AUDITORÍA EN APLICACIONES WEB: INYECCIÓN SQL

Nara Abril Nanfara

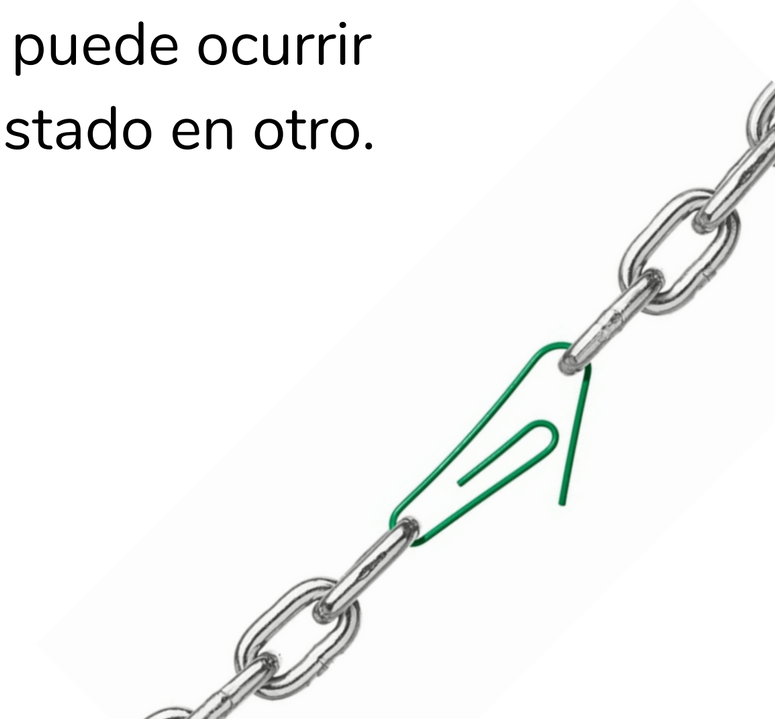
¿Qué es una inyección SQL?

Consiste en la inserción o "inyección" de una consulta SQL a través de los datos de entrada del cliente a la aplicación.
Un exploit de inyección SQL exitoso puede leer datos confidenciales de la base de datos, modificar los datos de la base de datos, ejecutar operaciones de administración en la base de datos, recuperar el contenido de un archivo dado presente en el archivo DBMS system y, en algunos casos, emitir comandos para el sistema operativo.

La vulnerabilidad

Se vale de una vulnerabilidad informática presente en una aplicación al nivel de **validación de las entradas** para realizar operaciones sobre una base de datos. El origen de la vulnerabilidad radica en la **incorrecta comprobación o filtrado de las variables** utilizadas en un programa que contiene o genera código SQL.

Es un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o script que esté incrustado en otro.



Inyección SQL y OWASP

La inyección SQL está contemplado en OWASP Top 10 como A1:2017 - Injection

- SQL Injection Prevention Cheat Sheet.
- OWASP Query Parameterization Cheat Sheet.
- OWASP Code Review Guide
- **OWASP Testing Guide**

Testing: Técnicas de detección

¿Cuándo la aplicación interactúa con un servidor de base de datos?

Típicamente: formularios de autenticación, motores de búsqueda y E-Commerce

¿Qué campos de entrada tiene valores que podrían usarse para elaborar una consulta SQL?

Solicitudes POST, encabezados HTTP y cookies.

¿Cómo probarlos?

Agregar una comilla simple (‘) o un punto y coma (;)

Utilizar delimitadores de comentarios (--o /* */, etc.) y otras palabras clave SQL como AND y OR para intentar modificar la consulta.

Simplemente insertar una cadena donde se espera un número.

Testing: Fingerprinting the DataBase

El lenguaje SQL es un estándar, pero cada DBMS tiene su peculiaridad.
La mejor forma es observando los errores.

Testing: Prueba de inyección SQL standar

SELECT * FROM Users WHERE Username='$username' AND Password='$password'

SELECT * FROM Users WHERE Username='1' OR '1'='1' AND Password='1' OR '1'='1'

SELECT * FROM products WHERE id_product=$id_product

SELECT * FROM products WHERE id_product=$id_product; INSERT INTO users (...)

SELECT * FROM products WHERE id_product=$id_product

http://www.example.com/product.php?id=10 AND 1=2

Testing: Técnicas de explotación

Técnica de explotación union

Técnica de explotación booleana

Técnica de explotación basada en errores

Técnica de explotación fuera de banda

Técnica de explotación por demora

Testing: Técnica de explotación sindical

Usando el operador UNION

1. Encontrar el número correcto de columnas.
2. Averiguar el tipo de columnas.
3. Localizar qué muestra la aplicación de la respuesta a la consulta.
4. Obtener los metadatos que nos interesen.
    a. Nombres de tablas.
    b. Nombres de columnas.
5. Estamos en condiciones de hacer las consultas.

Testing: Explotación automatizada SQLMap

SQLmap es una herramienta de prueba de penetración que automatiza el proceso de detección y explotación de fallas de inyección SQL.

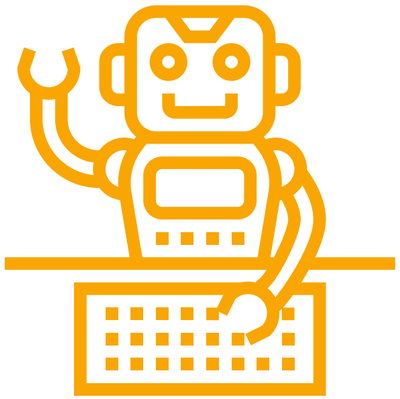
```
sqlmap.py -u "http://192.168.0.106/cat.php?id=1" --dbs --dump-all –batch
```

-u: URL

--dbs: enumera los SGBD

--dump-all: Vuelca todas las entradas de las tablas de bases de datos

--batch: Nunca pide inputs, usa el comportamiento predeterminado por lotes



¡Gracias!