4.65 se visualiza el resultado de la prueba para identificar los métodos configurados en el servidor web.

```

root@kali:~# nmap -sV --script=http-methods [redacted] -p80
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-11-11 15:36 ECT
Nmap scan report for [redacted]
Host is up (0.012s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 7.5
|_ http-methods:
|_   Supported Methods: OPTIONS TRACE GET HEAD POST
|_   Potentially risky methods: TRACE
|_   http-server-header: Microsoft-IIS/7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.74 seconds
  
```

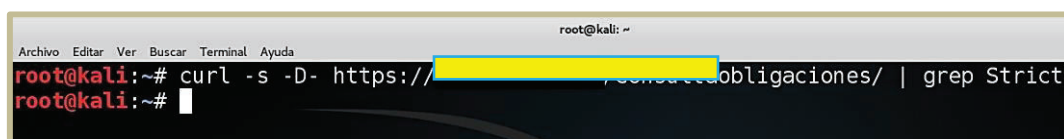
Métodos configurados

Figura 4.65 Métodos configurados en el servidor web

#### 4.2.2.6. Prueba de seguridad de transporte estricto HTTP - HSTS (OTG-CONFIG-007)

La figura 4.66 muestra el resultado obtenido con la herramienta curl, al tratar de verificar si este mecanismo de seguridad ha sido implementado.

Resultado de la prueba: como el comando *grep* no encontró coincidencias dentro de la cabecera HTTP, este no muestra nada en pantalla, esto quiere decir que el sistema HSTS no está implementado



```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# curl -s -D- https://[redacted] /comunicacion/obligaciones/ | grep Strict
root@kali:~#
  
```

Figura 4.66 Implementación de HSTS

La figura 4.67 muestra el resultado obtenido con la herramienta en línea SSL Server Test.

Resultado de la prueba: El método de seguridad no está implementado.

Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
<b>Strict Transport Security (HSTS)</b>	<b>No</b>
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No

Figura 4.67 Resultado de SSL Server Test

#### 4.2.2.7. Prueba de política de dominio cruzado RIA (OTG-CONFIG-008)

En la figura 4.68 se observa el resultado de la prueba, para esto se usa el navegador.

Resultados: No existe el archivo *crossdomain.xml*.

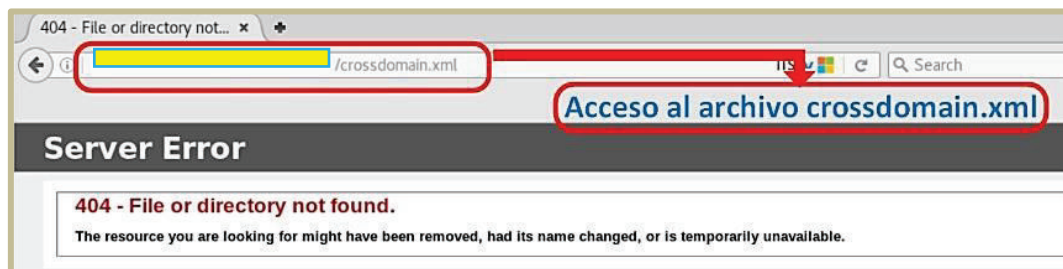


Figura 4.68 Archivo crossdomain.xml

### 4.2.3. RESULTADO DE PRUEBAS: AUTORIZACIÓN

#### 4.2.3.1. Prueba de directorio/path traversal (OTG-AUTHZ-001)

En la figura 4.69 se muestra el resultado obtenido con una herramienta de forma automatizada.

Resultados obtenidos: En la figura se observa que la herramienta dotdotpwn ha determinado que la página web es vulnerable al ataque de *path traversal*.

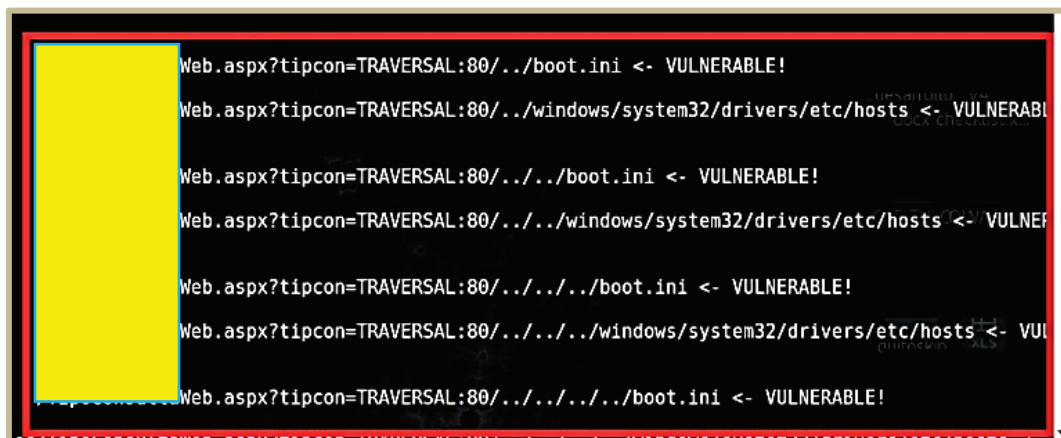


Figura 4.69 Path traversal con dotdotpwn

A continuación se realiza la prueba de manera manual, utilizando un navegador web.

Resultados obtenidos: La prueba no obtuvo resultados relacionados a *path traversal*, se obtiene un mensaje de error de una página no encontrada.

La figura 4.70 muestra el resultado que se obtuvo al realizar el ataque modificando la URL.



Figura 4.70 Path traversal modificando la URL

#### 4.2.3.2. Prueba de escalamiento de privilegios (OTG-AUTHZ-003)

La sección 4.1.3.2 presenta información acerca de esta prueba.

#### 4.2.3.3. Prueba de referencia directa insegura a objetos (OTG-AUTHZ-004)

La figura 4.71 presenta la página original sin modificar el parámetro *tipcon* en la URL.

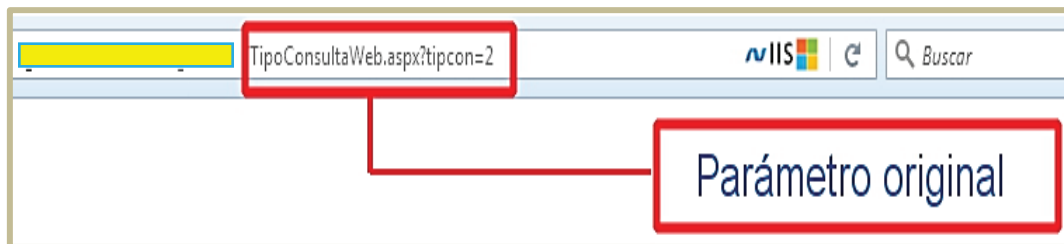


Figura 4.71 Página sin modificar parámetro

En la figura 4.72 se observa el resultado obtenido en el navegador cuando se ha modificado el parámetro *tipcon=30* en la URL.

Resultado obtenido:

Como resultado se produjo una ligera desfiguración en la página web, no se pudo acceder a funcionalidades ni privilegios especiales al modificar el parámetro de la URL.

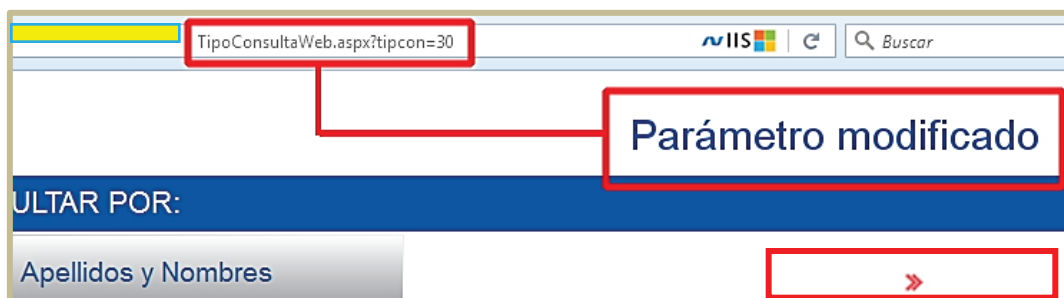


Figura 4.72 Página sin modificar parámetro

#### 4.2.4. RESULTADO DE PRUEBAS: GESTIÓN DE SESIONES

##### 4.2.4.1. Prueba de falsificación de peticiones en sitios cruzados - CSRF (OTG-SESS-005)

En la sección 4.1.4.1 se encuentra el resultado de la presente prueba.

#### 4.2.5. RESULTADO DE PRUEBAS: VALIDACIÓN DE ENTRADA

##### 4.2.5.1. Prueba de Cross Site Scripting reflejado (OTG-INPVAL-001)

La figura 4.73 presenta el resultado del ataque de XSS de manera automatizada.

Resultado obtenido: La herramienta ha probado todas las variantes para realizar ataques de XSS, dando como resultado únicamente fallos.

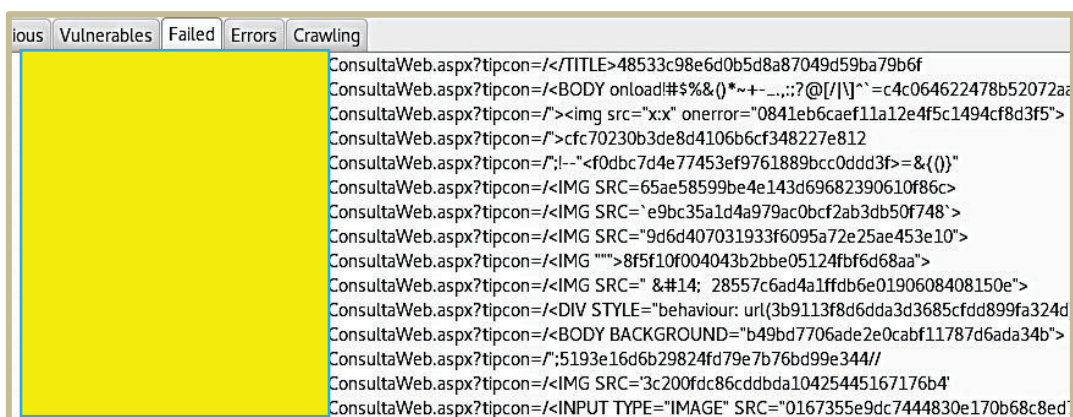


Figura 4.73 XSS con xsser [1]

En la figura 4.74 se aprecia el resultado del ataque realizado de forma manual, modificando la URL, con ayuda del navegador.

Resultado obtenido: No se obtuvo resultados.

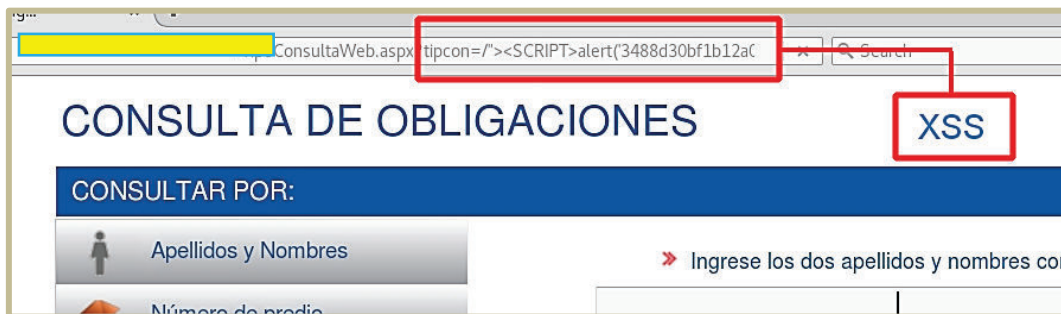


Figura 4.74 XSS en la URL

En la figura 4.75 se observa el resultado de la prueba cuando se inyecta el código en el cuadro de entrada de datos.

Resultado obtenido:

No se encontró resultados favorables, la entrada de datos esta validada, se visualiza un mensaje que indica que únicamente se puede utilizar números.

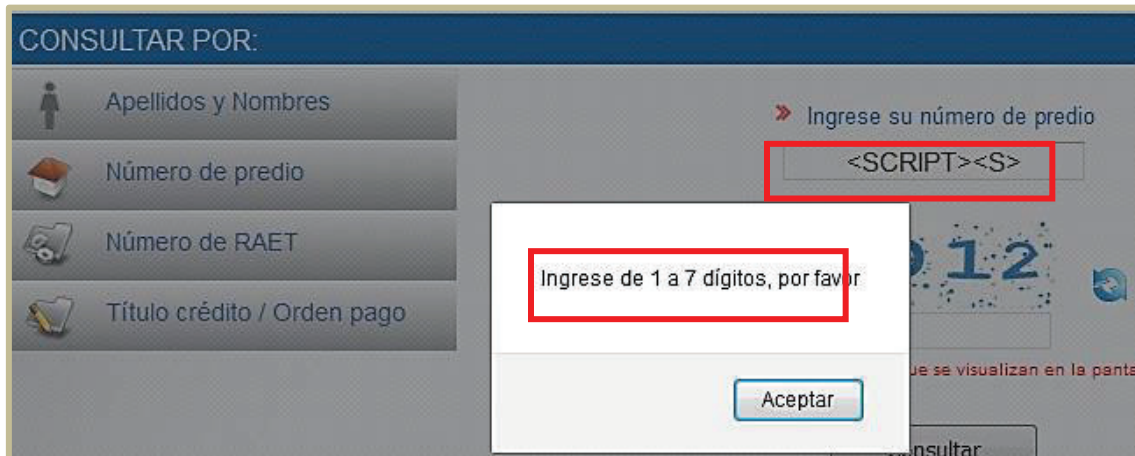


Figura 4.75 XSS en la entrada de datos

#### 4.2.5.2. Prueba de Cross Site Scripting almacenado (OTG-INPVAL-002)

La sección 4.1.5.2 indica el resultado de esta prueba.

#### 4.2.5.3. Prueba de manipulación de métodos HTTP (OTG-INPVAL-003)

La información más relevante que se obtuvo en esta prueba es la siguiente:



- Versión y tipo de servidor web: IIS/7.5
- Sistema operativo: Microsoft Windows Server
- *Framework*: ASP.NET

La figura 4.76 muestra el resultado de una consulta con el método TRACE.

La figura 4.77 presenta el resultado de una consulta con el método PUT.

Resultado obtenido: No se obtuvo información importante acerca del servidor web.

