

Índice

Notas previas	11
Introducción	
Las Inyecciones.....	13
Capítulo I	
SQL Injection a partir de (casi) cero	15
1. Preparando el entorno	15
2. Login	19
3. Inyectando SQL	20
4. Una contramedida	21
5. Más allá del acceso	24
6. Los mensajes de error	28
7. Leyendo de la Base de Datos sin mensajes de error	31
8. Esquemas y Datos	37
9. La configuración y la lectura de ficheros.....	42
10. Escribir ficheros.....	47
11. Ejecutar programas.....	50
12. Respuestas indirectas y otras “curiosidades”	58
13. Conclusiones	59
14. Referencias	60
Capítulo II	
Serialized SQL Injection.....	61
1. PostgreSQL	61

Funciones para XML.....	62
Versiones anteriores a la 8.3.....	67
2. Microsoft SQL Server 2000, 2005 y 2008: Cláusula FOR XML	70
3. Serialized SQL Injection en MySQL	76
4. Serialized SQL Injection en Oracle Databases	78
5. Serialized SQL Injection basada en errores.....	81
6. Automatización	82
7. Referencias	86

Capítulo III

Blind SQL Injection	87
1. Inyección en condiciones más difíciles.....	87
2. Todo está hecho de números	90
3. Blind SQL Injection “clásica”	92
4. Todo está hecho de bits	94
5. Automatización	96
6. Herramientas	97
SQLInjector.....	98
SQLbftools	99
Bfsql	101
SQL PowerInjector.....	101
Absinthe	102
Un ejemplo con Absinthe	102
7. Otras herramientas	105
8. Optimizando el proceso.....	107
Maximizando la información de la respuesta.....	108
Minimizando los bits del problema.....	113
9. Time-Based Blind SQL Injection: Blind SQL Injection completamente “a ciegas”	121
Time-Based Blind SQL Injection utilizando Heavy Queries	123
Marathon Tool	126
Reto Hacking I con Marathon Tool.....	127
10. Blind SQL Injection basada en errores	131
11. Aprovechando canales alternativos.....	133
12. Referencias	134

Capítulo IV

Objetivos Llamativos	135
1. Ejecutando programas.....	135
ORACLE.....	136
MySQL.....	146
SQL SERVER	146
2. Lectura y escritura de ficheros en aplicaciones web con SQL Injection	150
SQL SERVER y las fuentes de datos infrecuentes.....	152
Extrayendo un fichero de texto completo.....	156
Servidores vinculados y otras consideraciones sobre el uso de OLE DB y ODBC.....	157
Microsoft SQL Server 2000: opciones de carga masiva	158
Microsoft SQL Server 2005 & 2008: opciones de carga masiva	159
Creando ficheros en SQL Server	160
Aplicación práctica: comprimiendo una cadena	164
MySQL.....	165
Oracle Database	171
3. Cuentas de la base de datos	183
Listar los usuarios	183
Contraseñas de conexión a la Base de Datos	184
4. Automatizando con SQLmap	187
Ejecución de comandos.....	188
Archivos.....	193
Cuentas de usuario	195
Conclusiones	199
5. Referencias	199

Capítulo V

Otras diferencias entre DBMS.....	201
1. Sintaxis y construcciones	201
2. Información sobre la Base de Datos.	204
3. SQL Injection basada en errores.....	207
4. Algunos problemas típicos a la hora de inyectar código.....	215
Paréntesis.....	215
Inyecciones “zurdas”.....	216
Filtrados... insuficientes.....	218
Más medidas de seguridad... ..	232
Conclusiones	236

Capítulo VI

Escenarios avanzados	237
1. Arithmetic Blind SQL Injection	237
PoC: Soluciones para ABSQLi	238
PoC: Access y Arithmetic Blind SQL Injection	244
2. Explotación de SQLi en Access para ownear Windows.....	245
3. Obtener ventaja de las variables de sistema en MySQL.....	249
4. SQL Server in Paranoid Mode	251
5. Aplicación de la mínima exposición en servidores	255
6. Crea tu entorno práctico con Exploit-DB y los SQL Injection.....	257
Analizando las búsquedas y preparando entorno	257
7. Taint Analysis: Encontrando SQL Injection en el código fuente	260
Analizando plugins de wordpress	262
Índice de imágenes	265
Índice alfabético	269
Otros libros publicados.....	271