INYECCIÓN SQL EN LA APLICACIÓN WEB DVWA

Introducción:

En este proyecto, se va a realizar una explotación SQL a la aplicación web Damn Vulnerable Web Application (DVWA). Esta aplicación permite realizar estos ensayos, pues está en un entorno controlado, ya que ha sido configurada para la realización de estos test.

Descripción y método usado:

Durante la prueba de seguridad, se pudo comprobar una vulnerabilidad de inyección SQL en el formulario de identificación por "ID del usuario". Se verifica que al realizar una consulta SQL, se puedo obtener información de los usuarios de la base de datos.

Exploit utilizado:

Se utilizó la siguiente cadena para explotar la vulnerabilidad:

1' or '1' = '1

Al ejecutar esta consulta, el atacante puede evadir el filtro de autenticación o manipular las consultas a la base de datos para obtener acceso a información confidencial.

Impacto del incidente:

El atacante ha podido acceder a información confidencial, en este caso ha extraído datos del usuario administrador y de cuatro usuarios más.

Recomendaciones:

Para evitar este tipo de accidentes podemos realizar:

- ✓ Test de Penetración → con este método se puede evaluar la seguridad de nuestro sistema y poder identificar vulnerabilidades.
- ✓ Aplicar principios de privilegio mínimo en la base de datos.
- ✓ Realizar validaciones de entradas estrictas en todos los campos de usuario.

Adjunto imagen de los datos extraídos tras realizar la inyección SQL.