

Índice

Notas previas.....	9
Introducción. Las Inyecciones.....	11
Capítulo I. SQL Injection a partir de (casi) cero.....	13
1. Preparando el entorno.....	13
2. Login	17
3. Inyectando SQL.....	18
4. Una contramedida.....	20
5. Más allá del acceso.....	23
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”.....	59
13. Conclusiones.....	61
14. Referencias	62
Capítulo II. Serialized SQL Injection	63
1. PostgreSQL.....	63
1.1. Funciones para XML	64



1.2. Versiones anteriores a la 8.3.....	69
2. Microsoft SQL Server 2000, 2005 y 2008: Cláusula FOR XML.....	73
3. Serialized SQL Injection en MySQL	79
4. Serialized SQL Injection en Oracle Databases.....	82
5. Serialized SQL Injection basada en errores.....	85
6. Automatización	86
7. Referencias.....	91
Capítulo III. Blind SQL Injection	93
1. Inyección en condiciones más difíciles	93
2. Todo está hecho de números	96
3. Blind SQL Injection “clásica”.....	99
4. Todo está hecho de bits	100
5. Automatización	103
6. Herramientas	104
6.1. SQLInjector.....	104
6.2. SQLbftools.....	105
6.3. Bfsql	107
6.4. SQL PowerInjector	107
6.5. Absinthe.....	108
6.6. Un ejemplo con Absinthe.....	109
7. Otras herramientas.....	112
8. Optimizando el proceso.....	115
8.1. Maximizando la información de la respuesta	115
8.2. Minimizando los bits del problema.....	121
9. Time-Based Blind SQL Injection: Blind SQL Injection completamente “a ciegas”.....	129
9.1. Time-Based Blind SQL Injection utilizando Heavy Queries	131
9.2. Marathon Tool	134
9.3. Reto Hacking I con Marathon Tool	136
10. Blind SQL Injection basada en errores.....	139
11. Aprovechando canales alternativos	141
12. Referencias	142



Capítulo IV. Objetivos Llamativos	145
1. Ejecutando programas	145
1.1. ORACLE.....	146
1.2. MySQL	157
1.3. SQL SERVER	158
2. Lectura y escritura de ficheros en aplicaciones web con SQL Injection	162
2.1. SQL SERVER y las fuentes de datos infrecuentes	163
2.2. Extrayendo un fichero de texto completo	168
2.3. Servidores vinculados y otras consideraciones sobre el uso de OLE DB y ODBC	168
2.4. Microsoft SQL Server 2000: opciones de carga masiva.....	170
2.5. Microsoft SQL Server 2005 & 2008: opciones de carga masiva	171
2.6. Creando ficheros en SQL Server.....	172
2.7. Aplicación práctica: comprimiendo una cadena	176
2.8. MySQL	177
2.9. Oracle Database	184
3. Cuentas de la base de datos	196
3.1. Listar los usuarios	196
3.2. Contraseñas de conexión a la Base de Datos	197
4. Automatizando con SQLmap	200
4.1. Ejecución de comandos.....	200
4.2. Archivos.....	207
4.3. Cuentas de usuario.....	209
4.4. Conclusiones	213
5. Referencias	214
Capítulo V. Otras diferencias entre DBMS.....	215
1. Sintaxis y construcciones.....	215
2. Información sobre la Base de Datos.	218
3. SQL Injection basada en errores.....	222
4. Algunos problemas típicos a la hora de inyectar código	230
4.1. Paréntesis.....	230
4.2. Inyecciones “zurdas”	231
4.3. Filtrados... insuficientes.....	233
4.4. Más medidas de seguridad.....	247
4.5. Conclusiones	251



Capítulo VI. Escenarios avanzados.....253

- 1. Arithmetic Blind SQL Injection 253
 - 1.1. Poc: Soluciones para ABSQLi 254
 - 1.2. Poc: Access y Arithmetic Blind SQL Injection 261
- 2. Explotación de SQLi en Access para ownear Windows. 262
- 3. Obtener ventaja de las variables de sistema en MySQL..... 266
- 4. SQL Server in Paranoid Mode 268
- 5. Aplicación de la mínima exposición en servidores273

Índice de imágenes..... 277**Índice de palabras..... 281**