Vulnerabilidad campo User ID

Germán Alberto Parra Araque

4Geeks

Bogotá 2025

Introducción

En este documento se presentará un incidente encontrado en un ejercicio académico dentro de la plataforma DVWA. El objetivo de esta práctica es simular la detección y análisis de un incidente de ciberseguridad con fines educativos, como parte del entrenamiento del bootcamp de ciberseguridad.

Descripción del Incidente

Durante una práctica académica en la plataforma DVWA (Damn Vulnerable Web Application), se identificó una vulnerabilidad en uno de los formularios web que permite realizar pruebas de **SQL Injection**.

En el módulo correspondiente a esta vulnerabilidad, se observó que el sistema no implementa mecanismos adecuados de validación o sanitización de entradas del usuario. Aprovechando esta debilidad, se ejecutaron consultas SQL maliciosas que lograron acceder a información sensible contenida en la base de datos.

Mediante una inyección básica, se obtuvieron los registros almacenados en la tabla “users” de la base de datos DVWA, revelando información como:

- Nombres de usuario
- Apellido del usuario

Este comportamiento representa un riesgo alto, ya que en un entorno real permitiría a un atacante obtener acceso no autorizado a credenciales de usuarios y posiblemente comprometer el sistema.

Proceso de reproducción

Este incidente se reproduce con los siguientes requisitos

- Tener una máquina virtual con un sistema Linux instalado(Se usó Debían 12).
- Contar con MariaDB (MySQL) configurado y previamente configurado.
- Tener php configurado.

Se accede al sistema Linux y mediante la terminal se descarga el aplicativo DVWA. Se usan los siguientes comandos:

- `cd /var/www/html`

  Cambiamos al directorio “html” donde se encuentran (normalmente) los servicios WEB del sistema Linux

- `sudo apt-get install wget unzip`

  Se hace la instalación del mediante privilegios de administrador de los paquetes wget y unzip

- `sudo wget https://storage.googleapis.com/breathecode/virtualbox/DVWA.zip && sudo unzip DVWA.zip`

Permite descargar una archivo comprimido de la web indicada y mediante unzip descomprimir lo descargado, todo esto con privilegios de administrador.

- `sudo mv DVWA-master DVWA`

  Se mueve el directorio "DVWA-master" a "DVWA" (El directorio "DVWA-master" puede ser diferente).

- `cd DVWA/config`

  Se ingresa al directorio "DVWA/config"

- `sudo cp config.inc.php.dist config.inc.php`

  Con privilegios de administrador se realiza el renombramiento de archivo "`config.inc.php.dist`" a "`config.inc.php`"

- `sudo nano config.inc.php`

  Con privilegios de administrador se ingresa mediante el editor de texto "nano" al archivo "`config.inc.php`"

- Se verifica que las variables estén configuradas con los datos de la base de datos MariaDB

  $_DVWA['db_user'] = 'root';

$_ DVWA['db_password'] = 'tu_contraseña_de_root';

$_DVWA['db_database'] = 'dvwa';

- Dentro la terminal de Linux nuevamente se utiliza el comando "`sudo mysql -u root -p`" para ingresar al CLI (Command Line Interface) de MariaDb. Se nos pedirá contraseña del usuario administrador.
- Al ingresar al CLI se escribe el comando "CREATE DATABASE dvwa;" para crear la base de datos DVWA. Al concluir salimos de CLI con el comando "EXIT;"
- Nuevamente dentro de la terminal, se cambiará de manera recursiva el propietario y el grupo de la directorio DVWA "`sudo chown -R www-data:www-data /var/www/html/DVWA/`"
- Se ejecuta este comando para otorgar todos los permisos sobre el archivo al propietario "`sudo chmod -R 755 /var/www/html/DVWA/`". Asimismo se otorgaron permisos de lectura a usuarios del grupo "www-data" y a otros usuarios.

Después de hacer la ejecución de los comandos mencionados previamente, se configurara el aplicativo web DVWA:

- Se accede mediante http://localhost/DVWA/setup.php
- Se necesita crear o reiniciar la base de datos dentro del aplicativo web (ver imagen)

