# Informe de incidente de vulnerabilidad de SQL Injection — DVWA

Joao Paulo Nobre Medeiros

## Introducción

Este informe describe la identificación y explotación de una vulnerabilidad de inyección SQL descubierta durante una evaluación de seguridad de Damn Vulnerable Web Application (DVWA) para un proyecto de 4Geeks.

El objetivo de este informe es documentar la vulnerabilidad, explicar cómo se reprodujo, evaluar su impacto potencial y proporcionar recomendaciones para mitigar el riesgo de acuerdo con las mejores prácticas de seguridad de la información.

## Descripción del incidente

Durante la prueba, se identificó una vulnerabilidad de inyección SQL en el módulo de inyección SQL de la aplicación DVWA.

La aplicación no valida adecuadamente la entrada del usuario en el campo «ID de usuario», lo que permite que se ejecuten consultas SQL maliciosas directamente en la base de datos back-end y se obtenga información.

## Proceso de reproducción

**1.** Accedí a la aplicación DVWA a través del navegador en http://localhost/DVWA.

**2**. Inicié sesión en la aplicación con las credenciales predeterminadas (admin / password).

**3**. Establecí el nivel de seguridad en BAJO en la configuración de seguridad de DVWA.

**4**. Navegué hasta el módulo SQL Injection.

**5.** Introduje la siguiente carga útil en el campo ID de usuario:

1' OR '1'='1

**6.** Envié la solicitud.

*La aplicación devolvió todos los registros de usuario de la base de datos.*

Impacto del incidente

Esta vulnerabilidad representa un riesgo crítico para la seguridad, ya que permite a los atacantes obtener información confidencial de la base de datos sin autorización.

Los impactos potenciales incluyen el acceso no autorizado a los datos del usuario, la exposición de información confidencial y la posible manipulación o eliminación de registros de la base de datos.

Si se explota en un entorno de producción, esta vulnerabilidad puede provocar violaciones de datos y comprometer la integridad del sistema.

Recomendaciones

Mitigar esta vulnerabilidad

Implementar instrucciones preparadas

Validar todas las entradas del usuario

Aplicar el principio de privilegio mínimo a las cuentas de la base de datos

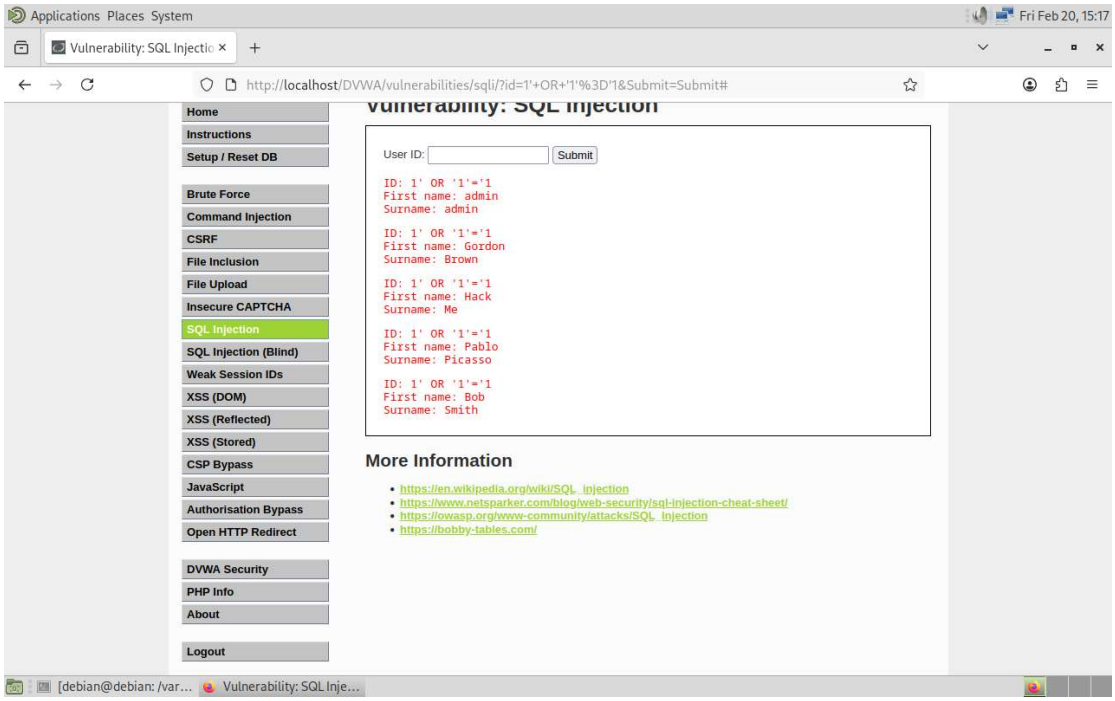
Seguir prácticas de codificación segura basadas en las directrices de OWASP

Y realizar siempre pruebas de seguridad

Conclusión

La vulnerabilidad de inyección SQL identificada en el entorno DVWA destaca la importancia de la validación adecuada de las entradas y la interacción segura con la base de datos.

La implementación de controles de seguridad adecuados puede reducir significativamente el riesgo de vulnerabilidades similares.


Applications Places System
Fri Feb 20, 15:17
Vulnerability: SQL Injectic
http://localhost/DVWA/vulnerabilities/sqli/?id=1'+OR+'1'%3D'1&Submit=Submit#
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: 1' OR '1'='1
First name: admin
Surname: admin
ID: 1' OR '1'='1
First name: Gordon
Surname: Brown
ID: 1' OR '1'='1
First name: Hack
Surname: Me
ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso
ID: 1' OR '1'='1
First name: Bob
Surname: Smith
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
[debian@debian: /var...
Vulnerability: SQL Inje...