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# telnet [redacted] 80
Trying [redacted] ...
Connected to [redacted].
Escape character is '^]'.
TRACE /index.aspx HTTP/1.1
Host:

HTTP/1.1 501 Not Implemented
Content-Type: text/html
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Fri, 25 Nov 2016 18:39:35 GMT
Content-Length: 1508

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http:

```

Figura 4.76 Solicitud con el método TRACE

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# telnet [redacted] 80
Trying [redacted] ...
Connected [redacted].
Escape character is '^]'.
PUT /index.aspx HTTP/1.1
Host:

HTTP/1.1 411 Length Required
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Fri, 25 Nov 2016 18:41:19 GMT
Connection: close
Content-Length: 344

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org

```

Figura 4.77 Solicitud con el método PUT

#### 4.2.5.4. Prueba de inyección SQL (OTG-INPVAL-005)

La figura 4.78 muestra el error que se generó al realizar la inyección SQL, con la ayuda del navegador.

Resultado obtenido: No se presentan errores relacionados con bases de datos. Quiere decir que la aplicación no es vulnerable a inyección SQL.



Figura 4.78 Inyección SQL de forma manual

En la figura 4.79 se observa el resultado de la prueba realizada de manera automatizada.

Resultado obtenido:

La prueba no obtuvo resultados de inyección SQL.

```

root@kali:~# sqlmap -u "http://[redacted]/TipoConsultaWeb.aspx?tipcon=1"
{1.0.8.2#dev}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse
[*] starting at 11:18:29

[11:18:29] [INFO] testing connection to the target URL
[11:18:59] [WARNING] turning off pre-connect mechanism because of connection time out(s)
[11:18:59] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[11:18:59] [WARNING] if the problem persists please check that the provided target URL is valid. In case that i
tch '--random-agent' turned on and/or proxy switches ('--ignore-proxy', '--proxy',...)
[11:20:30] [CRITICAL] connection timed out to the target URL

[*] shutting down at 11:20:30
  
```

Figura 4.79 SQLi con sqlmap [1], [47]

#### 4.2.5.5. Prueba de inclusión local de archivos (OTG-INPVAL-012)

La figura 4.80 muestra la prueba de LFI con la ayuda de dotdotpwn herramienta incluida en Kali Rolling 2016.2 para realizarla de manera automatizada.

Resultado obtenido:

Dotdotpwn determina que existen páginas vulnerables a LFI.

```

Web.aspx?tipcon=TRAVERSAL:80/../../boot.ini <- VULNERABLE!
Web.aspx?tipcon=TRAVERSAL:80/../../windows/system32/drivers/etc/hosts <- VULNERABLE!
Web.aspx?tipcon=TRAVERSAL:80/../../boot.ini <- VULNERABLE!
Web.aspx?tipcon=TRAVERSAL:80/../../windows/system32/drivers/etc/hosts <- VULNERABLE!
Web.aspx?tipcon=TRAVERSAL:80/../../boot.ini <- VULNERABLE!
Web.aspx?tipcon=TRAVERSAL:80/../../windows/system32/drivers/etc/hosts <- VULNERABLE!
/TipoConsultaWeb.aspx?tipcon=TRAVERSAL:80/../../boot.ini <- VULNERABLE!

```

Figura 4.80 LFI con dotdotpwn

#### 4.2.5.6. Prueba de inyección de comandos (OTG-INPVAL-013)

La figura 4.81 presenta el resultado de la prueba de inyección de comandos que se realizó de manera automatizada.

Resultado obtenido: La prueba no determina resultados referentes a inyección de comandos.

```

Checking connection to the target URL... [ SUCCEEDED ]
Setting the GET parameter 'tipcon' for tests.
Warning: Due to the relatively slow response of 'cmd.exe' in target host, there may be delays during
Testing the classic injection technique... [ FAILED ]
Testing the eval-based code injection technique... [ FAILED ]
Testing the time-based injection technique... [ FAILED ]
Trying to create a file in '\\inetpub\\wwwroot\\ConsultaObligaciones\\'...
Warning: It seems that you don't have permissions to read and/or write files in '\\inetpub\\wwwroot\\Con
Do you want to try the temporary directory (C:\\Windows\\TEMP\\) [Y/n/q] > y
Trying to create a file, in temporary directory (C:\\Windows\\TEMP\\)...
Testing the tempfile-based injection technique... [ 97.7% ] [x] Critical: Connection timed out.
ceback (most recent call last):

```

Figura 4.81 Inyección de comandos con commix

## 4.2.6. RESULTADO DE PRUEBAS: MANEJO DE ERRORES

### 4.2.6.1. Análisis de códigos de error (OTG-ERR-001)

En la figura 4.82 se aprecia el resultado obtenido utilizando el navegador web.

Resultado obtenido: Al revisar el mensaje de error no se encuentra información importante de ningún tipo referente al servidor web, únicamente el código 404 correspondiente a una página no encontrada.

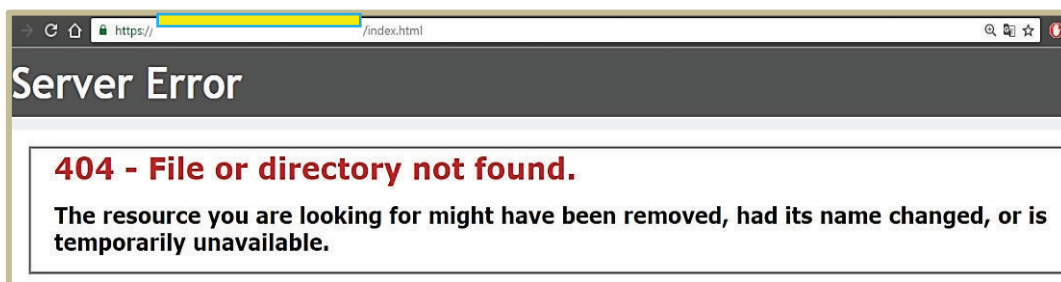


Figura 4.82 Mensaje de error de página inexistente

Por otro lado en la figura 4.83 indica que si se expone información sobre el servidor cuando se utiliza para esta prueba la herramienta telnet. Entre la información más relevante se tiene:

- Versión y tipo de servidor web: IIS 7.5
- Sistema operativo: Microsoft Windows Server
- *Framework*: ASP.NET

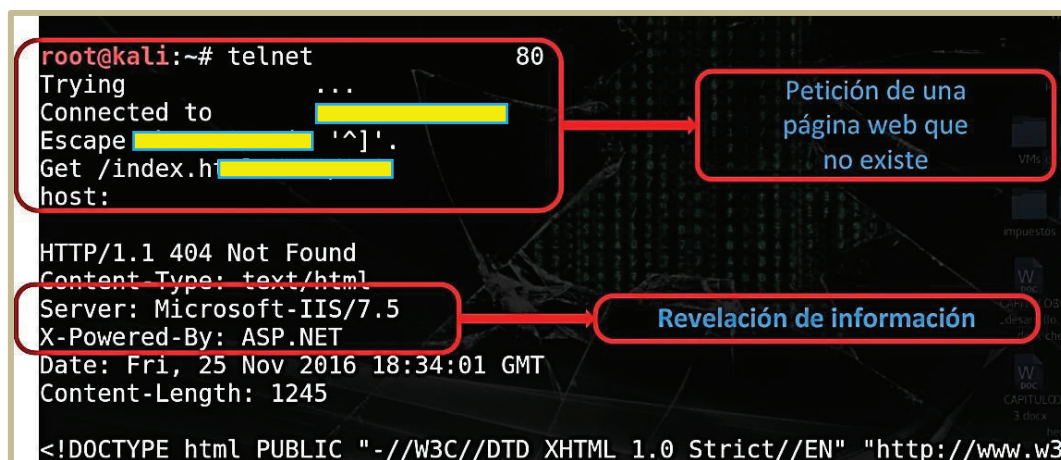


Figura 4.83 Petición de una página inexistente con telnet

## 4.2.7. RESULTADO DE PRUEBAS: CRIPTOGRAFÍA

### 4.2.7.1. Prueba de cifrado SSL/TLS débil y protección insuficiente de capa de transporte (OTG-CRYPST-001)

En la imagen 4.84 se presenta la información que se obtuvo al analizar el objetivo con SSL Server Test. Resultado de la prueba: La aplicación ha implementado el sistema de cifrado SSL/TLS

Protocols	
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3 <b>INSECURE</b>	Yes
SSL 2	No

Cipher Suites (sorted by strength as the server has no preference; deprecated and SSL 2 suites at the end)	
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128

Figura 4.84 Información sobre SSL/TLS

La figura 4.85 lista otra información sobre la implementación de SSL/TLS en servidor web. Resultado de la prueba: La aplicación ha implementado el sistema de cifrado SSL/TLS. Resultado de la prueba: La aplicación ha implementado el sistema de cifrado SSL/TLS

```

* SSLV3 Cipher Suites:
  Preferred:
    RC4-SHA - 128 bits HTTP 403 Forbidden
  Accepted:
    RC4-SHA - 128 bits HTTP 403 Forbidden
    RC4-MD5 - 128 bits HTTP 403 Forbidden
    DES-CBC3-SHA - 112 bits HTTP 403 Forbidden

* TLSV1 Cipher Suites:
  Preferred:
    ECDHE-RSA-AES256-SHA ECDH-256 bits 256 bits HTTP 403 Forbidden
  Accepted:
    ECDHE-RSA-AES256-SHA ECDH-256 bits 256 bits HTTP 403 Forbidden
    DHE-RSA-AES256-SHA DH-1024 bits 256 bits HTTP 403 Forbidden
    AES256-SHA - 256 bits HTTP 403 Forbidden
    ECDHE-RSA-AES128-SHA ECDH-256 bits 128 bits HTTP 403 Forbidden
    DHE-RSA-AES128-SHA DH-1024 bits 128 bits HTTP 403 Forbidden
    RC4-SHA - 128 bits HTTP 403 Forbidden
    RC4-MD5 - 128 bits HTTP 403 Forbidden
    AES128-SHA - 128 bits HTTP 403 Forbidden
    DES-CBC3-SHA - 112 bits HTTP 403 Forbidden

```

Figura 4.85 Información SSL/TLS con sslyze

#### 4.2.7.2. Prueba de información sensible enviada por canales sin encriptar (OTG-CRYPT-003)

La información de esta prueba se muestra en la figura 4.86.

Resultado obtenido: Este resultado permite apreciar que la información que se transmite por la aplicación no viaja en texto claro, para esta se capturó tráfico de red con la herramienta wireshark.

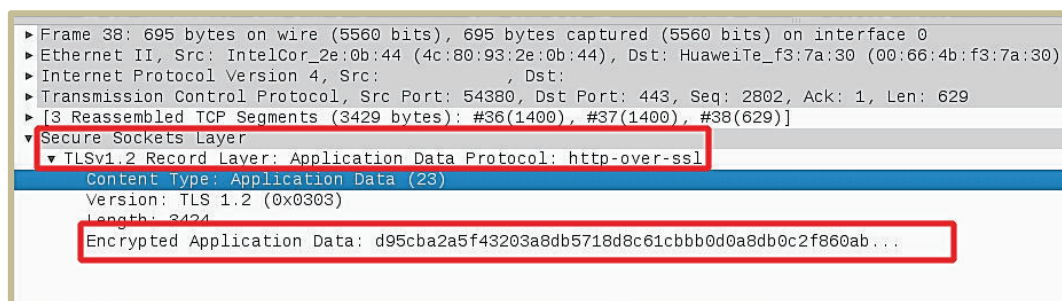


Figura 4.86 Captura de tráfico con wireshark

La fecha y hora de la realización de cada una de las pruebas de penetración se encuentran listadas en el Anexo G.

### 4.3. ANÁLISIS DE RESULTADO PARA EL PORTAL WEB DEL MDMQ

En esta sección se realiza el análisis de resultados, con el fin de determinar si la vulnerabilidad existe o solamente se trata de un falso positivo<sup>57</sup>. En la tabla 4.3 se describe el análisis de resultados en concordancia con los resultados obtenidos.

CATEGORÍA	CÓDIGO REFERENCIA	RESULTADO OBTENIDO
Recopilación de Información	OTG-INFO-001	Se obtuvo información sobre los subdominios relacionados con dominio principal, se realizaron varias consultas avanzadas y se encontró una interfaz administrativa relacionada con un sitio basado en una plantilla Joomla, versiones y tipos de servidores web y páginas con parámetros en la URL susceptibles a XSS e inyección SQL.

<sup>57</sup> Los falsos positivos son hallazgos o pruebas que se consideran verdaderas pero que luego se demuestran falsas.

CATEGORÍA	CÓDIGO REFERENCIA	RESULTADO OBTENIDO
Recopilación de Información	OTG-INFO-002	Los resultados detallan información sobre el tipo y versión del servidor web, también se obtuvo datos sobre el sistema operativo sobre el cual está implementado el servidor web.
	OTG-INFO-003	Se visualizó el meta archivo robots.txt y con eso se pudo determinar que el sitio web está basado en una plantilla Joomla, el archivo también lista los directorios que no se desea que los motores de búsqueda indexen <sup>58</sup> en sus resultados y con esto se puede determinar que existe una interfaz de administración.
	OTG-INFO-004	Los resultados listan una serie de puertos tanto los que se encuentran abiertos, como los que se encuentran cerrados, también se encontró información sobre los nombres y versiones de los servicios que se encuentran instalados y el tipo de sistema operativo.
	OTG-INFO-005	Se encontró comentarios que no revelan información sensible sobre el portal del MDMQ, al revisar los metadatos se obtuvo información del framework de la aplicación y sobre el sistema gestor de contenido.
	OTG-INFO-006	El resultado de esta prueba indica que no existen parámetros en la URL que puedan ser modificados y con eso realizar tareas para las que no ha sido destinado el portal del MDQM. Se encontró la cookie _ga, que no posee información de relevancia.
	OTG-INFO-007	Mediante el proceso de <i>spidering</i> se obtuvo un árbol de directorios y recursos del portal web del MDMQ, particularmente se encontró el meta archivo robots.txt donde se encuentra información sobre el CMS y una interfaz de administración.
	OTG-INFO-008	El resultado de esta indica que se puede obtener información muy relevante como versión y tipo de servidor web, sistema operativo, gestor de contenido, dirección IP y framework de la aplicación web.

<sup>58</sup> Indexar es agregar una o más páginas web a las bases de datos de los buscadores de internet.

