
14. SQL Injection
Julio Javier Iglesias Pérez
C|EH Julio Iglesias Pérez

Introducción

SQL Injection es la vulnerabilidad más común en Internet.

Es una falla en las aplicaciones Web y no así en los servidores Web o de Base de datos.

¿Qué es SQL Injection?

Es una técnica utilizada para tomar ventaja de las vulnerabilidades de entrada no válida para pasar los comando SQL a aplicaciones Web para su ejecución.

¿Qué es SQL Injection?

SQL Injection puede ser utilizado para realizar los siguientes tipos de ataque:

- Salto en la autenticación.
- Revelación de información.
- Integridad de los datos comprometida.
- Disponibilidad de los datos comprometida.
- Ejecución de código remoto.

¿Qué es SQL Injection?

Ejemplo de consulta SQL normal

```
SELECT Count(*) FROM Users WHERE
UserName='Jason' AND
Password='Sprinfield'
```

Ejemplo de SQL Injection

```
SELECT Count(*) FROM Users WHERE
UserName='Blah' or 1=1
--AND Password='Sprinfield'
```

Detección de SQL Injection

Paso 1: Revisar si la aplicación Web se conecta a un servidor de DB para acceder a algún dato.

Paso 2: Listar todos los campos de entrada, archivos ocultos, y solicitudes de post.

Paso 3. Intentar inyectar códigos dentro de los campos de entrada para generar un error.

Detección de SQL Injection

Paso 4. Intentar insertar una valor de cadena donde un número es esperado en el campo de entrada.

Paso 5. El operador UNION es utilizado en SQL Injections para unir una consulta a la consulta original.

Paso 6. Detallar los mensajes de error proveer una riqueza de información a un atacante para ejecutar SQL Injection.

Métodos adicionales para detectar SQL Injection

Fuzzing Testing. Function Testing.
Static/Dynamic Testing.

Ejemplo de function testing:

http://juggyboy/?parameter=123
http://juggyboy/?parameter=1'
http://juggyboy/?parameter=1'#
http://juggyboy/?parameter=1"
http://juggyboy/?parameter=1 AND 1=!--
http://juggyboy/?parameter=1 AND 1=2--
http://juggyboy/?parameter=1'/*
http://juggyboy/?parameter=1 order by 1000

SQL Injection Black Box Pen Testing

- Detectando problemas SQL Injection. Enviando comillas simples para atrapar instancias donde la entrada del usuario no está saneada. Dobles comillas para capturar instancias donde la entrada del usuario no está saneada.
- Detectando Modificación SQL. Utilizar brackets] como carácter de entrada para capturar instancias donde la entrada del usuario es utilizada como parte de un identificador SQL sin ser saneado.

SQL Injection Black Box Pen Testing

- Detectando problemas de truncado. enviar cadenas largas, para detectar buffer overruns. Esta acción puede mostrar errores en la página.

Tipos de SQL Injection

- SQL Injection simple
  - UNION SQL Injection.
  - Error Based SQL Injection.
- SQL Injection ciega

Ataque simple SQL Injection

- System Stored Procedire.
- Union Query.
- Tautology.
- Illegal/Logically Incorrect Query.
- End Line Comment.

Ejemplo UNION SQL Injection

Extrayendo tabla Column Names

```
http://juggyboy.com/page.aspx?id=1
UNION SELECT ALL 1,column_name,3,4 from
DB_NAME.information_schema.clumns
where table_name = 'EMPLOYEE_TABLE' --
```

SQL Injection Error Based

Extrayendo la primera tabla de la BD

```
http://juggyboy.com/page.aspx?id=1 or
1=convert(int, (select top 1 name from
sysobjects where xtype=char(85)))--
```

SQL Injection ciega

Es utilizado cuando una aplicación Web es vulnerable a SQL Injection pero los resultados de la inyección no son visibles para el atacante. Es idéntica a un SQL Injection normal excepto que cuando un atacante intenta explotar una aplicación, una página a medida es mostrada. Puede ser intensiva.

