Informe de Vulnerabilidad: SQL Injection en DVWA

1. Contexto y Descripción de la Vulnerabilidad

En muchas aplicaciones web, como una tienda en línea, los usuarios utilizan una caja de búsqueda para encontrar productos. Esta caja interactúa con una base de datos usando SQL (Structured Query Language), un lenguaje que permite consultar y manipular datos.

Si la aplicación no valida o sanitiza correctamente las entradas del usuario, un atacante puede insertar código SQL malicioso. Por ejemplo, ingresando el siguiente texto:
' OR 1=1 --
Este fragmento hace que la condición de búsqueda siempre sea verdadera, logrando que la base de datos retorne toda la información, incluyendo datos sensibles como usuarios y contraseñas.

2. Procedimiento Realizado

- Se instaló DVWA (Damn Vulnerable Web Application) en un servidor Apache corriendo sobre Debian.
- Se configuró DVWA para establecer la seguridad en nivel mínimo, facilitando la explotación.
- Se ingresó la cadena SQL maliciosa ' OR 1=1 -- en la caja de búsqueda o login simulando un ataque.
- Como resultado, se obtuvo acceso a datos confidenciales (usuarios y contraseñas) que normalmente deberían estar protegidos.

3. Resultados y Observaciones

- La aplicación no validó la entrada del usuario, permitiendo la inyección SQL.
- Se mostró información sensible y privilegiada que pone en riesgo la seguridad del sistema.
- Esto demuestra que una vulnerabilidad SQL Injection sin control puede comprometer completamente la base de datos y los datos almacenados.

4. Recomendaciones

- Implementar validación y sanitización estricta de todas las entradas del usuario.
- Utilizar consultas preparadas (prepared statements) o procedimientos almacenados para evitar concatenación directa de SQL.
- Configurar el nivel de seguridad en aplicaciones web para evitar vulnerabilidades.
- Realizar auditorías y pruebas de penetración periódicas para detectar este tipo de fallos.
- Restringir accesos a bases de datos y proteger credenciales con buenas prácticas (hashing, salting).

5. Conclusión

El ejercicio con DVWA nos permitió simular un ataque SQL Injection y evidenciar cómo esta vulnerabilidad puede permitir a un atacante obtener acceso a información sensible en un servidor web. Es fundamental asegurar que las aplicaciones validen correctamente los datos de entrada para proteger la confidencialidad, integridad y disponibilidad de

la información.

6. Comandos / Pasos Ejecutados

```
# Instalación de DVWA y configuración en Apache/Debian (resumen):
sudo apt-get update
sudo apt-get install apache2 php php-mysqli git
cd /var/www/html
sudo git clone https://github.com/digininja/DVWA.git
sudo chown -R www-data:www-data DVWA/
sudo service apache2 restart

# Configuración de DVWA (desde interfaz web)
# - Ajustar nivel de seguridad a "Low"
# - Ingresar en la caja de búsqueda o login: ' OR 1=1 --

# Resultado: Listado de usuarios y contraseñas visibles
```