CATEGORÍA	CÓDIGO REFERENCIA	RESULTADO OBTENIDO
Recopilación de Información	OTG-INFO-009	Esta prueba revela información sensible sobre, el sistema operativo, gestor de contenido, versión y tipo del servidor web, dirección IP y framework de la aplicación.
Gestión de la Configuración y la Implementación	OTG-CONFIG-001	El objetivo de esta prueba es mostrar la infraestructura que protege a la aplicación web, para saber el nivel de seguridad con el que cuenta, sin embargo por el compromiso de disponibilidad de información el MDMQ no proporcionó un diagrama de red con muchos detalles por lo que no se puede decir que tan protegido está el portal web del MDMQ.
	OTG-CONFIG-002	Los resultados de esta prueba indican que todos los módulos activados en el servidor web son necesarios para cumplir con el debido funcionamiento del portal del MDMQ.
	OTG-CONFIG-004	Se obtuvo información sobre la localización de los registros del servidor web, estos están en sitios personalizados dentro del servidor web. Este dato es importante ya que lo primero que un atacante hace luego de realizar cualquier actividad es borrar evidencia de la misma, evidencia que se encuentra en los registros.
	OTG-CONFIG-005	Se obtuvo acceso a una interfaz de administración Joomla para el portal del MDMQ, pero por el acuerdo de confidencialidad y disponibilidad de información no se logró ingresar como tal ya que no se pudo disponer de las credenciales necesarias para el acceso.
	OTG-CONFIG-006	Los resultados indican que los siguientes métodos han sido implementados: OPTIONS, HEAD, GET y POST.
	OTG-CONFIG-007	Los resultados confirmaron que el mecanismo de seguridad HSTS no se encuentra implementado en el portal web del MDMQ.
	OTG-CONFIG-008	El resultado obtenido en esta prueba indica que la política concede acceso a los recursos Adobe Flash alojados en el servidor, desde cualquier dominio.



CATEGORÍA	CÓDIGO REFERENCIA	RESULTADO OBTENIDO
Autorización	OTG-AUTHZ-001	La prueba realizada de manera automatizada indica que existe una página vulnerable a directorio traversal, sin embargo al realizarla de manera manual se confirma que se trata de un falso positivo.
	OTG-AUTHZ-003	El resultado de la prueba indica que no se puede realizar escalamiento de privilegios tanto horizontal como vertical.
	OTG-AUTHZ-004	Los resultados indican que al modificar parámetros en la URL no se puede acceder a directorios o recursos para los cuales se necesita tener privilegios de nivel superior.
Gestión de Sesiones	OTG-SESS-005	El resultado de la prueba indica que no se puede realizar ataques de CSRF ya que para ello se necesita estar logeado en la aplicación, sistema con el cual no cuenta el portal del MDMQ.
Validación de Datos de Entrada	OTG-INPVAL-001	Los resultados de las pruebas, tanto manuales como automatizadas indican que no se puede inyectar código para realizar ataques de XSS.
	OTG-INPVAL-002	El resultado que se obtuvo de esta prueba indica que no se puede realizar ataques de XSS almacenado, ya que no existe ningún método de guardar información del usuario.
	OTG-INPVAL-003	Con las pruebas realizadas en el servidor web con métodos no implementados se determinó que la solicitud se hizo de manera correcta (código 200), pero en la respuesta se revela información sensible sobre: versión y tipo de servidor web, framework de la aplicación web y sistema operativo.
	OTG-INPVAL-005	El resultado que se obtuvo de las pruebas realizadas, confirmaron que en el portal web del MDMQ no es posible realizar ataques exitosos de inyección SQL.
	OTG-INPVAL-012	La inclusión local de archivos también se refiere a escalamiento vertical de privilegios y path traversal, los resultados ratifican que no es posible realizar ataques de esta índole.
	OTG-INPVAL-013	Esta prueba se realizó de forma automatizada y el resultado indica que no se puede inyectar comando del sistema operativo.

CATEGORÍA	CÓDIGO REFERENCIA	RESULTADO OBTENIDO
Manejo de Errores	OTG-ERR-001	La primera prueba realizada de forma manual en el navegador indica que si se tiene implementadas páginas de error personalizadas, sin embargo, cuando se realizan peticiones de recursos no existente en el servidor mediante la herramienta Telnet en el mensaje de error (código 404) también se observa que se revela información sobre versión y tipo de servidor web, framework de la aplicación y tipo de sistema operativo.
Criptografía	OTG-CRYPST-001	El resultado obtenido de las pruebas indica que el portal web del MDMQ no tiene implementado servicios que utilicen cifrado SSL/TLS.
	OTG-CRYPST-003	El resultado obtenido en la prueba de cifrado SSL/TLS y el reporte del escáner Nessus confirman que la información que se envía a través del portal web del MDMQ viaja en texto claro, esto supone una riesgo alto ya que al ingresar las credenciales en la interfaz de administración éstas podrían ser visualizadas sin ningún problema si alguien ha capturado el tráfico en el momento de la autenticación.

**Tabla 4.3 Análisis de resultados portal MDMQ**

#### 4.4. ANÁLISIS DE RESULTADO PARA EL PORTAL DE PAGO DE IMPUESTOS POR INTERNET

En esta sección se realiza el análisis de resultados, con el fin de determinar si la vulnerabilidad existe o solamente se trata de un falso positivo. En la tabla 4.4 se describe el análisis de resultados en concordancia con los resultados obtenidos.

CATEGORÍA	CÓDIGO REFERENCIA	RESULTADO OBTENIDO
Recopilación de Información	OTG-INFO-001	Se obtuvo información sobre los subdominios relacionados con dominio principal, se realizaron varias consultas avanzadas y no se encontraron interfaces administrativas, versiones o tipos de servidores web. Se encontraron páginas con parámetros en la URL susceptibles a XSS e inyección SQL, esto quiere decir que estos parámetros pueden ser modificados para inyectar código y realizar dichos ataques.

CATEGORÍA	CÓDIGO REFERENCIA	RESULTADO OBTENIDO
Recopilación de Información	OTG-INFO-002	Los resultados detallan información sobre el tipo y versión del servidor web, también se obtuvo datos sobre el sistema operativo sobre el cual esta implementado el servidor web.
	OTG-INFO-003	El resultado de la prueba no visualizó meta archivos importantes como el robots.txt, con esa información no se pudo determinar si el sitio web está basado en una plantilla Joomla, WordPress, Drupal o cualquier CMS, por lo cual tampoco se detectó ninguna interfaz de administración.
	OTG-INFO-004	Los resultados listan una serie de puertos tanto los que se encuentran abiertos, como los que se encuentran cerrados, también se encontró información sobre los nombres y versiones de los servicios que se encuentran instalados y el tipo de sistema operativo.
	OTG-INFO-005	Se encontró comentarios que no revelan información sensible sobre el objetivo de estudio, al revisar los metadatos se obtuvo información del framework de la aplicación.
	OTG-INFO-006	El resultado de esta prueba indica que existen parámetros interesantes en la URL, idubro, idrub, desrub, pago, fpago, trans, coopro, referentes al pago del impuesto, estos se modificaron pero no se logró realizar tareas para las que no ha sido destinada la aplicación web. Se encontró la cookie _ga, _utma, _utmz, ASP.NET_Sessionid <sup>59</sup> , que no posee información de relevancia.
	OTG-INFO-007	Mediante el proceso de <i>spidering</i> se obtuvo un árbol de directorios y recursos de la aplicación web, no se localizó meta archivos ni interfaz de administración.
	OTG-INFO-008	El resultado de esta indica que se puede obtener información muy relevante como versión y tipo de servidor web, sistema operativo, dirección IP y framework de la aplicación web.
	OTG-INFO-009	Esta prueba revela información sensible sobre, el sistema operativo, versión y tipo del servidor web, dirección IP y framework de la aplicación.

<sup>59</sup> El SessionID se usa para identificar de forma única un explorador con datos de la sesión en el servidor.

CATEGORÍA	CÓDIGO REFERENCIA	RESULTADO OBTENIDO
Gestión de la Configuración y la Implementación	OTG-CONFIG-001	El objetivo de esta prueba es mostrar la infraestructura que protege a la aplicación web, para saber el nivel de seguridad con el que cuenta, sin embargo por el compromiso de disponibilidad de información el MDMQ no proporcionó un diagrama de red detallado por lo que no se puede el grado de protección con el que cuenta esta aplicación web del MDMQ.
	OTG-CONFIG-002	Los resultados de esta prueba indican que todos los features activados en el servidor web son necesarios para cumplir con el debido funcionamiento de la aplicación web.
	OTG-CONFIG-004	Se obtuvo información sobre la localización de los registros del servidor web, estos están en sitios personalizados dentro del servidor web.
	OTG-CONFIG-005	El resultado de esta prueba indica que no existen interfaces administrativas de CMS conocidos, como son: Joomla, Drupal o WordPress.
	OTG-CONFIG-006	Los resultados indican que los siguientes métodos han sido implementados: TRACE, HEAD, GET y POST.
	OTG-CONFIG-007	Los resultados confirmaron que el mecanismo de seguridad HSTS no se encuentra implementado en la aplicación web del MDMQ.
	OTG-CONFIG-008	El resultado obtenido en esta prueba indica que no existe ningún archivo de política de dominio cruzado.
	Autorización	OTG-AUTHZ-001
OTG-AUTHZ-003		El resultado de la prueba indica que no se puede realizar escalamiento de privilegios tanto horizontal como vertical.
OTG-AUTHZ-004		Los resultados indican que al modificar parámetros en la URL no se puede acceder a directorios o recursos para los cuales se necesita tener privilegios de nivel superior.
Gestión de Sesiones	OTG-SESS-005	El resultado de la prueba indica que no se puede realizar ataques de CSRF ya que para ello se necesita estar logeado en la aplicación, sistema con el cual no cuenta esta aplicación web del MDMQ.

CATEGORÍA	CÓDIGO REFERENCIA	RESULTADO OBTENIDO
Validación de Datos de Entrada	OTG-INPVAL-001	Los resultados de las pruebas, tanto manuales como automatizadas indican que no se puede inyectar código para realizar ataques de XSS.
	OTG-INPVAL-002	El resultado que se obtuvo de esta prueba indica que no se puede realizar ataques de XSS almacenado, ya que no existe ningún método de guardar información del usuario.
	OTG-INPVAL-003	Con las pruebas realizadas en el servidor web con métodos no implementados se determinó los códigos 501 <sup>60</sup> y 411 <sup>61</sup> respectivamente, pero en la respuesta se revela información sensible sobre: versión y tipo de servidor web, framework de la aplicación web y sistema operativo.
	OTG-INPVAL-005	El resultado que se obtuvo de las pruebas realizadas, confirmaron que en la aplicación web del MDMQ no es posible realizar ataques de inyección SQL.
	OTG-INPVAL-012	La inclusión local de archivos también se refiere a escalamiento vertical de privilegios y path traversal, los resultados ratifican que no es posible realizar ataques de esta índole.
	OTG-INPVAL-013	Esta prueba se realizó de forma automatizada y el resultado indica que no se puede inyectar comandos del sistema operativo.
Manejo de Errores	OTG-ERR-001	La primera prueba realizada de forma manual en el navegador indica que si se tiene implementadas páginas de error personalizadas, sin embargo, cuando se realizan peticiones de recursos no existente en el servidor mediante la herramienta Telnet en el mensaje de error (código 404) también se observa que se revela información sobre versión y tipo de servidor web, framework de la aplicación y tipo de sistema operativo.
Criptografía	OTG-CRYPST-001	El resultado obtenido de las pruebas indica que el portal web del MDMQ si tiene implementado servicios que utilicen cifrado SSL/TLS.

<sup>60</sup> *Not Implemented*: El servidor no soporta alguna funcionalidad.

<sup>61</sup> *Length Required*: El servidor rechaza la petición del navegador porque no incluye la cabecera Content-Length adecuada.

CATEGORÍA	CÓDIGO REFERENCIA	RESULTADO OBTENIDO
Criptografía	OTG-CRYPST-003	El resultado obtenido en la prueba de cifrado SSL/TLS, el reporte del escáner Nessus y captura de tráfico de red con la herramienta wireshark confirman que la información que se envía a través de la aplicación web del MDMQ no viaja en texto claro.

Tabla 4.4 Análisis de resultados Pago de Impuestos por Internet

#### 4.5. MITIGACIÓN DE VULNERABILIDADES PARA EL PORTAL WEB DEL MDMQ

En la tabla 4.5 se listan las formas de mitigar las vulnerabilidades encontradas durante la fase de análisis de resultados.

CATEGORÍA	CÓDIGO REFERENCIA	VULNERABILIDAD	MITIGACIÓN
Recopilación de Información	OTG-INFO-001	Revelación de información	Considerar la importancia y criticidad de la información antes de ser publicada en línea.[1]
	OTG-INFO-002	Revelación de información	Ofuscar <sup>62</sup> los encabezados del servidor web de la capa de presentación [1]
	OTG-INFO-003	Revelación de meta archivos	Redireccionar los recursos a un error 404 <sup>63</sup> modificando el archivo .htaccess <b>Redirect 404 /antiguodestino</b> o prohibir la indexación del fichero con la meta etiqueta <b>meta name="robots" content="noindex"</b> . [50] [51]
	OTG-INFO-004	Enumeración de puertos	Esconder los servicios cambiando el número de puerto a la escucha, también se puede dificultar el escaneo implementando políticas en IPTABLES o abrir puertos exclusivamente necesarios.[52]-[54]
	OTG-INFO-005	Revelación de meta datos	Eliminar u ocultar la línea que contenga el metadato que revele la información sensible del código fuente de la página web. [55], [56]

<sup>62</sup> Encubrir el significado de una comunicación haciéndola más confusa y complicada de interpretar.

<sup>63</sup> Recurso no encontrado. Se utiliza cuando el servidor web no encuentra la página o recurso solicitado.

CATEGORÍA	CÓDIGO REFERENCIA	VULNERABILIDAD	MITIGACIÓN
Recopilación de Información	OTG-INFO-007	Enumeración de directorios	En cada directorio que no se quiere la indexación crear un archivo <b>index.html</b>   <b>index.php</b>   <b>index.htm</b> , redireccionar a otro destino mediante el archivo <b>.htaccess</b> <b>Redirect 404 /antiguodestino.</b> [51], [57]
	OTG-INFO-008	Revelación de información	Revisar la configuración y ofuscar o deshabilitar todo en la cabecera HTTP que revele información. Manualmente remover todo el contenido en el código HTML que pueda contener información sensible.[1]
	OTG-INFO-009	Revelación de información	Revisar la configuración y ofuscar o deshabilitar todo en la cabecera HTTP que revele información. Manualmente remover todo el contenido en el código HTML que pueda contener información sensible.[1]
Gestión de la configuración y la implementación	OTG-CONFIG-005	Acceso a interfaz de administración	Redireccionar los recursos a un error 404 modificando el archivo <b>.htaccess</b> <b>Redirect 404 /interfaz-admin</b> , cambiar la dirección de la interfaz para que no sea tan fácil de localizar. [51]
	OTG-CONFIG-007	HSTS no implementado	Modificar el archivo <b>httpd.conf</b> y habilitar el módulo de cabeceras <b>mod_headers.so</b> , luego se agrega al virtual host un tiempo de validez para la política STS <b>&lt;VirtualHost IP_de_Host:443&gt;</b> <b>Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains;"</b> <b>&lt;/VirtualHost&gt;</b> [58]
	OTG-CONFIG-008	Política de dominio cruzado expuesta	Política muy permisiva, debería configurarse con el principio de privilegios mínimos.[59]
Validación de datos de entrada	OTG-INPVAL-003	Métodos HTTP permitidos	Editar el archivo de configuración <b>httpd.conf</b> y desactivar el método <b>TraceEnable Off.</b> [60]
Manejo de errores	OTG-ERR-001	Revelación de información	Las respuestas de errores se pueden configurar y personalizar en el servidor web con la directiva <b>ErrorDocument</b> <b>ErrorDocument 404 "Customized Not Found error message"</b> También se gestionan errores utilizando el archivo <b>.htaccess</b> o usando las directivas <b>ServerTokens</b> y <b>ServerSignature</b> en el archivo de configuración de Apache. [1], [51], [61]
Criptografía	OTG-CRYPST-001	Cifrado SSL/TLS débil	Configurar apropiadamente los protocolos SSL/TLS.[1]

CATEGORÍA	CÓDIGO REFERENCIA	VULNERABILIDAD	MITIGACIÓN
Criptografía	OTG-CRYPST-003	Información se transporta en texto claro	Configurar apropiadamente los protocolos SSL/TLS y el cifrado de datos.[1]

Tabla 4.5 Remediación de vulnerabilidad del portal del MDMQ

#### 4.6. MITIGACIÓN DE VULNERABILIDADES PARA EL PORTAL DE PAGO DE IMPUESTOS POR INTERNET

En la tabla 4.6 se listan las formas de mitigar las vulnerabilidades encontradas durante la fase de análisis de resultados.