Como son retornados los mensajes de error, utilizar el comando "wait for" para revisar el estado de ejecución de SQL. Ej: waitfor delay '0:0:10'--

Metodología SQL Injection

1. Information Gathering. Extraer el nombre de la DB, versión, usuarios, mecanismo de salida, tipo de DB, nivel de privilegios de usuario y nivel de interacción con el S.O:

2. SQL Injection Vulnerability Detection. Listar todos los campos de entrada, ocultos, solicitudes post. Intentar inyectar códigos dentro de los campos para generar errores. Entrar ('), (;), (--), AND, OR en el campo de entrada, un mensaje de error significa vulnerabilidad.

Metodología SQL Injection

3. Lanch SQL Injection Attacks. Realizar Blind (Waitfor Delay) SQL Injection. Realizar errores basados en SQL Injection. Realizar uniones basadas en SQL Injection.

4. Extraer los Datos. Extraer nombres de tablas, columnas, datos.

5. Interact with the O.S. Extraer contraseñas de aplicaciones del S.O., acceder a los archivos del sistema y ejecutar comandos.

6. Compromise the network. Mecanismos de penetración adicionales en la red, instalar troyanos y keyloggers.

SQL Avanzada

Los mensajes de error son esenciales para extraer información sobre la base de datos.

- Tipos de bases de datos. SQL distintos tienen sintaxis distintas.
- Nivel de privilegio. Identificar el nivel de privilegio utilizado par ala base de datos, DBA, sysadmin, etc.
- Interacción con el S.O. A través de comandos se compromete toda la red.

Extrayendo información a través de los mensajes de error

- Grouping Error.
- Type Mismatch.
- Blind Injection.

Entendiendo las consultas SQL

- Inyecciones. La mayoría se encuentran en el medio de SELECT. SELECT casi siempre sigue o termina con la sección WHERE.
- Determinando El tipo de base de datos. La mayoría de las DB mostrará mensajes de error en la DB que se esté trabajando.
- La declaración Select: SELECT * FROM tabla WHERE....

Enumeración de DB, tabla y columna

1. Identificar el nivel de privilegio del usuario.
2. Administradores DB.
3. Descubrir la estructura DB.
4. Enumeración de columnas DB.

Enumeración Avanzada

Oracle

SYS.USER_OBJECTS

SYS.TAB.SYS.USER_TEBLES

SYS.USER_VIEWS

SYS.USER_TAB_COLUMNS

SYS.USER_CATALOG

Enumeración Avanzada

MS Access

MsysACEs

MsysObjects

MsysQueries

MsysRelationships

MySQL

msql.user

msql.host

mysql.db

Enumeración Avanzada

MS SQL Server

sysobjects

syscolumns

systypes

sysdatabases

Transfiriendo la DB a la máquina del usuario

SQL Server puede ser vinculado a la DB del atacante utilizando OPENROWSET

Interacción con el S.O.

Hay maneras de interactuar con el S.O.

1. Leyendo y escribiendo archivos del sistema desde el disco.
2. Ejecución de comandos directa vía shell remota.

Encontrar passwords y ejecutar comandos

Ambos métodos están restringidos por los privilegios y permisos de la DB.

Interacción con el FileSystem

LOAD_FILE()

Es utilizada para leer y retornar los contenidos de un archivo localizado en un servidor MySQL.

INTO OUTFILE()

Para ejecutar una consulta y arrojar los resultados en un archivo.

Herramientas

BSQLHacker: Herramienta automatizada SQL Injection que soporta Blind SQL Injection, Time Based Blind SQL Injection, Deep Blind SQL Injection, Error Based SQL Injection.

Herramientas

Marathon Tool: Para enviar consultas pesadas para realizar ataque Time-Based Blind SQL Injection.

- Extracción del esquema de DB desde SQL Server, Oracle y MySQL.
- Inyección de parámetros utilizando HTTP GET o POST.
- Soporta SSL.
- Conexión HTTP proxy disponible.
- Métodos de autenticación: anonymous, basíc, digest y NTLM.

Herramientas

Con Havij un atacante puede realizar un fingerprint, recibir Hashes usuarios y contraseñas, dumpear tablas y columnas, etc.

Evadiendo IDS

Los ataques utilizan técnicas de evasión para ocultar cadenas de entradas para impedir la detección de los sistemas de detección de firmas.

