

Índice

Introducción	13
Capítulo I	
Fuzzing Tecnologías Web	15
1. Introducción.....	15
2. Configuración del navegador web.....	15
3. Sesiones persistentes.....	18
4. Escáner pasivo	18
PoC: protección anti-XSS del servidor web.....	20
5. Modificación y reenvío de las peticiones al servidor web	22
PoC: modificación y reenvío de las peticiones POST.....	22
PoC: Modificación y reenvío de las peticiones GET	25
6. Puntos de interrupción o breakpoints	27
PoC: Comportamiento ante errores.....	27
7. Spider.....	29
8. Configuración del Spider	31
PoC: analizando el fichero robots.txt	32
PoC: descubrimiento de direccionamiento IP Privado.....	34
9. AJAX Spider	36
Configuración del AJAX Spider.....	36
PoC: búsqueda de un formulario de autenticación basado en AJAX.....	38
10. Forced Browse	39
Configuración Forced Browser	40
PoC: descubrimiento de directorios mediante fuerza bruta	41
11. Fuzzing.....	44
12. Configuración del fuzzer.....	44
13. PoC: fuerza bruta sobre un formulario de autenticación.....	45



14. PoC: detección de una vulnerabilidad SQL injection por GET.....	48
15. PoC: detección de una vulnerabilidad XSS	51
16. Escaneo activo.....	53
17. Tipos de Ataques.....	54
18. Tecnologías soportadas en el escaneo activo	56
PoC: SQL injection y Directory Browsing descubiertos con un escaneo activo	57

Capítulo II

LDAP Injection & Blind LDAP Injection.....	59
1. Tecnología LDAP.....	59
2. Descubrir los servidores LDAP.....	62
3. Autenticación en servidores LDAP.....	65
3.1 Árboles LDAP con acceso anónimo	65
3.2 Atacar credenciales de usuario de acceso al árbol LDAP	76
3.3 Captura de información transmitida.....	85
4. LDAP Injection & Blind LDAP Injection	96
4.1 Filtros LDAP.....	96
4.2 LDAP Injection en aplicaciones Web.....	97
4.3 Implementaciones LDAP Server.....	98
4.4 LDAP Injection & Blind LDAP injection.....	104
4.5 Login Bypass.....	114
5. Aplicaciones web vulnerables a LDAP Injection.....	116
6. OpenLDAP Baseline Security Analyzer	119

Capítulo III

Ejecución de código en Servidores Web Remotos.....	121
1. Command Injection y Code Injection	121
1.1 Command Injection en código	122
1.2 Operadores comunes para realizar Command Injection	124
1.3 Testear la existencia de un Command Injection.....	125
1.4 Testear con Blind Command Injection.....	126
1.5 Automatización de los tests para la detección.....	127
1.6 Escenarios con Command Injection.....	127
1.7 Prevenir los Command Injection.....	134
2. Remote File Inclusion.....	134
2.1 Remote File Inclusion en código.....	135
2.2 Prevención de Remote File Inclusion	136



3. Ejecutar código remoto con PHP en modo CGI.....	136
3.1 Ejecución de comandos remotos	138
3.2 Inyección de una WebShell	139
4. Ataques PHP Object Injection.....	140
4.1 Magic Methods en aplicaciones PHP con POO	140
4.2 Serialización de Objetos.....	142
4.3 Un ataque de PHP Object Injection.....	142
4.4 Preparando el payload de PHP Object Injection	143
4.5 Más bugs y exploitis de PHP Object Injection.....	144
5. El bug de ShellShock.....	146
5.1 Inyectar Web Shells en servidores vulnerables a ShellShock	147
5.2 Otras explotaciones de ShellShock	150
5.3 Creación de un módulo de Metasploit para ShellShock	151
5.4 ShellShock Client-Side Scripting Attack	157
5.5 ShellShock Client-Side Scripting Attack: Paso a paso	158

Capítulo IV

Connection String Attacks	161
1. Ataques a Cadenas de Conexión en aplicaciones web.....	161
2. Cadenas de Conexión a Bases de datos	161
2.1 Ficheros UDL, DNS y ODC de configuración.....	162
2.2 Explotación de un fichero de cadena de conexión en formato UDL, DNS u ODC	167
3. Autenticación en aplicaciones web y cadenas de conexión	170
3.1 Múltiples usuarios de la aplicación web, una cadena de conexión.....	170
3.2 Múltiples usuarios de la aplicación web, varias cadenas de conexión.....	171
3.3 Autenticación y Autorización Delegada al SGBD	174
4. Ataque de Connection String Injection	175
5. Ataques de Connection String Parameter Polution	176
5.1 Autenticación Integrada en conexiones al SGBD	179
6. Connection String Parameter Pollution Attacks tecnologías Microsoft SQL Server	180
6.1 Ataque 1: User Hash stealing con CSSP	181
6.2 Ataques SSRF y XSPA.....	182
6.3 Ataque 3: Hijacking Web Credentials (Login Bypass)	192
7. Connection String Parameter Pollution Attacks tecnologías Oracle Database.	199
8. Connection String Parameter Pollution Attacks tecnologías MySQL Database.....	201
9. Conclusiones y recomendaciones de seguridad	204



Capítulo V

Info Leaks	207
1. HeartBleed	207
1.1 Extracción de datos con HeartBleed	209
1.2 Detección y explotación de HeartBleed	209
1.3 PoC: Robo de credenciales con Heartbleed	211
1.4 PoC: Buscar bugs de HeartBleed en Well-Known Ports.....	213
2. Bugs LFI (Local File Inclusion)	217
2.1 Un ataque LFI para robar una BBDD	217
2.2 Info Leak de WAF por protección contra ataques LFI.....	222
3. Paneles de monitorización, estadísticas y traza	223
3.1 Trace Viewer & Elmah en Aplicaciones .NET.....	224
3.2 Herramientas de monitorización	228
3.3 Herramientas de estadística.....	230
3.4 Herramientas de monitorización de red	237

Capítulo VI

Xpath Injection & Blind Xpath Injection.....	239
1. Xpath 1.0	239
2. Inyectando Xpath	241
3. Errores.....	244
4. ¿Dónde estoy?	246
4.1 Calculando un valor numérico	247
4.2 Los caracteres de la cadena	248
5. Sin errores	252
5.1 El buscador.....	252
5.2 El nombre de un nodo	257
5.3 Los nodos hijos	259
5.4 El orden de los nodos hijos	260
5.5 Atributos.....	261
5.6 El contenido de un comentario.....	261
5.7 Sobre las instrucciones de proceso.....	262
6. Comentarios de Xpath	263
7. Notas finales	263
8. Automatizando.....	264
9. Conclusiones	270



Capítulo VII

NoSQL Injection (Mongodb Injection)	271
1. Introducción.....	271
2. Preparación del entorno	272
3. Inyección NoSQL en PHP.....	276
3.1 Inyecciones por POST: formulario de autenticación	278
3.2 Inyecciones por GET: usuarios del sistema	280
4. Server-Side Javascript Injection	282
4.1 Inyecciones SSJS por POST: formulario de autenticación	283
4.2 Inyecciones SSJS por GET: usuarios del sistema	284
4.3 Blind NoSQL Injection	285
4.4 Denegación de servicio mediante SSJS injection	292
Índice alfabético	293
Índice de imágenes	297