CATEGORÍA	CÓDIGO REFERENCIA	VULNERABILIDAD	MITIGACIÓN
Recopilación de Información	OTG-INFO-001	Revelación de información	Considerar la importancia y criticidad de la información antes de ser publicada en línea. [1]
	OTG-INFO-002	Revelación de información	Ofuscar los encabezados del servidor web de la capa de presentación. [1]
	OTG-INFO-004	Enumeración de puertos	Esconder los servicios cambiando el número de puerto a la escucha y deshabilitar los puertos que estén innecesariamente abiertos. [52]-[54]
	OTG-INFO-005	Revelación de meta datos	Eliminar la línea que contenga el metadato que revele la información sensible del código fuente de la página web. [55], [56]
	OTG-INFO-007	Enumeración de directorios	Mediante el panel de control de IIS se coloca en el directorio que se quiere evitar la enumeración de directorios y en la opción examen de directorio se escoge la opción deshabilitar. [57]
	OTG-INFO-008	Revelación de información	Revisar la configuración y ofuscar o deshabilitar todo en la cabecera HTTP que revele información. Manualmente remover todo el contenido en el código HTML que pueda contener información sensible. [1], [55], [56]
	OTG-INFO-009	Revelación de información	Revisar la configuración y ofuscar o deshabilitar todo en la cabecera HTTP que revele información. Manualmente remover todo el contenido en el código HTML que pueda contener información sensible. [1], [55], [56]



CATEGORÍA	CÓDIGO REFERENCIA	VULNERABILIDAD	MITIGACIÓN
Gestión de la Configuración y la Implementación	OTG-CONFIG-006	Métodos HTTP permitidos	Deshabilitar el método TRACE, instalar la herramienta UrlScan la cual restringe las peticiones HTTP que pueden llegar al servidor IIS. [62], [63]
	OTG-CONFIG-007	HSTS no implementado	<p>Editar el archivo de configuración system.webServer y agregar la política STS</p> <pre>&lt;system.webServer&gt; &lt;httpProtocol&gt; &lt;customHeaders&gt; &lt;add name="Strict-Transport-Security" value="max-age=31536000"/&gt; &lt;/customHeaders&gt; &lt;/httpProtocol&gt; &lt;/system.webServer&gt; [29], [64], [65]</pre>
Validación de Datos de Entrada	OTG-INPVAL-003	Métodos HTTP permitidos	Deshabilitar el método TRACE, instalar la herramienta UrlScan la cual restringe las peticiones HTTP que pueden llegar al servidor IIS. [29], [62], [63]
Manejo de Errores	OTG-ERR-001	Revelación de información	<p>Modificar la configuración de Web.config en la sección de errores.</p> <pre><b>&lt;customErrors defaultRedirect="myerrorpagedefault.aspx" mode="On RemoteOnly"&gt; &lt;error statusCode="404" redirect="myerrorpagefor404.aspx"/&gt; &lt;error statusCode="500" redirect="myerrorpagefor500.aspx"/&gt; &lt;/customErrors&gt;</b></pre> <p>Modo "On" activará los errores y el modo "RemoteOnly" mostrará los errores personalizados solo a los usuarios remotos a la aplicación. [29], [66], [67]</p>

Tabla 4.6 Remediación de vulnerabilidad para Pago de Impuestos por Internet

#### 4.7. VULNERABILIDADES ENCONTRADAS, COMANDOS Y HERRAMIENTAS UTILIZADAS EN EL DESARROLLO DEL TRABAJO [68]

En las tablas 4.6 y 4.7 se detallan las pruebas, vulnerabilidades encontradas y las herramientas utilizadas en el desarrollo del presente trabajo, respectivamente del portal web del MDMQ y del portal de pagos por Internet. Mientras que la tabla 4.8 muestra vulnerabilidades conocidas para los sistemas operativos y versiones de software encontrados.

CATEGORÍA	CODIGO PRUEBA	NOMBRE DE LA PRUEBA	VULNERABILIDAD	HERRAMIENTA UTILIZADA
Recopilación de Información	OTG-INFO-001	Descubrimiento con motores de y reconocimiento por fugas de información	Revelación de información	google, mozilla firefox
	OTG-INFO-002	Fingerprint del servidor web	Revelación de información	httprint, greghatcher.com
	OTG-INFO-003	Revisión de meta-archivos por fugas de información	Revelación de meta archivos	wget, mozilla firefox
	OTG-INFO-004	Enumerar aplicaciones en el servidor web	Enumeración de puertos	nmap, nessus
	OTG-INFO-005	Revisar comentarios en la página web y metadatos por fugas de información	Revelación de meta datos	mozilla firefox, desenmascara.me
	OTG-INFO-006	Identificar los puntos de entrada de la aplicación	N/E	burp suite
	OTG-INFO-007	Mapear rutas de ejecución a través de la aplicación	Enumeración de directorios	burp suite, owasp zap
	OTG-INFO-008	Fingerprint el framework de la aplicación web	Revelación de información	whatweb
	OTG-INFO-009	Fingerprint a la aplicación web	Revelación de información	wappalyzer, whatweb

CATEGORÍA	CÓDIGO PRUEBA	NOMBRE DE LA PRUEBA	VULNERABILIDAD	HERRAMIENTA UTILIZADA
Gestión de la Configuración y la Implementación	OTG-CONFIG-001	Prueba de configuración de red/infraestructura	N/E	N/A
	OTG-CONFIG-002	Prueba de configuración de la plataforma de la aplicación	N/E	N/A
	OTG-CONFIG-004	Archivos de backup y no referenciados con información sensible	N/E	N/A
	OTG-CONFIG-005	Enumerar interfaces de administración de aplicaciones y de infraestructura	Acceso a interfaz de administración	mozilla firefox, owasp zap
	OTG-CONFIG-006	Prueba de métodos HTTP	N/E	nmap, nessus
	OTG-CONFIG-007	Prueba de seguridad de transporte estricto HTTP - HSTS	HSTS no implementado	curl, ssl test server
	OTG-CONFIG-008	Prueba de política de dominio cruzado RIA	Política de dominio cruzado expuesta	mozilla firefox
	OTG-AUTHZ-001	Prueba de directorio/path traversal	N/E	dotdotpwn, mozilla firefox
Autorización	OTG-AUTHZ-003	Prueba de escalamiento de privilegios	N/A	N/A
	OTG-AUTHZ-004	Prueba de referencia directa insegura a objetos	N/E	mozilla firefox
	OTG-SESS-005	Prueba de falsificación de peticiones en sitios cruzados CSRF	N/A	N/A
Validación de Datos de Entrada	OTG-INPVAL-001	Prueba de <i>Cross Site Scripting</i> reflejado	N/E	xsser, mozilla firefox

CATEGORÍA	CÓDIGO PRUEBA	NOMBRE DE LA PRUEBA	VULNERABILIDAD	HERRAMIENTA UTILIZADA
Validación de Datos de Entrada	OTG-INPVAL-002	Prueba de Cross Site Scripting almacenado	N/A	N/A
	OTG-INPVAL-003	Prueba de manipulación de métodos HTTP	Métodos HTTP permitidos	telnet, netcat
	OTG-INPVAL-005	Prueba de inyección SQL	N/E	mozilla firefox, sqlmap
	OTG-INPVAL-012	Prueba de inclusión local de archivos	N/E	dotdotpwn, mozilla firefox
	OTG-INPVAL-013	Prueba de inyección de comandos	N/E	commix
Manejo de Errores	OTG-ERR-001	Análisis de códigos de error	Revelación de información	telnet, mozilla firefox
	OTG-CRYPST-001	Prueba de cifrado ssl/tls débil y protección insuficiente de capa de transporte	Cifrado SSL/TLS débil	nmap, mozilla firefox
Criptografía	OTG-CRYPST-003	Prueba de información sensible enviada por canales sin encriptar	Información se transporta en texto claro	nessus

**Tabla 4.6 Vulnerabilidades encontradas, herramientas utilizadas portal web MDMQ**

CATEGORÍA	CODIGO PRUEBA	NOMBRE DE LA PRUEBA	VULNERABILIDAD	HERRAMIENTA UTILIZADA
Recopilación de Información	OTG-INFO-001	Descubrimiento con motores de y reconocimiento por fugas de información	Revelación de información	google, mozilla firefox
	OTG-INFO-002	Fingerprint del servidor web	Revelación de información	httprint, wappalyzer
	OTG-INFO-003	Revisión de meta-archivos por fugas de información	N/E	wget, owasp zap
	OTG-INFO-004	Enumerar aplicaciones en el servidor web	Enumeración de puertos	nmap, nessus
	OTG-INFO-005	Revisar comentarios en la página web y metadatos por fugas de información	Revelación de meta datos	mozilla firefox, desenmascara.me
	OTG-INFO-006	Identificar los puntos de entrada de la aplicación	N/E	burp suite
	OTG-INFO-007	Mapear rutas de ejecución a través de la aplicación	Enumeración de directorios	burp suite, owasp zap
	OTG-INFO-008	Fingerprint el framework de la aplicación web	Revelación de información	whatweb
	OTG-INFO-009	Fingerprint a la aplicación web	Revelación de información	builtwith.com, whatweb
Gestión de la Configuración y la Implementación	OTG-CONFIG-001	Prueba de configuración de red/infraestructura	N/E	N/A
	OTG-CONFIG-002	Prueba de configuración de la plataforma de la aplicación	N/E	N/A
	OTG-CONFIG-004	Archivos de backup y no referenciados con información sensible	N/E	N/A
	OTG-CONFIG-005	Enumerar interfaces de administración de aplicaciones y de infraestructura	N/E	mozilla firefox, owasp zap

CATEGORÍA	CÓDIGO PRUEBA	NOMBRE DE LA PRUEBA	VULNERABILIDAD	HERRAMIENTA UTILIZADA
Gestión de la Configuración y la Implementación	OTG-CONFIG-006	Prueba de métodos HTTP	Métodos HTTP permitidos	nmap
	OTG-CONFIG-007	Prueba de seguridad de transporte estricto HTTP - HSTS	HSTS no implementado	curl, ssl test server
	OTG-CONFIG-008	Prueba de política de dominio cruzado RIA	N/E	mozilla firefox
Autorización	OTG-AUTHZ-001	Prueba de directorio/path traversal	N/E	dotdotpwn, mozilla firefox
	OTG-AUTHZ-003	Prueba de escalamiento de privilegios	N/A	N/A
	OTG-AUTHZ-004	Prueba de referencia directa insegura a objetos	N/E	mozilla firefox
	OTG-SESS-005	Prueba de falsificación de peticiones en sitios cruzados CSRF	N/A	N/A
Validación de Datos de Entrada	OTG-INPVAL-001	Prueba de Cross Site Scripting reflejado	N/E	xsser, mozilla firefox
	OTG-INPVAL-002	Prueba de Cross Site Scripting almacenado	N/A	N/A
	OTG-INPVAL-003	Prueba de manipulación de métodos HTTP	Métodos HTTP permitidos	telnet
	OTG-INPVAL-005	Prueba de inyección SQL	N/E	mozilla firefox, sqlmap
	OTG-INPVAL-012	Prueba de inclusión local de archivos	N/E	dotdotpwn, mozilla firefox
Manejo de Errores	OTG-INPVAL-013	Prueba de inyección de comandos	N/E	commix
	OTG-ERR-001	Análisis de códigos de error	Revelación de información	telnet, mozilla firefox

CATEGORÍA	CÓDIGO PRUEBA	NOMBRE DE LA PRUEBA	VULNERABILIDAD	HERRAMIENTA UTILIZADA
Criptografía	OTG-CRYPST-001	Prueba de cifrado ssl/tls débil y protección insuficiente de capa de transporte	N/E	sslyze, ssl test server
	OTG-CRYPST-003	Prueba de información sensible enviada por canales sin encriptar	N/E	nessus, wireshark

Tabla 4.7 Vulnerabilidades encontradas, herramientas utilizadas portal pagos por Internet

SOFTWARE	CVE	TIPO	EXPLOIT	MITIGACIÓN
Apache 2.4.6	CVE-2016-5387	Security bypass	No existe	Actualizar a última versión [69]
	CVE-2014-3523	DoS	No existe	Actualizar a última versión [70]
Windows Server 2008 R2	CVE-2017-0004	DoS	No existe	Actualización 3212642 [71]
	CVE-2013-0075	DoS	No existe	Actualización Windows6.0-KB2790655-x64.msu [72]
	CVE-2012-2556	Ejecución de comando	No existe	Actualización Windows6.0-KB2753842-v2-x64.msu y Windows6.0-KB2779030-x64.msu [73]
PHP 5.4.16	CVE-2016-7478	DoS	No existe	Actualizar a última versión [74]
	CVE-2015-8876	DoS	No existe	Actualizar a última versión [75]
IIS 7.5	CVE-2015-0231	Ejecución de comando	No existe	Actualizar a última versión [76]
	CVE-2010-3972	DoS	No existe	Actualización Windows6.1-KB2489256-x64.msu [77]
	CVE-2010-2730	Ejecución de comando	No existe	Actualización Windows6.0-KB2124261-x64.msu [78]

<b>SOFTWARE</b>	<b>CVE</b>	<b>TIPO</b>	<b>EXPLOIT</b>	<b>MITIGACIÓN</b>
IIS 7.5	CVE-2010-1899	DoS	No existe	Actualización Windows6.0-KB2124261-x64.msu [79]
VSFTPD 3.0.2	CVE-2015-1419	Security bypass	No existe	Actualizar a última versión [80]
	CVE-2004-2259	DoS	No existe	Actualizar a última versión [81]
MySQL 5.5.44	CVE-2015-4819	Info	No existe	Actualizar a última versión [82]
	CVE-2015-4879	Info	No existe	Actualizar a última versión [83]

**Tabla 4.8 Vulnerabilidades conocidas para el software encontrado en las pruebas de seguridad**



## CAPÍTULO 5

### CONCLUSIONES Y RECOMENDACIONES

Una vez culminadas las pruebas de penetración y realizado el respectivo análisis de vulnerabilidades encontradas en las aplicaciones web del MDMQ, se concluye y recomienda lo siguiente:

#### 5.1. CONCLUSIONES

- Las pruebas de penetración realizado a las aplicaciones web que presta el MDMQ se realizó porque actualmente las aplicaciones y portales web de las organizaciones no cuentan con un nivel de seguridad aceptable, por lo que la información que se intercambia por ellas se encuentra expuesta a las amenazas y atacantes que se encuentran en el Internet.
- El Municipio del Distrito Metropolitano de Quito cuenta con una dependencia la cual es la responsable de manejar la infraestructura informática del MDMQ, esta cuenta con los mecanismos y dispositivos de seguridad que permitan detectar intrusiones y ataques, también ha instaurado controles, políticas y buenas prácticas para mejorar la Seguridad de la Información. Sin embargo, el MDMQ ha sufrido incidentes de seguridad, es por eso que se realizaron las pruebas de penetración con el propósito de identificar si existen o no vulnerabilidades en las aplicaciones web que presta el MDMQ.
- Existen varias metodologías para realizar pruebas de seguridad, pruebas de penetración y evaluaciones de seguridad en redes, como OSSTMM, ISSAF, NIST800-115, PTES Sin embargo, varios de los servicios y aplicaciones que presta el MDMQ son a través de Internet, es por esta razón que utilizó la Guía *Open Web Application Security Project (OWASP) V4*.