Los sistemas de detección basados en firmas construyen cadenas de ataques de SQL Injection (firmas) y luego compara las cadenas ingresadas con la firma de base de datos para detectar ataques.

Tipos de Técnicas de evasión de firma

- Matches sofisticados: Utilizar alternativamente la expresión "OR 1=1"
- Codificación HEX. Para representar una cadena SQL.
- Comentario in-line. Oculta las cadenas ingresadas insertando comentarios in-line entre las palabras clave SQL.
- Codificación de caracteres.

Tipos de Técnicas de evasión de firma

Técnica de evasión: Codificación HEX

Utiliza codificación hexadecimal para representar una cadena. Por ej, la cadena "SELECT" puede ser representada por el número hexadecimal: 0x736556c656174, lo cual no será detectado por los mecanismos de protección de firmas.

Tipos de Técnicas de evasión de firma

Técnica de evasión: Manipulando espacios en blanco

- Obstaculiza la entrada de cadenas quitando o agregando espacios en blanco entre la keyword SQL y la cadena o números.

Dropping spaces: 'OR'1=1' (sin espacios)

Tipos de Técnicas de evasión de firma

Técnica de evasión: Comentario in-line

Espacios en blanco entre las palabras clave SWL son remplazadas agregando comentarios /* */

UNION/**/SELECT/**/.....

Tipos de Técnicas de evasión de firma

Técnica de evasión: Codificación Char

La función Char() puede ser utilizado para inyectar declaraciones dentro de MySQL sin utilizar dobles cotas 'or username line char(37);

' union select * from users where login = char(114,111,111,116);

Tipos de Técnicas de evasión de firma

Técnica de evasión: Concatenación de cadena

Dividir instrucciones para impedir la detección de firmas utilizando comandos de ejecución que permitan concatenar texto en el servidor de DB.

MS SQL: EXEC ('DRO' + 'P T' + 'AB' + 'LE')

MySQL: EXECUTE CONCAT ('INSE','R T US','ER')

Tipos de Técnicas de evasión de firma

Técnica Códigos ocultos

¿Cómo defenderse contra ataques SQL Injection?

- No hacer supuestos sobre tamaño, tipo o contenido de los datos cuando es recibida por la aplicación.
- Probar el tamaño y el tipo de datos de entrada y forzar límites apropiados para prevenir buffer overruns.
- Probar el contenido de las cadenas de variables y aceptar solo valores esperados.
- Rechazar entradas que contengan datos binarios, secuencias escape, y caracteres comentario.

¿Cómo defenderse contra ataques SQL Injection?

- Nunca construir declaraciones de transacciones SQL directamente desde la entrada del usuario y utilizar procedimientos almacenados para validar la entrada del usuario.
- Implementar capas múltiples de validación y nunca concatenar entradas de usuarios que no son válidas.
- Que la entrada sea tratada como un valor literal en vez de un código ejecutable.
- Los checks y tipos deben ser forzados utilizando colección de parámetro.

Herramientas de detección de SQL Injection

- Microsoft Source Code Analyzer: Para encontrar vulnerabilidades de SQL Injection en código ASP. Escanea código fuente ASP y genera advertencias relacionadas a vulnerabilidades SQL Injection de primer orden y segundo orden.

Herramientas de detección de SQL Injection

- Microsoft UrlScan: Restringe los tipos de solicitudes HTTP que el IIS procesa. Bloquea solicitudes HTTP específicas, previniendo potencial solicitudes perjudiciales de las aplicaciones que llegan en el servidor.

Herramientas de detección de SQL Injection

- dotDefender: Wen Application Firewall. Complementa al firewall de red, IPS y otros. Inspecciona tráfico HTTP/HTTPS sospechoso. Detecta y bloquea ataques SQL Injection.
- IMB AppScan: Escaneador de seguridad en las aplicaciones Web. Previene ataques SQL Injection en los Sitios Web. Escanea sitios en búsqueda de malware introducido.

Reglas Snort para detectar ataques SQL Injection

```
/(\%27|(\')|(\-\-)|(\%23)|(#)/ix
/exec*\s|\+)+*s|x)p\w+/ix
i((\%27)|(\'))union/ix
^w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%
52))/ix
```


¡Muchas Gracias!
C|EH Julio Iglesias Perez