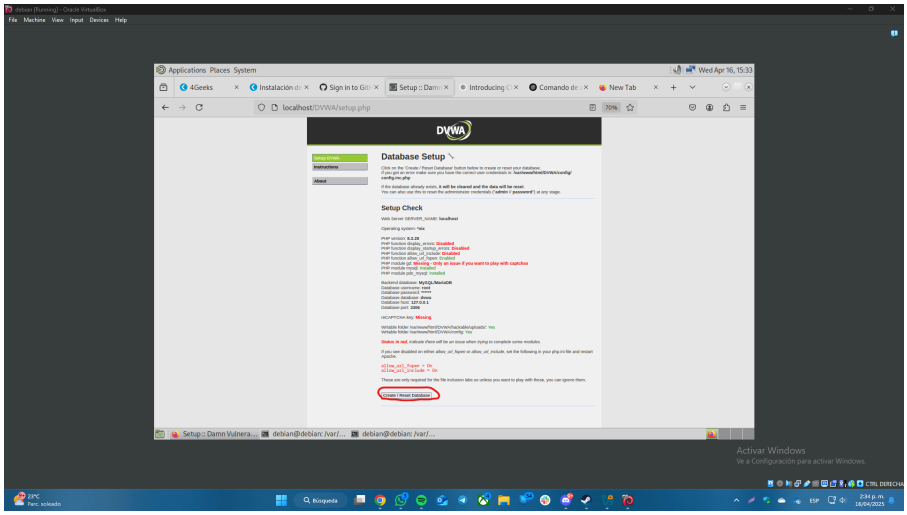

Imagen 1: Creación/reinicio base de datos DVWA

- Se debe autenticar (*Usuario: admin *Contraseña: password).
- Se configura el tipo de seguridad del aplicativo web en la opción “DVWA security" (menú lateral). Se establece el valor de seguridad en “Low” y se usa el botón de submit.
- Se identifica en el menú lateral la opción “SQL Injection”, se ingresa y dentro del campo de entrada “User id”, colocar la siguiente cadena de caracteres “1' OR '1'='1”

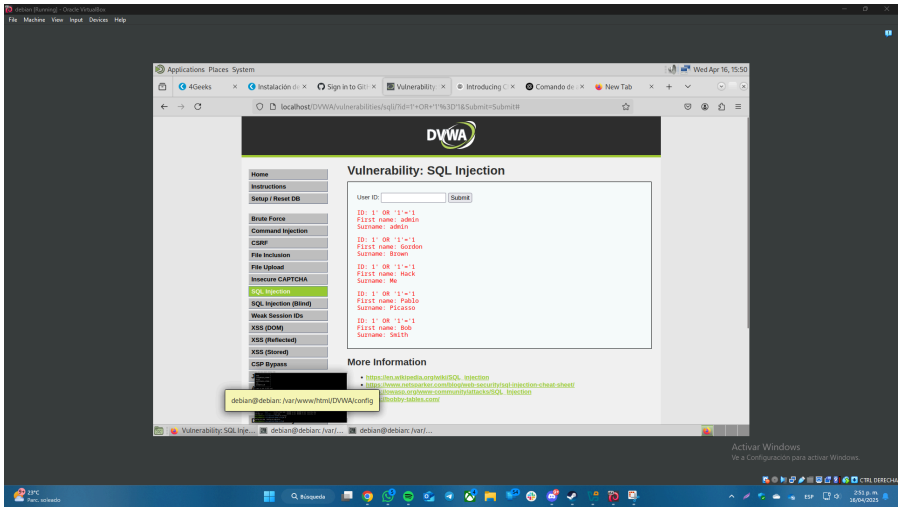

Imagen 2: Vulnerabilidad SQL-Injection

Impacto del incidente

El ataque SQL Injection al que el sistema es vulnerable (DVWA), genera un problema dentro de la base de datos, el cual culmina con la entrega de los registros de la tabla “users”. Esta vulnerabilidad permite que un usuario malintencionado tenga acceso a la tabla que usa el campo de entrada “User Id” para consultar la información protegida.

Esto puede generar entrega de información protegida por el aplicativo, por lo cual puede generar diferentes incidentes de seguridad.

RECOMENDACIONES

Es necesario entender que la ejecución del ataque SQL-injection presenta información que debería estar protegida por la base de datos, por lo cual es necesario hacer un proceso de auditoría, sobre el aplicativo web.

Es necesario revisar los campos de entrada y hacer un proceso de sanitizar las entradas que se le otorgan al usuario. Es necesario establecer una planeación para el equipo red team y que realice pruebas sobre el aplicativo web.

Es necesario concientizar al equipo de desarrollo del aplicativo para evitar este posible ataque.

CONCLUSIÓN

La presente práctica permitió comprender de manera práctica cómo funciona una vulnerabilidad del tipo **SQL Injection** y cuál es su impacto potencial en una aplicación web. A través del entorno controlado de DVWA, se logró explotar esta debilidad para acceder a información sensible almacenada en la base de datos, demostrando la facilidad con la que un atacante puede comprometer la confidencialidad de los datos cuando no se implementan mecanismos adecuados de validación de entradas.

En conclusión, el ataque de SQL Injection es una amenaza crítica pero prevenible.