Evaluación de Vulnerabilidad por Inyección SQL en DVWA

Introducción

Este informe documenta una prueba controlada de seguridad realizada en un entorno de laboratorio usando la aplicación vulnerable Damn Vulnerable Web Application (DVWA), con el objetivo de demostrar la existencia y explotación de una vulnerabilidad de inyección SQL. Esta actividad forma parte de un ejercicio de concienciación y entrenamiento en ciberseguridad.

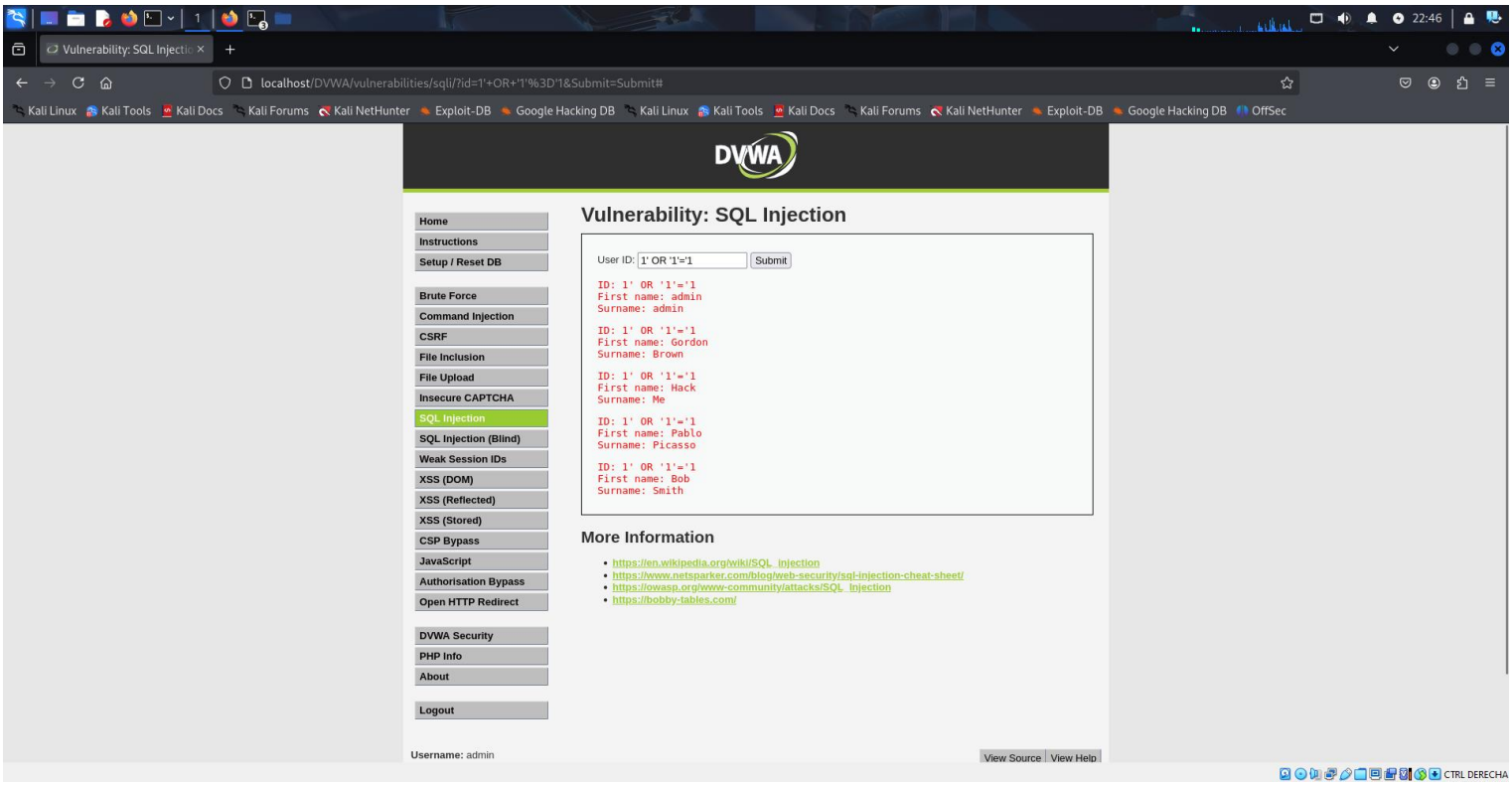
Descripción del Incidente

Durante la prueba, se identificó una vulnerabilidad crítica de tipo SQL Injection en el parámetro User ID del módulo correspondiente. Esta falla permite a un atacante inyectar comandos SQL maliciosos en el sistema, lo que puede provocar la exposición no autorizada de datos almacenados en la base de datos como los usuarios registrados con sus contraseñas actualizadas.

La inyección utilizada fue: 1' OR '1'='1

Esta cadena engaña a la consulta SQL subyacente para que devuelva todos los registros de la base de datos, sin necesidad de autenticación válida.

Proceso de Reproducción



1. Acceder a DVWA (Damn Vulnerable Web Application) a través de http://localhost/DVWA.

2. Seleccionar el módulo “SQL Injection” del menú lateral.

3. En el campo User ID, ingresar la cadena: 1' OR '1'='1.

4. Hacer clic en “Submit”.

5. Como resultado, se muestran todos los registros disponibles en la base de datos, incluyendo usuarios con privilegios administrativos.

Impacto del Incidente

- Divulgación de Información Sensible: Se exponen datos personales como nombres, apellidos y usuarios administrativos.
- Acceso No Autorizado: Es posible eludir controles de acceso.
- Escalada de Privilegios: Puede derivar en comprometer toda la base de datos.
- Integridad y Confidencialidad Amenazada: Riesgo de manipulación de datos o robo de información.

Recomendaciones

- Uso de consultas preparadas (prepared statements) con parámetros en lugar de concatenar cadenas SQL.
- Validación y sanitización de entradas del usuario.
- Uso de ORM (Object-Relational Mapping) que abstrae la interacción directa con SQL.
- Implementar controles de acceso robustos y segmentación de privilegios en la base de datos.
- Activar logs de acceso y auditoría para detectar comportamientos anómalos.
- Actualizar frameworks y librerías a versiones seguras.

Conclusión

La prueba confirmó una vulnerabilidad grave en el campo User ID al ingresar el comando “1' OR '1'='1.”, que permite acceder a toda la base de datos sin autenticación. Este tipo de falla puede poner en riesgo información confidencial y permitir a un atacante tomar control total del sistema. Es urgente corregir esta falla y aplicar medidas de seguridad como validar entradas y usar consultas seguras para evitar futuros ataques.