- La guía de pruebas OWASP V4 detalla alrededor de 90 pruebas y procedimientos para realizar una evaluación de seguridad en aplicaciones y portales web, así como las herramientas que podrían ser utilizadas para ejecutar cada una de ellas, incluso se puede encontrar en algunas de ellas la forma de remediar la vulnerabilidad en caso de ser encontrada. Sin embargo, en el presente trabajo no se efectuaron todas, ya que ciertas pruebas de la guía no podían ser ejecutadas a la aplicación y portal web que fueron auditados, por cuestiones de su programación y funcionalidad. Por ejemplo, las pruebas referentes a autenticación de la sección OTG-AUTHN y las de manejo de cuentas de usuario de la sección OTG-IDENT, no fueron realizadas porque no existen estos mecanismos implementados en las aplicaciones web auditadas.
- Kali Rolling 2016.2 es un sistema operativo libre, excelente para realizar pruebas de penetración, hacking ético y evaluaciones de seguridad en la red. Cuenta con herramientas de tipo open source, las cuales ayudaron al desarrollo del trabajo. Sin embargo, estas tienen limitantes respecto a las herramientas de pago, ya que estas contienen ciertas funcionalidades adicionales que podrían facilitar aún más el trabajo y presentar los resultados de una manera más comprensible. Por ejemplo Burp Suite, un proxy que ayudó al *spidering* y análisis de solicitudes, consta con un escáner de vulnerabilidades, analizador de contenido, y también puede programar las tareas. Todo esto en su versión de pago; esto habría facilitado la realización del trabajo. En Kali Rolling la mayoría de herramientas no cuentan con interfaz gráfica dificultando su uso.
- El Departamento de Informática del MDMQ generó un compromiso de confidencialidad y disponibilidad sobre la información que podía o no ser compartida para la elaboración del presente trabajo. Es por esta razón que ciertas pruebas de seguridad no se llevaron a cabo, ya sea por la falta de información, o por la criticidad del recurso a ser auditado y su necesaria

continuidad con el trabajo para el cual ha sido implementado. En este caso no se pudo realizar la prueba de denegación de servicio.

- Una vez terminadas las pruebas de penetración, con los resultados obtenidos en las pruebas y su debido análisis se pudo determinar la existencia de vulnerabilidades en las aplicaciones web que presta el MDMQ. También se pudo identificar la presencia de falsos positivos. La mayoría de vulnerabilidades encontradas fue revelación de información, versiones y tipos de software. Mientras que el falso positivo se dió en la prueba OTG-AUTHZ-001 correspondiente al ataque de ruta transversal utilizando la herramienta dotdotpwn.

## **5.2. RECOMENDACIONES**

- Se recomienda al Departamento de Informática del MDMQ crear una dependencia para la Seguridad de la Información cuyas funciones sean, encargarse de los incidentes de seguridad, mitigar, reducir o transferir los mismos. Además de formular normas y políticas para un uso seguro de la información y las tecnologías de la información.
- Se recomienda al Departamento de Informática del MDMQ implantar un Sistema de Gestión de Seguridad de la Información, el cual crea controles y procedimientos que ayudan a gestionar incidentes de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información, y en conjunto con el Departamento de Seguridad de la Información hacer que las aplicaciones web y la red corporativa del MDMQ sean más segura.
- Se recomienda al MDMQ por ser una entidad de administración pública implemente el Esquema Gubernamental de Seguridad de la Información (EGSI), elaborado en base a la Norma NTE INEN-ISO/IEC 27002, el cual promueve la estandarización de procesos, políticas, procedimientos para

mejorar la calidad de tecnologías de la información y mantener la seguridad de la información.

- Se recomienda al MDMQ para futuras pruebas de penetración a los servicios y aplicaciones que presta a través de Internet tomar en cuenta la Guía OWASP V4, ya que en ella se detallan los procedimientos a realizar y herramientas que se pueden utilizar, específicamente para aplicaciones y portales web.
- La seguridad en el funcionamiento y desempeño de la aplicación web parte desde la etapa de desarrollo, por consiguiente se recomienda tomar en cuenta los lineamientos de la Guía OWASP V4, no solo para la realización de las pruebas de seguridad, sino también para el desarrollo, mantenimiento de aplicaciones y portales web seguros.
- Antes de ejecutar las pruebas que se encuentran detalladas en la Guía OWASP V4, es recomendable descartar todas aquellas que no se adaptan a la lógica o a la funcionalidad para la que fue desarrollada la aplicación web, ya que al realizar pruebas que no van a producir resultados, implica pérdida de tiempo y dinero.
- Es recomendable por lo menos tomar en cuenta el Top Ten de OWASP para las pruebas de seguridad dentro de una organización, este documento detalla 10 de las vulnerabilidades más importantes que presentan las aplicaciones web.
- Se recomienda hacer pruebas de penetración no solo a aplicaciones web, sino también a los sistemas informáticos e incluso al recurso humano con la ayuda de la Ingeniería Social, para reducir riesgos, e identificar vulnerabilidades.
- En el caso de ser pruebas de penetración de caja blanca. Se recomienda a la organización que está siendo auditada proveer la información necesaria al

analista de seguridad para realizar todas las pruebas que han sido consideradas para el mismo, de no ser así se podrían dejar vulnerabilidades sin identificar. Por ejemplo, la Denegación de Servicio, un ataque que ser realizado en cualquier momento.

- Se recomienda al Departamento de Informática del MDMQ tomar en cuenta los métodos de remediación para reducir y mitigar las vulnerabilidades encontradas.

## REFERENCIAS BIBLIOGRÁFICAS

- [1] OWASP (2014, Septiembre). "OWASP Testig Guide". [Documento PDF]. Versión 4.0 Obtenido en:<https://www.owasp.org/images/1/19/OTGv4.pdf> [2016, 10 Octubre].
- [2] J. Muniz, A. Lakhani (2013, Septiembre). "Web Penetration Testing With Kali Linux". [Documento PDF]. Obtenido en:<ftp://lab.dnict.vn/1.DNICT/2.Ebooks/books/Web%20Penetration%20Testing%20with%20Kali%20Linux.pdf> [2016, 10 Octubre].
- [3] Municipio del Distrito Metropolitano de Quito, "Manual Orgánico Funcional", Secretaría General de Planificación, Quito - Ecuador, Resolución No. A0010, Dic. 2012.
- [4] FLORES, Fanny Paulina. Diseño de un Sistema de Gestión de Seguridad de la Información para la empresa MEGADATOS S.A. en la ciudad de Quito, aplicando las Normas ISO 27001 e ISO 27002, Facultad de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional, Ecuador, 2010.
- [5] *INTERNATIONAL STANDARD ISO/IEC 27001, Information technology – Security techniques – Code of practice for information security controls*, Second edition, 2013.
- [6] COELLO, María Grabirela. Procedimiento Formal de Ethical Hacking para la infraestructura tecnológica de los servicios por internet de la Banca Ecuatoriana, Facultad de Sistemas, Escuela Politécnica Nacional, Ecuador, 2012.
- [7] IZA, Shirla Freycy. Diseño de un Toolkit de Pruebas de Intrusión basado en OSSTMM, Facultad de Sistemas, Escuela Politécnica Nacional, Ecuador, 2015.

- [8] Aakbar Rubaiyyat (2016, Agosto). "Overview of Information Security for New (and non-IT) Project Managers". [En Línea]. Disponible en: <https://www.linkedin.com/pulse/overview-information-security-new-non-it-project-managers-aakbar> [2016, 23 Septiembre].
- [9] Municipio del Distrito Metropolitano de Quito, "Declaración de Aplicabilidad – ISO/IEC 27001". Dirección Metropolitana de Informática, Quito - Ecuador, Ene. 2015.
- [10] Raúl Siles (2008, Marzo). "Seguridad en Aplicaciones Web". [Documento PDF]. Obtenido en: [https://www.owasp.org/images/b/be/OWASP\\_III\\_Amenazas\\_e\\_incidentes\\_en\\_aplicaciones\\_Web\\_v2.0\\_RaulSiles.pdf](https://www.owasp.org/images/b/be/OWASP_III_Amenazas_e_incidentes_en_aplicaciones_Web_v2.0_RaulSiles.pdf) [2016, 23 Septiembre].
- [11] René Guamán Quinche (2011). "Seguridad en Entornos Web para Sistemas de Gestión Académica". [Documento PDF]. Obtenido en: <http://repositorio.educacionsuperior.gob.ec/bitstream/28000/120/1/Seguridad%20de%20entornos%20web.pdf> [2016, 23 Septiembre].
- [12] Alfonso Lorenzo Pérez (2016, Septiembre). "Riesgo, Amenaza y Vulnerabilidad (ISO 27001)". [En Línea]. Disponible en: <http://eq2b.com/riesgo-amenaza-y-vulnerabilidad-iso-27001/> [2016, 24 Septiembre].
- [13] Meta-Thrunks (2015, Julio). "Man in the middle". [En Línea]. Disponible en: <http://www.btk-clan.ch/2015/07/02/man-in-the-middle/> [2016, 24 Septiembre].
- [14] Michael Byrne (2016, Enero). "How To Go From 0 to Sniffing Packets in 10 Minutes". [En Línea]. Disponible en: <http://motherboard.vice.com/read/how-to-go-from-0-to-sniffing-packets-in-10-minutes> [2016, 24 Septiembre].
- [15] Florian (2015, Mayo). "Analysing a Denial of Service Attack Tool". [En Línea]. Disponible en: <https://bogner.sh/2015/05/analysing-a-denial-of-service-attack-tool/> [2016, 24 Septiembre].

- [16] Malli Nenib (2013, Noviembre). "How to test for SQL Injection?". [En Línea]. Disponible en:<https://itsecurityconcepts.com/tag/sql-injection/> [2016, 24 Septiembre].
- [17] Avik Sarkar (2012, Diciembre). "HP Training Center Official Website Hacked & Defaced". [En Línea]. Disponible en:<http://www.voiceofgreyhat.com/2012/08/HP-Training-Center-Official-Website-Hacked.html> [2016, 24 Septiembre].
- [18] Darril Gibson (2015). "Black Box Testing and More". [En Línea]. Disponible en:<http://blogs.getcertifiedgetahead.com/black-box-testing-and-more/> [2016, 25 Septiembre].
- [19] ESOLN.NET. "Introduction to Ethical Hacking". [En Línea]. Disponible en:[http://esoln.net/Hacking/CEH%20Guide\\_Chapter%201%20-%20Ethical%20Hacking%20Basics%20.php](http://esoln.net/Hacking/CEH%20Guide_Chapter%201%20-%20Ethical%20Hacking%20Basics%20.php) [2016, 10 Octubre].
- [20] Offensive Security (2016). "Kali Linux Tools Listing". [En Línea]. Disponible en:<http://tools.kali.org/tools-listing> [2016, 10 Octubre].
- [21] Juraj Komlosi (2015, Marzo). "Protection against Cross-site request forgery (CSRF, XSRF)". [En Línea]. Disponible en:[https://devnet.kentico.com/articles/protection-against-cross-site-request-forgery-\(csrf-xsrf\)](https://devnet.kentico.com/articles/protection-against-cross-site-request-forgery-(csrf-xsrf)) [2016, 1 Noviembre].
- [22] L. Allen (2012, Mayo). "Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide". [Documento PDF]. Obtenido en:<https://news.asis.io/sites/default/files/%E2%80%8Cbook.pdf> [2016, 15 Octubre].
- [23] BackTrack Academy (2013, Marzo). "Penetration Testing With BackTrack: Manual Traducido". [Documento PDF]. Obtenido en:<http://es.slideshare.net/JuanCarlosCampos7/backtrack-5-manual-traducido-42334676> [2016, 29 Septiembre].



