

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
19. Cómo saltar Cluodflare para scrapear un sitio web	58
20. Fuerza bruta a directorios	61
Dirbuster.....	62
Dirb	64
Diccionarios	66
21. MagicRecon.....	67

Capítulo II

LDAP Injection & Blind LDAP Injection.....	69
1. Tecnología LDAP.....	69
2. Descubrir los servidores LDAP.....	72
3. Autenticación en servidores LDAP	75
Árboles LDAP con acceso anónimo	75
Atacar credenciales de usuario de acceso al árbol LDAP.....	86
Ataque de Replay. Autenticación doble en entornos Pre-Shared Key	86
Downgrading de Autenticación en LDAP	87
Captura de información transmitida.....	95
Hijacking LDAP-s. Paso 1: Configuración de servicio LDAP-s	96
Paso 2: Hijacking de sesión LDAP-s.....	100
Contraseñas LDAP hardcodeadas en aplicaciones	103
Exportaciones de datos LDAP.....	105
4. LDAP Injection & Blind LDAP Injection	106
Filtros LDAP.....	106
LDAP Injection en aplicaciones Web.....	107
Implementaciones LDAP Server.....	108
LDAP Injection & Blind LDAP injection.....	114
AND LDAP Injection	114
AND Blind LDAP Injection	116
LDAP Injector.....	122
OR LDAP Injection	123
OR Blind LDAP Injection	123
Login Bypass.....	124

5. Aplicaciones web vulnerables a LDAP Injection.....	126
6. OpenLDAP Baseline Security Analyzer	129

Capítulo III

Ejecución de código en servidores web remotos131

1. Command Injection y Code Injection	131
Command Injection en código	132
Operadores comunes para realizar Command Injection	134
Testear la existencia de un Command Injection.....	135
Testear con Blind Command Injection.....	136
Automatización de los tests para la detección.....	137
Escenarios con Command Injection.....	137
PoC: Explotación y consecución de una shell	138
PoC: Explotación y consecución de Meterpreter.....	142
Prevenir los Command Injection.....	144
2. Remote File Inclusion.....	144
Remote File Inclusion en código.....	145
Ejemplo 1: Remote File Inclusion básico	145
Ejemplo 2: Remote File Inclusion bypassando extensión	145
Prevención de Remote File Inclusion	146
3. Ejecutar código remoto con PHP en modo CGI.....	146
Ejecución de comandos remotos	148
Inyección de una WebShell.....	149
4. Ataques PHP Object Injection.....	150
Magic Methods en aplicaciones PHP con POO	150
Serialización de Objetos.....	152
Un ataque de PHP Object Injection.....	152
Preparando el payload de PHP Object Injection	153
Más bugs y exploits de PHP Object Injection.....	154
5. El bug de ShellShock.....	156
Inyectar Web Shells en servidores vulnerables a ShellShock	157
Otras explotaciones de ShellShock	160
Creación de un módulo de Metasploit para ShellShock	161
ShellShock Client-Side Scripting Attack	167
ShellShock Client-Side Scripting Attack: Paso a paso	168
6. Ejecución de comandos en Apache Struts.....	170
7. PHP-FPM y la ejecución de código	171

Capítulo IV

Connection String Attacks175

1. Ataques a Cadenas de Conexión en aplicaciones web.....	175
2. Cadenas de Conexión a Bases de datos	175
Ficheros UDL, DSN y ODC de configuración.....	176
Explotación de un fichero de cadena de conexión en formato UDL, DSN u ODC	181
3. Autenticación en aplicaciones web y cadenas de conexión	184
Múltiples usuarios de la aplicación web, una cadena de conexión.....	184
Múltiples usuarios de la aplicación web, varias cadenas de conexión.....	185
Autenticación y Autorización Delegada al SGBD	188
4. Ataque de Connection String Injection	189
5. Ataques de Connection String Parameter Polution	190
Autenticación Integrada en conexiones al SGBD.....	193
6. Connection String Parameter Pollution Attacks tecnologías Microsoft SQL Server.....	194
Ataque 1: User Hash stealing con CSSP.....	195
Ejemplo: ASP.NET Enterprise Manager.....	195
Ataques SSRF y XSPA.....	196
Ataque 2: Escaneo de puertos anónimo (XSPA) con SSRF en CSPP	200
Ejemplo: myLittleSQLAdmin & MyLittleBackup.....	201
Ejemplo: Un cliente de SQL Server en Citrix	204
Ataque 3: Hijacking Web Credentials (Login Bypass)	206
Ejemplo: SQL Web Data Administrator	206
Ejemplo: ASP.NET Enterprise Manager.....	208
Ejemplo: myLittleAdmin & myLittleBackup.....	210
CSPP Scanner	212
7. Connection String Parameter Pollution Attacks tecnologías Oracle Database.	213
8. Connection String Parameter Pollution Attacks tecnolog. MySQL Database...	215
9. Conclusiones y recomendaciones de seguridad	218

Capítulo V

Info Leaks	221
1. HeartBleed	221
Extracción de datos con HeartBleed	223
Detección y explotación de HeartBleed.....	223
PoC: Robo de credenciales con Heartbleed	225
PoC: Buscar bugs de HeartBleed en Well-Known Ports.....	227
2. Bugs LFI (Local File Inclusion)	231
Un ataque LFI para robar una BBDD	231
Info Leak de WAF por protección contra ataques LFI.....	236

3. Paneles de monitorización, estadísticas y traza	237
Trace Viewer & Elmah en Aplicaciones .NET.....	238
Herramientas de monitorización	242
Herramientas de estadística.....	244
Herramientas de monitorización de red	251
4. Cómo conocer tu motor de base de datos desde tu SAP	252
5. Optionsbleed	255

Capítulo VI

Xpath Injection & Blind Xpath Injection	257
1. Xpath 1.0	257
2. Inyectando Xpath	259
3. Errores.....	262
4. ¿Dónde estoy?	264
Calculando un valor numérico	265
Los caracteres de la cadena	266
5. Sin errores	270
El buscador.....	270
El nombre de un nodo	275
Los nodos hijos	277
El orden de los nodos hijos	278
Atributos.....	279
El contenido de un comentario.....	279
Sobre las instrucciones de proceso.....	280
6. Comentarios de Xpath	281
7. Notas finales	281
8. Automatizando.....	282
9. Conclusiones	288

Capítulo VII

NoSQL Injection (Mongodb Injection)	289
1. Introducción.....	289
2. Preparación del entorno	290
3. Inyección NoSQL en PHP.....	294
Inyecciones por POST: formulario de autenticación	296
Inyecciones por GET: usuarios del sistema	298

4. Server-Side Javascript Injection	300
Inyecciones SSJS por POST: formulario de autenticación	301
Inyecciones SSJS por GET: usuarios del sistema	302
Blind NoSQL Injection	303
Extracción de la versión de MongoDB.....	306
Extracción del número de colecciones de la base de datos	306
Extracción del nombre de las colecciones	306
Extracción de la colección de datos.....	307
Denegación de servicio mediante SSJS injection	310
5. NoSQLMap	310
Funcionamiento.....	311
Índice de imágenes	315
Índice alfabético	327
Otros libros publicados.....	331