- [24] A. Singh (2012, Junio). "Metasploit Penetration Testing Cookbook". [Documento PDF]. Obtenido en: <http://www.it-docs.net/ddata/3788.pdf> [2016, 4 Octubre].
- [25] A. Singh, M. Agarwal (2013, Octubre). "Metasploit Penetration Testing Cookbook: Second Edition". [Documento PDF]. Obtenido en: <http://www.arthur-training.com/Downloads/ITT/Metasploit%20Penetration%20Testing%20Cookbook%20-%20Agarwal,%20Monika.pdf> [2016, 5 Octubre].
- [26] M. Aharoni (2011). "Penetration Testing With BackTrack". [Documento PDF]. Obtenido en: <https://ebook.konfigurasi.net/Hacking%20and%20Pentest/Offensive-Security-Penetration-Testing-with-BackTrack-Lab-Guidev3.2.pdf> [2016, 20 Septiembre].
- [27] Offensive Security (2013, Septiembre). "Penetration Testing With Kali Linux". [Documento PDF]. Obtenido en: <https://www.offensive-security.com/documentation/penetration-testing-with-kali.pdf> [2016, 11 Octubre].
- [28] C. Hadnagy (2010, Octubre). "Social Engineering: The Art Of Human Hacking". [Documento PDF]. Obtenido en: [http://sin.thectulhu.com/library/security/social\\_engineering/The\\_Art\\_of\\_Human\\_Hacking.pdf](http://sin.thectulhu.com/library/security/social_engineering/The_Art_of_Human_Hacking.pdf) [2016, 11 Octubre].
- [29] SENATI (2012, Febrero). "Administración y Mantenimiento de Windows Server 2008". [Documento PDF]. Obtenido en: <https://rubicell.files.wordpress.com/2011/03/manual-windows-2008-server-byreparaciondepc-cl.pdf> [2016, 12 Octubre].
- [30] J. Calles, P. Gonzáles (2011). "La Biblia del Footprinting". [Documento PDF]. Obtenido en:

- [http://plataforma.josedomingo.org/pledin/pluginfile.php/1836/mod\\_resource/content/1/recursos/pentest/La\\_Biblia\\_del\\_Footprinting.pdf](http://plataforma.josedomingo.org/pledin/pluginfile.php/1836/mod_resource/content/1/recursos/pentest/La_Biblia_del_Footprinting.pdf) [2016, 15 Octubre].
- [31] Paul Asadoorian (2014, Julio). “Installing and Using Nessus on Kali Linux”. [En línea]. Disponible en: <https://www.tenable.com/blog/installing-and-using-nessus-on-kali-linux> [2016, 16 Octubre].
- [32] Alonso Caballero Quezada (2016, Enero). “Instalación de Nessus en Kali Linux”. [En Línea]. Disponible en: [http://www.reydes.com/d/?q=Instalacion\\_de\\_Nessus\\_en\\_Kali\\_Linux](http://www.reydes.com/d/?q=Instalacion_de_Nessus_en_Kali_Linux) [2016, 17 Octubre].
- [33] Caleb Bucker (2012, Octubre). “[Penetration Testing - Hacking Etico] Análisis Web - Evaluación de Vulnerabilidades – Explotacion”. [En Línea]. Disponible en: <http://calebbucker.blogspot.com/2012/10/penetration-testing-hacking-etico.html> [2016, 18 Octubre].
- [34] D. De Smet, W. Pritchett (2012, Diciembre). “BackTrack 5 Cookbook”. [Documento PDF]. Obtenido en: <http://pdf.th7.cn/download/files/1411/BackTrack%20%20Cookbook.pdf> [2016, 19 Octubre].
- [35] P. Calderón (2012, Noviembre). “Nmap 6: Network Exploration and Security Auditing Cookbook”. [Documento PDF]. Obtenido en: <http://it-ebooks.directory/book-1849517487.html> [2016, 19 Octubre].
- [36] O. Arévalo, K. Escalante, N. Guevara (2009, Mayo). “Análisis de Riesgo de la Seguridad de la Información”. [Documento PDF]. Obtenido en: <https://upload.wikimedia.org/wikipedia/commons/8/87/Riesgoinformatico.pdf> [2016, 19 Octubre].
- [37] Municipio del Distrito Metropolitano de Quito, “Catálogo de Servicios – Prioridad Final”, Dirección Metropolitana de Informática, Quito – Ecuador, Dic. 2016.

- [38] G. Najera (2016, Febrero). "Kali Linux Web Penetration Testing Cookbook". [Documento PDF]. Obtenido en: <http://it-ebooks.directory/book-178439291x.html> [2016, 20 Octubre].
- [39] Open Web Application Security Project (2013). "Top 10 2013-Top 10 – OWASP". [En Línea]. Disponible en: [https://www.owasp.org/index.php/Top\\_10\\_2013-Top\\_10](https://www.owasp.org/index.php/Top_10_2013-Top_10) [2016, 25 Octubre].
- [40] P. Engebreston (2011). "The Basics of Hacking and Penetration Testing". [Documento PDF]. Obtenido en: <http://it-ebooks.directory/book-0124116442.html> [2016, 25 Octubre].
- [41] P. Hope (2008, Octubre). "Web Security Testing Cookbook". [Documento PDF]. Obtenido en: <http://it-ebooks.directory/book-0596514832.html> [2016, 25 Octubre].
- [42] K. Butler, A. Collins, H. Meer (2007). "Penetration Tester's Open Source Toolkit". [Documento PDF]. Obtenido en: <http://www.arthur-training.com/Downloads/ITT/Syngress%20-%20Penetration%20Tester's%20Open%20Source%20Toolkit%20-%20Vol.2.pdf> [2016, 10 Noviembre].
- [43] J. Faircloth (2011). "Penetration Tester's Open Source Toolkit Third Edition". [Documento PDF]. Obtenido en: [http://data.ceh.vn/Ebook/ebooks.shahed.biz/HACK/Penetration\\_Tester\\_\\_s\\_Open\\_Source\\_Toolkitplus.pdf](http://data.ceh.vn/Ebook/ebooks.shahed.biz/HACK/Penetration_Tester__s_Open_Source_Toolkitplus.pdf) [2016, 10 Noviembre].
- [44] T. Wilhelm (2010). "Professional Penetration Testing: Creating and Operating a Formal Hacking Lab". [Documento PDF]. Obtenido en: [http://index-of.es/eBooks/15\\_Profesional\\_PenetrationA.pdf](http://index-of.es/eBooks/15_Profesional_PenetrationA.pdf) [2016, 12 Noviembre].
- [45] J. Erickson (2008). "Hacking: The Art of Exploitation, 2nd Edition". [Documento PDF]. Obtenido en: <https://leaksource.files.wordpress.com/2014/08/hacking-the-art-of-exploitation.pdf> [2016, 15 Noviembre].

- [46] D. Stuttard, M. Pinto (2011). "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Second Edition". [Documento PDF]. Obtenido en: <https://leaksource.files.wordpress.com/2014/08/the-web-application-hackers-handbook.pdf> [2016, 15 Noviembre].
- [47] B. Damele, M. Stampar (2011). "SQLmap User's Manual". [Documento PDF]. Obtenido en: <http://www.it-docs.net/ddata/4956.pdf> [2016, 18 Noviembre].
- [48] M.Shema (2011). "Web Application Security for Dummies". [Documento PDF]. Obtenido en: <http://www.bradreese.com/qualys-web-application-security-for-dummies.pdf> [2016, 18 Noviembre].
- [49] SysAdmin Audit, Networking and Security Institute (2013). "Introduction to the OWASP Multillidae II Pen-Test Training Environment". [Documento PDF]. Obtenido en: <https://www.sans.org/reading-room/whitepapers/testing/introduction-owasp-mutillidae-ii-web-pen-test-training-environment-34380> [2016, 18 Noviembre].
- [50] Joan Boluda (2012). "Guía del archivo robots.txt". [En Línea]. Disponible en: <https://boluda.com/tutorial/guia-del-archivo-robots-txt/> [2016, 10 Noviembre].
- [51] Foros del Web (2005). "Robots.txt es seguro?". [En Línea]. Disponible en: <http://www.forosdelweb.com/f91/robots-txt-seguro-494885/> [2016, 14 Diciembre].
- [52] José Chica (2012, Mayo). "Defensas contra nmap". [En línea]. Disponible en: <https://www.securityartwork.es/2012/05/22/defensas-contra-nmap/>. [2016, 14 Diciembre].
- [53] Luis Silva (2013, Octubre). "Denegar escaneo de puertos con iptables". [En línea]. Disponible en: <http://www.enlinux.org/denegar-escaneo-de-puertos-con-iptables/>. [2016, 14 Diciembre].

- [54] David García Martín (2010, Octubre). “Guía para evitar un escaneo de puertos”. [En línea]. Disponible en: <https://www.redeszone.net/2010/10/24/guia-para-evitar-un-escaneo-de-puertos/>. [2016, 14 Diciembre].
- [55] Microsoft Developer Network (2011). “Agregar o quitar metadatos”. [En línea]. Disponible en: <https://msdn.microsoft.com/es-es/library/cc295486.aspx>. [2016, 15 Diciembre].
- [56] David Yakutiel (2016, Julio). “Hide Metadata in full post”. [En Línea]. Disponible en: <https://wordpress.org/support/topic/hide-metadata-in-full-posts/> [2016, 15 Diciembre].
- [57] Erick (2011, Diciembre). “Evitar listado de directorios, archivo en Apache y IIS. [En Línea]. Disponible en: <https://darkchicles.com/quien-es-darkchicles/> [2016, 15 Diciembre].
- [58] IT IGLOO (2015, Enero). “How to configure HTTP Strict Transport Security (HSTS) on Apache & NGINX”. [En Línea]. Disponible en: <https://itigloo.com/security/how-to-configure-http-strict-transport-security-hsts-on-apache-nginx/> [2016, 16 Diciembre].
- [59] ACUNETIX (2014). “Insecure crossdomain.xml file”. [En Línea]. Disponible en: <https://www.acunetix.com/vulnerabilities/web/insecure-crossdomain-xml-file> [2016, 16 Diciembre].
- [60] Marius Ducea (2007, Octubre). “Apache Tips: Disable the HTTP TRACE Method”. [En Línea]. Disponible en: <http://www.ducea.com/2007/10/22/apache-tips-disable-the-http-trace-method/> [2016, 16 Diciembre].
- [61] Apache.org. “Respuestas de error personalizadas”. [En Línea]. Disponible en: <https://httpd.apache.org/docs/2.4/custom-error.html> [2016, 16 Diciembre].
- [62] Glenn Darmanin (2014, Noviembre). “8 tips for secure you IIS installation”. [En

- Línea]. Disponible en: <http://www.acunetix.com/blog/articles/8-tips-secure-iis-installation/> [2016, 16 Diciembre].
- [63] Robert McMurray (2010, Julio). "UrlScan 3 Reference". [En Línea]. Obtenido en: <https://www.iis.net/learn/extensions/working-with-urlscan/urlscan-3-reference> [2016, 16 Diciembre].
- [64] Scott Hanselman (2015, Junio). "How to enable HTTP Strict Transport Security (HSTS) in IIS7+". [En línea]. Disponible en: <http://www.hanselman.com/blog/HowToEnableHTTPStrictTransportSecurityHSTSInIIS7.aspx>. [2016, 16 Diciembre].
- [65] Jan Reilink (2015, Junio). "How to enable HTTP Strict-Transport-Security (HSTS) on IIS - Windows Server". [En Línea]. Disponible en: <http://www.hanselman.com/blog/HowToEnableHTTPStrictTransportSecurityHSTSInIIS7.aspx> [2016, 17 Diciembre].
- [66] Jamie Furr (2012, Junio). "How to set up custom error pages in IIS 7.5 with ASP.NET". [En Línea]. Disponible en: <http://www.sherweb.com/blog/how-to-create-custom-error-pages-in-iis-7-5-with-asp-net/> [2016, 17 Diciembre].
- [67] Lerrie Oblego (2013, Febrero). "Custom pages 404 redirect and error display : The Official Microsoft IIS Forums". [En línea]. Disponible en: <https://forums.iis.net/t/1195922.aspx>. [2016, 17 Diciembre].
- [68] CVEdetails.com. "CVE Details: The Ultimate Security vulnerability Datasource". [En Línea]. Disponible en: <https://www.cvedetails.com/> [2016, 23 Diciembre].
- [69] Security Focus. (2016, Julio). "Apache HTTP Server CVE-2016-5387 Security Bypass Vulnerability". [En Línea]. Disponible en: <http://www.securityfocus.com/bid/91816/info> [2016, 23 Diciembre].
- [70] Security Focus. (2014, Julio). "Apache HTTP Server CVE-2014-3523 Remote

- Denial of Service Vulnerability”. [En Línea]. Disponible en: <http://www.securityfocus.com/bid/68747/info> [2016, 23 Diciembre].
- [71] CVEdetails.com. “CVE Details: CVE-2017-0004”. [En Línea]. Disponible en: <https://www.cvedetails.com/cve/CVE-2017-0004/> [2016, 23 Diciembre].
- [72] CVEdetails.com. “CVE Details: CVE-2013-0075”. [En Línea]. Disponible en: <https://www.cvedetails.com/cve/CVE-2013-0075/> [2016, 23 Diciembre].
- [73] CVEdetails.com. “CVE Details: CVE-2012-2556”. [En Línea]. Disponible en: <https://www.cvedetails.com/cve/CVE-2012-2556/> [2016, 23 Diciembre].
- [74] CVEdetails.com. “CVE Details: CVE-2016-7478”. [En Línea]. Disponible en: <https://www.cvedetails.com/cve/CVE-2016-7478/> [2016, 23 Diciembre].
- [75] CVEdetails.com. “CVE Details: CVE-2015-8876”. [En Línea]. Disponible en: <https://www.cvedetails.com/cve/CVE-2015-8876/> [2016, 23 Diciembre].
- [76] CVEdetails.com. “CVE Details: CVE-2015-0231”. [En Línea]. Disponible en: <https://www.cvedetails.com/cve/CVE-2015-0231/> [2016, 23 Diciembre].
- [77] CVEdetails.com. “CVE Details: CVE-2010-3972”. [En Línea]. Disponible en: <https://www.cvedetails.com/cve/CVE-2010-3972/> [2016, 23 Diciembre].
- [78] CVEdetails.com. “CVE Details: CVE-2010-2730”. [En Línea]. Disponible en: <https://www.cvedetails.com/cve/CVE-2010-2730/> [2016, 23 Diciembre].
- [79] CVEdetails.com. “CVE Details: CVE-2010-1899”. [En Línea]. Disponible en: <https://www.cvedetails.com/cve/CVE-2010-1899/> [2016, 23 Diciembre].
- [80] CVEdetails.com. “CVE Details: CVE-2015-1419”. [En Línea]. Disponible en: <https://www.cvedetails.com/cve/CVE-2015-1419/> [2016, 23 Diciembre].
- [81] CVEdetails.com. “CVE Details: CVE-2004-2259”. [En Línea]. Disponible en: <https://www.cvedetails.com/cve/CVE-2004-2259/> [2016, 23 Diciembre].

- [82] CVEdetails.com. “CVE Details: CVE-2015-4819”. [En Línea]. Disponible en: <https://www.cvedetails.com/cve/CVE-2015-4819/> [2016, 23 Diciembre].
- [83] CVEdetails.com. “CVE Details: CVE-2015-4879”. [En Línea]. Disponible en: <https://www.cvedetails.com/cve/CVE-2015-4879/> [2016, 23 Diciembre].
- [84] Municipio del Distrito Metropolitano de Quito, “Políticas de Gestión de Información”, Dirección Metropolitana de Informática, Quito – Ecuador, Dic. 2016.
- [85] Municipio del Distrito Metropolitano de Quito, “Formulario de no Divulgación de la Información”, Dirección Metropolitana de Informática, Quito – Ecuador, Dic. 2016.
- [86] Municipio del Distrito Metropolitano de Quito, “Entrevistas, cuestionarios, observación, contratos”, Talento Humano, Dirección Metropolitana de Informática, Quito – Ecuador, Dic. 2016.
- [87] Municipio del Distrito Metropolitano de Quito, “Matriz de Dependencias”, Dirección Metropolitana de Informática, Quito – Ecuador, Dic. 2016
- [88] Portswigger Web Security. “Burp Suite editions and features”. [En línea]. Disponible en: <https://portswigger.net/burp/>. [2017, 3 Enero].
- [89] OWASP. “OWASP Zed Attack Proxy Project - OWASP”. [En línea]. Disponible en: [https://www.owasp.org/index.php/OWASP\\_Zed\\_Attack\\_Proxy\\_Project](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project). [2017, 3 Enero].
- [90] CIRT.net. “Nikto2 | CIRT.net”. [En línea]. Disponible en: <https://cirt.net/Nikto2>. [2017, 3 Enero].
- [91] Telnet.org. “telnet.org – information about telnet” [En línea]. Disponible en: <http://www.telnet.org/>. [2017, 3 Enero].
- [92] NETSQUARE. “Research and Tools”. [En línea]. Disponible en: <http://www.net->



- square.com/httpprint.html. [2017, 3 Enero].
- [93] MorningStar Security. “urbanadventurer/WhatWeb”. [En línea]. Disponible en: <https://github.com/urbanadventurer/WhatWeb>. [2017, 3 Enero].
- [94] The GNU Netcat Project. “urbanadventurer/WhatWeb”. [En línea]. Disponible en: <https://github.com/urbanadventurer/WhatWeb>. [2017, 3 Enero].
- [95] Curl. “curl”. [En línea]. Disponible en: <https://curl.haxx.se/>. [2017, 3 Enero].
- [96] GNU Operating Systems. “gnu.org”. [En línea]. Disponible en: <https://www.gnu.org/software/wget/>. [2017, 3 Enero].
- [97] iSECPartners. “iSECPartners/sslyze”. [En línea]. Disponible en: <https://github.com/iSECPartners/sslyze>. [2017, 3 Enero].
- [98] Titania. “ioerror/sslsan”. [En línea]. Disponible en: <https://github.com/ioerror/sslsan>. [2017, 3 Enero].
- [99] DotDotPwn. “DotDotPwn - The Directory Traversal Fuzzer”. [En línea]. Disponible en: <http://dotdotpwn.sectester.net/>. [2017, 3 Enero].
- [100] XSSer. “XSSer: Cross Site ‘Scripter’”. [En línea]. Disponible en: <https://xsser.03c8.net/>. [2017, 3 Enero].
- [101] OWASP. “Category:OWASP DirBuster Project - OWASP”. [En línea]. Disponible en: [https://www.owasp.org/index.php/Category:OWASP\\_DirBuster\\_Project](https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project). [2017, 3 Enero].
- [102] Laera Loris. “llaera/slowloris.pl”. [En línea]. Disponible en: <https://github.com/llaera/slowloris.pl>. [2017, 3 Enero].
- [103] Wappalyzer. “Wappalyzer”. [En línea]. Disponible en: <https://wappalyzer.com/>. [2017, 3 Enero].

- [104] Firebug Web Development Evolved. "Firebug". [En línea]. Disponible en: <http://getfirebug.com/>. [2017, 3 Enero].
- [105] Paterva. "Maltego CE". [En línea]. Disponible en: <https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php>. [2017, 3 Enero].
- [106] Eleven Paths. "FOCA". [En línea]. Disponible en: <https://www.elevenpaths.com/es/labstools/foca-2/index.html>. [2017, 3 Enero].
- [107] Gregthatcher.com. "Fingerprint Web Server". [En línea]. Disponible en: <http://www.gregthatcher.com/InformationTechnology/FingerprintWebServer.aspx>. [2017, 3 Enero].
- [108] BuiltWith Technology Lookup. "BuiltWith - Web Technology Profiler". [En línea]. Disponible en: <https://builtwith.com/>. [2017, 3 Enero].
- [109] Desenmascara.me. "Servicio de seguridad web, desenmascaramame". [En línea]. Disponible en: <http://desenmascara.me/>. [2017, 3 Enero].
- [110] Qualys SSL Labs. "SSL Server Test (Powered by Qualys SSL Labs)". [En línea]. Disponible en: <https://www.ssllabs.com/ssltest/>. [2017, 3 Enero].
- [111] Commix Project. "GitHub - commixproject/commix: Automated All-in-One OS command injection and exploitation tool". [En línea]. Obtenido en: <https://github.com/commixproject/commix> [2017, 3 Enero].
- [112] Stakewinner00. "Hack x Crack Hacking Buscadores". [Documento PDF]. Obtenido en: <https://es.scribd.com/document/139157932/Hack-x-Crack-Hacking-Buscadores> [2017, 3 Enero].

## **ANEXOS**

**ANEXO A** Declaración de Aplicabilidad

**ANEXO B** Catálogo de servicios prioridad final

**ANEXO C** Matriz de dependencias

**ANEXO D** Lista de los módulos habilitados en el servidor apache

**ANEXO E** Resultado del análisis de vulnerabilidades de Nessus, Portal web del MDMQ

**ANEXO F** Resultado del análisis de vulnerabilidades de Nessus, Portal de pago de impuestos por internet

**ANEXO G** Calendario de realización de pruebas de seguridad

## ANEXO A: DECLARACIÓN DE APLICABILIDAD

En la tabla A-1 se presenta la Declaración de Aplicabilidad.

OBJETIVO DE CONTROL	CONTROL	CUMPLE		
		NO CUMPLE	PARCIAL	TOTAL
A.5 Política de seguridad	A.5.1.1 Documentar política de seguridad de información			X
	A.5.1.2 Revisión de la política de seguridad de la información	X		
A.6 Organización de la seguridad de la información	A.6.1.1 Compromiso de la gerencia con la seguridad de la información			X
	A.6.1.2 Coordinación de la seguridad de información		X	
	A.6.1.3 Asignación de responsabilidades de la seguridad de la información		X	
	A.6.1.4 Proceso de autorización para los medios de procesamiento de información			X
	A.6.1.5 Acuerdos de confidencialidad			X
	A.6.1.6 Contacto con autoridades			X

	A.6.1.7 Contacto con grupos de interés especial			X	
	A.6.1.8 Revisión independiente de la seguridad de la información			X	
	A.6.2.1 Identificación de riesgos relacionados con entidades externas				X
	A.6.2.2 Tratamiento de la seguridad cuando se trabaja con clientes				X
	A.6.2.3 Tratamiento de la seguridad en contratos con terceras personas			X	
	A.7.1.1 Inventarios de activos				X
	A.7.1.2 Propiedad de los activos				X
	A.7.1.3 Uso aceptable de los activos				X
	A.7.2.1 Lineamientos de clasificación			X	
	A.7.2.2 Etiquetado y manejo de la información			X	
	A.8.1.1 Roles y responsabilidades			X	
	A.8.1.2 Selección				X
	A.8.1.3 Términos y condiciones de empleo				X
	A.8.2.1 Gestión de responsabilidades				X
<b>A.7</b>	<b>Gestión de activos</b>				
<b>A.8</b>	<b>Seguridad de los recursos humanos</b>				





A.10.3.1	Gestión de capacidad		X	
A.10.3.2	Aceptación del sistema			X
A.10.4.1	Controles contra software malicioso		X	
A.10.5.1	Back-up o respaldo de la información		X	
A.10.6.1	Controles de red			X
A.10.6.2	Seguridad de los servicios de red		X	
A.10.7.1	Gestión de los medios removibles		X	
A.10.7.2	Eliminación de medios		X	
A.10.7.3	Procedimientos de manejo de la información		X	
A.10.7.4	Seguridad de documentación del sistema			X
A.10.8.1	Procedimientos y políticas de información y software		X	
A.10.8.2	Acuerdos de intercambio			X



A.10.8.3 Medios físicos en tránsito		X	
A.10.8.4 Mensajes electrónicos		X	
A.10.8.5 Sistemas de información comercial			X
A.10.9.1 Comercio electrónico	X		
A.10.9.2 Transacciones en línea			X
vA.10.9.3 Información disponible públicamente	X		
A.10.10.1 Registro de auditoría	X		
A.10.10.2 Uso del sistema de monitoreo			X
A.10.10.3 Protección de la información del registro	X		
A.10.10.4 Registros del administrador y operador		X	
A.10.10.5 Registro de fallas		X	
A.10.10.6 Sincronización de relojes		X	
A.11.1.1 Política de control de acceso			X
A.11.2.1 Inscripción del usuario		X	

**A.11**  
**Control de**  
**acceso**

A.11.2.2	Gestión de privilegios			X	
A.11.2.3	Gestión de la clave del usuario			X	
A.11.3.1	Uso de clave			X	
A.11.4.1	Política sobre el uso de servicios en red			X	
A.11.4.2	Autenticación del usuario para conexiones externas			X	
A.11.4.3	Identificación del equipo en red			X	
A.11.4.4	Protección del puerto de diagnóstico remoto				X
A.11.4.5	Segregación en redes				X
A.11.5.1	Procedimientos de registro en el terminal			X	
A.11.5.2	Identificación y autenticación del usuario			X	
A.11.5.3	Sistema de gestión de claves			X	
A.11.5.4	Uso de utilidades del sistema			X	

A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información	A.11.5.5 Sesión inactiva				X
	A.11.5.6 Limitación de tiempo de conexión				X
	A.11.6.1 Restricción al acceso a la información				X
	A.11.6.2 Aislamiento del sistema sensible				X
	A.11.7.1 Computación móvil y comunicaciones	X			
	A.12.1.1 Análisis y especificación de los requerimientos de seguridad				X
	A.12.2.1 Validación de data de Insumo				X
	A.12.2.2 Control de procesamiento interno				X
	A.12.2.3 Integridad del mensaje				X
	A.12.2.4 Validación de data de output				X
A.12.3.1 Política sobre el uso de controles criptográficos				X	
A.12.3.2 Gestión clave				X	
A.12.4.1 Control de software operacional		X			
A.12.4.3 Control de acceso al código fuente del programa				X	

	A.12.5.1	Procedimientos de control de cambio			X	
	A.12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo			X	
	A.12.5.3	Restricciones sobre los cambios en los paquetes de software				X
	A.12.5.4	Filtración de información				X
	A.12.5.5	Desarrollo de outsourced software				X
	A.12.6.1	Control de vulnerabilidades técnicas	X			
	A.13.1.1	Reporte de eventos en la seguridad de la información				X
	A.13.1.2	Reporte de debilidades en la seguridad				X
	A.13.2.1	Responsabilidades y procedimientos			X	
	A.13.2.2	Aprendizaje de los incidentes en la seguridad de la información	X			
	A.13.2.3	Recolección de evidencia				X
	A.14.1.1	Incluir seguridad de la información en el proceso de gestión de continuidad comercial			X	
	A.14.1.2	Continuidad comercial y evaluación del riesgo			X	
<b>A. 13</b>	<b>Gestión de incidentes en la seguridad de la información</b>					
<b>A.14</b>	<b>Gestión de la continuidad comercial</b>					

	A.14.1.3 Desarrollar e implementar planes de continuidad incluyendo seguridad de la información		X	
	A.14.1.4 Marco referencial para la planeación de la continuidad comercial		X	
	A.14.1.5 Prueba, mantenimiento y re-evaluación de planes de continuidad coerciales		X	
	A.15.1.1 Identificación de legislación aplicable		X	
	A.15.1.2 Derechos de propiedad intelectual (IPR)		X	
	A.15.1.3 Protección los registros organizacionales	X		
	A.15.1.4 Protección de data y privacidad de información personal		X	
	A.15.1.6 Regulación de controles criptográficos	X		
	A.15.2.1 Cumplimiento con las políticas y estándares de seguridad		X	
	A.15.2.2 Chequeo de cumplimiento técnico		X	
	A.15.3.2 Protección de las herramientas de auditoria de los sistemas de información		X	

**Tabla A-1** Declaración de aplicabilidad

**A.15**  
**Cumplimiento**

## ANEXO B: CATÁLOGO DE SERVICIOS PRIORIDAD FINAL

En la Tabla B-1 se muestra el formato del Catálogo de Servicios Prioridad Final

Prioridad	Servicio Informático / Infraestructura	Usuarios Finales
1. Muy Alta	Sistema 1	Usuario 1, Usuario 2
1. Muy Alta	Sistema 2	Usuario 3, Usuario 5
1. Muy Alta	Sistema 3	Usuario 4, Usuario 8
1. Muy Alta	Sistema 4	Usuario 14, Usuario 19
1. Muy Alta	Sistema 5	Usuario 4, Usuario 6
1. Muy Alta	Sistema 6	Usuario 2
2. Alta	Sistema 9	Usuario 1, Usuario 2
2. Alta	Sistema 10	Usuario 14
2. Alta	Sistema 11	Usuario 13
2. Alta	Sistema 12	Usuario 1
2. Alta	Sistema 13	Usuario 12
2. Alta	Sistema 14	Usuario 19, Usuario 2
2. Alta	Sistema 15	Usuario 15
3. Normal	Sistema 16	Usuario 16 Usuario 17
3. Normal	Sistema 17	Usuario 7, Usuario 2
3. Normal	Sistema 18	Usuario 18
3. Normal	Sistema 19	Usuario 13, Usuario 2
3. Normal	Sistema 20	Usuario 19
3. Normal	Sistema 21	Usuario 6, Usuario 12
4. Moderada	Sistema 22	Usuario 16, Usuario 9
4. Moderada	Sistema 23	Usuario 17, Usuario 20
4. Moderada	Sistema 25	Usuario 9, Usuario 2
4. Moderada	Sistema 26	Usuario 1, Usuario 10
4. Moderada	Sistema 27	Usuario 1, Usuario 3
5. Baja	Sistema 28	Usuario 17, Usuario 13
5. Baja	Sistema 29	Usuario 6, Usuario 5
5. Baja	Sistema 30	Usuario 1, Usuario 7
5. Baja	Sistema 31	Usuario 11, Usuario 20
5. Baja	Sistema 32	Usuario 12, Usuario 20

Tabla B-1 Formato Catálogo de Servicios Prioridad Final

### ANEXO C: MATRIZ DE DEPENDENCIAS

En la Tabla C-1 se muestra el formato de la Matriz de dependencias entre aplicaciones y sistemas del MDMQ.

SERVICIO	Sistema 1	Sistema 2	Sistema 3	Sistema 4	Sistema 5	Sistema 6	Sistema 7	Sistema 8	Sistema 9	Sistema 10	Sistema 11	Sistema 12	Sistema 13	Sistema 14	Sistema 15	Sistema 16
Sistema 1	■															
Sistema 2		■														
Sistema 3			■													
Sistema 4				■												
Sistema 5					■											
Sistema 6						■										
Sistema 7							■									
Sistema 8								■								
Sistema 9									■							
Sistema 10										■						
Sistema 11											■					
Sistema 12												■				
Sistema 13													■			
Sistema 14														■		
Sistema 15															■	
Sistema 16																■

**Tabla C-1** Formato de la Matriz de dependencias entre aplicaciones y sistemas del MDMQ

## ANEXO D: LISTA DE LOS MÓDULOS HABILITADOS EN EL SERVIDOR APACHE

```
[root@smodules]# httpd -M
Loaded Modules:
  core_module (static)
  so_module (static)
  http_module (static)
  access_compat_module (shared)
  actions_module (shared)
  alias_module (shared)
  allowmethods_module (shared)
  auth_basic_module (shared)
  auth_digest_module (shared)
  authn_anon_module (shared)
  authn_core_module (shared)
  authn_dbd_module (shared)
  authn_dbm_module (shared)
  authn_file_module (shared)
  authn_socache_module (shared)
  authz_core_module (shared)
  authz_dbd_module (shared)
  authz_dbm_module (shared)
  authz_groupfile_module (shared)
  authz_host_module (shared)
  authz_owner_module (shared)
  authz_user_module (shared)
  autoindex_module (shared)
  cache_module (shared)
  cache_disk_module (shared)
  data_module (shared)
  dbd_module (shared)
  deflate_module (shared)
  dir_module (shared)
  dumpio_module (shared)
  echo_module (shared)
  env_module (shared)
  expires_module (shared)
  ext_filter_module (shared)
  filter_module (shared)
  headers_module (shared)
  include_module (shared)
  info_module (shared)
  log_config_module (shared)
  logio_module (shared)
```



```
mime_magic_module (shared)
mime_module (shared)
negotiation_module (shared)
remoteip_module (shared)
reqtimeout_module (shared)
rewrite_module (shared)
setenvif_module (shared)
slotmem_plain_module (shared)
slotmem_shm_module (shared)
socache_dbm_module (shared)
socache_memcache_module (shared)
socache_shmcb_module (shared)
status_module (shared)
substitute_module (shared)
suexec_module (shared)
unique_id_module (shared)
unixd_module (shared)
userdir_module (shared)
version_module (shared)
vhost_alias_module (shared)
dav_module (shared)
dav_fs_module (shared)
dav_lock_module (shared)
lua_module (shared)
mpm_prefork_module (shared)
proxy_module (shared)
lbmethod_bybusyness_module (shared)
lbmethod_byrequests_module (shared)
lbmethod_bytraffic_module (shared)
lbmethod_heartbeat_module (shared)
proxy_ajp_module (shared)
proxy_balancer_module (shared)
proxy_connect_module (shared)
proxy_express_module (shared)
proxy_fcgi_module (shared)
proxy_fdpass_module (shared)
proxy_ftp_module (shared)
proxy_http_module (shared)
proxy_scgi_module (shared)
systemd_module (shared)
cgi_module (shared)
php5_module (shared)
```

## ANEXO E: RESULTADO DEL ANÁLISIS DE VULNERABILIDADES DE NESSUS, PORTAL WEB DEL MDMQ

Critical	High	Medium	Low	Info	Total
0	0	5	1	24	30
Details					
Severity	Plugin Id	Name			
Medium (5.0)	11213	<b>HTTP TRACE / TRACK Methods Allowed</b>			
Medium (5.0)	11411	<b>Backup Files Disclosure</b>			
Medium (5.0)	40984	<b>Browsable Web Directories</b>			
Medium (5.0)	46803	<b>PHP expose_php Information Disclosure</b>			
Medium (4.3)	85582	<b>Web Application Potentially Vulnerable to Clickjacking</b>			
Low (2.6)	26194	<b>Web Server Transmits Cleartext Credentials</b>			
Info	10107	<b>HTTP Server Type and Version</b>			
Info	10302	<b>Web Server robots.txt Information Disclosure</b>			
Info	10662	<b>Web mirroring</b>			
Info	11032	<b>Web Server Directory Enumeration</b>			
Info	11219	<b>Nessus SYN scanner</b>			
Info	11419	<b>Web Server Office File Inventory</b>			
Info	18261	<b>Apache Banner Linux Distribution Disclosure</b>			
Info	24260	<b>HyperText Transfer Protocol (HTTP) Information</b>			
Info	32318	<b>Web Site Cross-Domain Policy File Detection</b>			
Info	33817	<b>CGI Generic Tests Load Estimation (all tests)</b>			
Info	39470	<b>CGI Generic Tests Timeout</b>			
Info	40406	<b>CGI Generic Tests HTTP Errors</b>			
Info	40773	<b>Web Application Potentially Sensitive CGI Parameter Detection</b>			
Info	42057	<b>Web Server Allows Password Auto-Completion</b>			

Info	43111	<b>HTTP Methods Allowed (per directory)</b>
Info	47830	<b>CGI Generic Injectable Parameter</b>
Info	48243	<b>PHP Version</b>
Info	49704	<b>External URLs</b>
Info	50344	<b>Missing or Permissive Content-Security-Policy HTTP Response Header</b>
Info	50345	<b>Missing or Permissive X-Frame-Options HTTP Response Header</b>
Info	84574	<b>Backported Security Patch Detection (PHP)</b>
Info	85601	<b>Web Application Cookies Not Marked HttpOnly</b>
Info	85602	<b>Web Application Cookies Not Marked Secure</b>
Info	91815	<b>Web Application Sitemap</b>

## ANEXO F: RESULTADO DEL ANÁLISIS DE VULNERABILIDADES DE NESSUS, PORTAL DE PAGO DE IMPUESTOS POR INTERNET

Critical	High	Medium	Low	Info	Total
0	1	7	5	35	48

### Details

Severity	Plugin Id	Name
High (7.5)	41028	SNMP Agent Default Community Name (public)
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Medium (4.3)	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low (2.6)	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
Low (2.6)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Low	10547	Microsoft Windows LAN Manager SNMP LanMan Services Disclosure
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10546	Microsoft Windows LAN Manager SNMP LanMan Users Disclosure
Info	10548	Microsoft Windows LAN Manager SNMP LanMan Shares Disclosure
Info	10550	SNMP Query Running Process List Disclosure
Info	10551	SNMP Request Network Interfaces Enumeration

Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10800	SNMP Query System Information Disclosure
Info	10863	SSL Certificate Information
Info	10940	Windows Terminal Services Enabled
Info	11011	Microsoft Windows SMB Service Detection
Info	11936	OS Identification
Info	14274	Nessus SNMP Scanner
Info	19506	Nessus Scan Information
Info	19763	SNMP Query Installed Software Disclosure
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	34022	SNMP Query Routing Information Disclosure
Info	35296	SNMP Protocol Version Detection
Info	35716	Ethernet Card Manufacturer Detection
Info	40448	SNMP Supported Protocols Detection
Info	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported

Info	64814	Terminal Services Use SSL/TLS
Info	66173	RDP Screenshot
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

## ANEXO G: CALENDARIO DE REALIZACIÓN DE PRUEBAS DE SEGURIDAD

En la Tabla G-1 se muestra la fecha y hora de realización de las pruebas de seguridad.

DIRECCIÓN METROPOLITANA DE INFORMÁTICA DEL MDMQ						
CALENDARIZACIÓN DE PRUEBAS DE PENETRACIÓN						
ID	N° DE PRUEBA	CÓDIGO DE REFERENCIA	IP OBJETIVO	HORA DE REALIZACIÓN	FECHA DE REALIZACIÓN	
1	1	OTG-INFO-001	IP 1	10h00	20-Oct-2016	
2	2	OTG-INFO-001	IP 1	10h15	20-Oct-2016	
3	3	OTG-INFO-001	IP 1	10h30	20-Oct-2016	
4	4	OTG-INFO-001	IP 1	10h45	20-Oct-2016	
5	5	OTG-INFO-001	IP 1	11h00	20-Oct-2016	
6	6	OTG-INFO-001	IP 1	11h45	20-Oct-2016	
7	1	OTG-INFO-002	IP 1	10h38	21-Oct-2016	
8	2	OTG-INFO-002	IP 1	9h30	21-Oct-2016	
9	1	OTG-INFO-003	IP 1	9h42	21-Oct-2016	
10	2	OTG-INFO-003	IP 1	9h38	21-Oct-2016	
11	1	OTG-INFO-004	IP 1	15h07	28-Oct-2016	
12	1	OTG-INFO-005	IP 1	15h44	14-Dic-2016	
13	2	OTG-INFO-005	IP 1	15h56	14-Dic-2016	
14	1	OTG-INFO-006	IP 1	9h57	21-Oct-2016	
15	1	OTG-INFO-007	IP 1	9h37	21-Oct-2016	

16	2	OTG-INFO-007	IP 1	9h40	21-Oct-2016
17	1	OTG-INFO-008	IP 1	10h35	21-Oct-2016
18	1	OTG-INFO-009	IP 1	10h43	21-Oct-2016
19	2	OTG-INFO-009	IP 1	10h53	21-Oct-2016
20	1	OTG-CONFIG-005	IP 1	10h49	21-Oct-2016
21	1	OTG-CONFIG-006	IP 1	14h21	28-Oct-2016
22	1	OTG-CONFIG-007	IP 1	14h47	28-Oct-2016
23	2	OTG-CONFIG-007	IP 1	15h19	1-Dic-2016
24	1	OTG-CONFIG-008	IP 1	14h49	28-Oct-2016
25	1	OTG-AUTHZ-001	IP 1	13h04	7-Dic-2016
26	2	OTG-AUTHZ-001	IP 1	13h05	7-Dic-2016
27	1	OTG-AUTHZ-004	IP 1	11h24	16-Dic-2016
28	2	OTG-AUTHZ-004	IP 1	11h31	16-Dic-2016
29	1	OTG-INPVAL-001	IP 1	14h00	7-Dic-2016
30	2	OTG-INPVAL-001	IP 1	14h01	7-Dic-2016
31	1	OTG-INPVAL-003	IP 1	17h00	25-Nov-2016
32	2	OTG-INPVAL-003	IP 1	16h56	25-Nov-2016
33	1	OTG-INPVAL-005	IP 1	14h11	7-Dic-2016
34	2	OTG-INPVAL-005	IP 1	14h31	7-Dic-2016
35	1	OTG-INPVAL-012	IP 1	13h24	7-Dic-2016
36	1	OTG-INPVAL-013	IP 1	15h58	7-Dic-2016



37	1	OTG-ERR-001	IP 1	16h45	25-Nov-2016
38	2	OTG-ERR-001	IP 1	16h48	25-Nov-2016
39	1	OTG-CRYPST-001	IP 1	12h20	25-Nov-2016
40	2	OTG-CRYPST-001	IP 1	12h24	25-Nov-2016
41	1	OTG-CRYPT-003	IP 1	12h13	20-Dic-2016
42	1	OTG-INFO-001	IP 2	12h00	20-Oct-2016
43	2	OTG-INFO-001	IP 2	12h15	20-Oct-2016
44	3	OTG-INFO-001	IP 2	12h30	20-Oct-2016
45	4	OTG-INFO-001	IP 2	12h45	20-Oct-2016
46	5	OTG-INFO-001	IP 2	13h00	20-Oct-2016
47	6	OTG-INFO-001	IP 2	13h15	20-Oct-2016
48	1	OTG-INFO-002	IP 2	14h37	28-Oct-2016
49	2	OTG-INFO-002	IP 2	14h51	28-Oct-2016
50	1	OTG-INFO-003	IP 2	14h57	11-Nov-2016
51	2	OTG-INFO-003	IP 2	15h01	11-Nov-2016
52	1	OTG-INFO-004	IP 2	15h44	11-Nov-2016
53	1	OTG-INFO-005	IP 2	16h11	14-Dic-2016
54	2	OTG-INFO-005	IP 2	16h18	14-Dic-2016
55	1	OTG-INFO-006	IP 2	15h04	11-Nov-2016
56	1	OTG-INFO-007	IP 2	15h18	11-Nov-2016
57	1	OTG-INFO-008	IP 2	15h23	11-Nov-2016

58	1	OTG-INFO-009	IP 2	15h23	11-Nov-2016
59	2	OTG-INFO-009	IP 2	15h34	11-Nov-2016
60	1	OTG-CONFIG-005	IP 2	15h31	11-Nov-2016
61	2	OTG-CONFIG-005	IP 2	15h31	11-Nov-2016
62	3	OTG-CONFIG-005	IP 2	15h34	11-Nov-2016
63	1	OTG-CONFIG-006	IP 2	15h36	11-Nov-2016
64	1	OTG-CONFIG-007	IP 2	15h40	11-Nov-2016
65	2	OTG-CONFIG-007	IP 2	15h23	1-Dic-2016
66	1	OTG-CONFIG-008	IP 2	15h41	11-Nov-2016
67	1	OTG-AUTHZ-001	IP 2	11h07	9-Dic-2016
68	2	OTG-AUTHZ-001	IP 2	11h09	9-Dic-2016
69	1	OTG-AUTHZ-004	IP 2	11h38	16-Dic-2016
70	2	OTG-AUTHZ-004	IP 2	11h47	16-Dic-2016
71	1	OTG-INPVAL-001	IP 2	11h24	9-Dic-2016
72	2	OTG-INPVAL-001	IP 2	11h26	9-Dic-2016
73	3	OTG-INPVAL-001	IP 2	11h28	9-Dic-2016
74	1	OTG-INPVAL-003	IP 2	13h40	25-Nov-2016
75	2	OTG-INPVAL-003	IP 2	13h42	25-Nov-2016
76	1	OTG-INPVAL-005	IP 2	11h28	9-Dic-2016
77	2	OTG-INPVAL-005	IP 2	11h29	9-Dic-2016
78	1	OTG-INPVAL-012	IP 2	11h07	9-Dic-2016

79	1	OTG-INPVAL-013	IP 2	12h26	9-Dic-2016
80	1	OTG-ERR-001	IP 2	13h30	25-Nov-2016
81	2	OTG-ERR-001	IP 2	13h37	25-Nov-2016
82	1	OTG-CRYPST-001	IP 2	13h43	25-Nov-2016
83	2	OTG-CRYPST-001	IP 2	13h51	25-Nov-2016
84	1	OTG-CRYPT-003	IP 2	12h49	20-Dic-2016
REALIZADO POR: Milton Tituaña		REVISADO POR: Ing. Diego Aguirre	COMENTARIOS		
			-----		
			-----		
			-----		

Tabla G-1 Calendario de pruebas de seguridad realizadas