

## Reporte de Incidente: Inyección SQL en DVWA

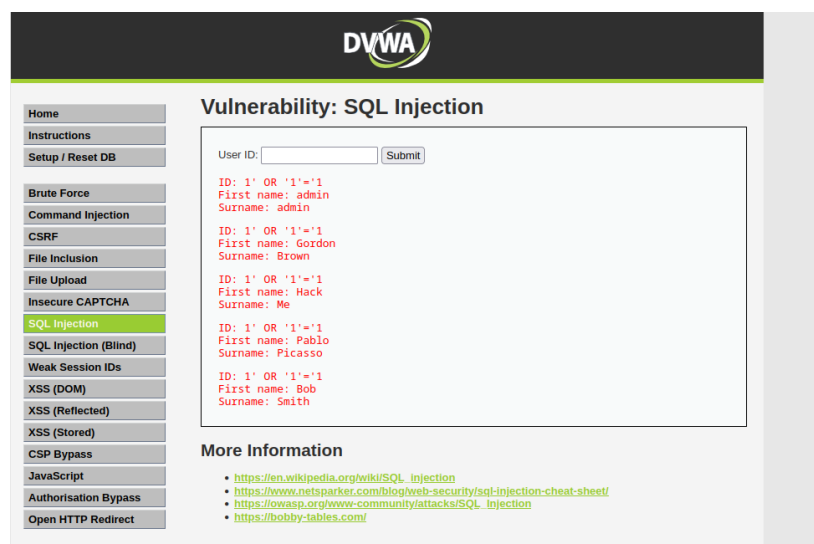
El siguiente reporte se documenta un ejercicio en un entorno controlado y virtual para probar la seguridad en la aplicación DVWA, explotando una vulnerabilidad de inyección SQL en un entorno Debian con Apache, MariaDB y PHP.

### Descripción del incidente

Se identifica una vulnerabilidad de inyección SQL con la sección SQL injection de DVWA, esto permitiría la manipulación de consultas hacia la base de datos dvwa creada para el ejercicio. Se produce por una falta de sanitización en los parámetros que ingresa un usuario a través de un formulario web.

### Proceso de Reproducción

1. Se accede a <http://localhost/DVWA/>
2. Ingresamos las credenciales:
  - a. Usuario: admin
  - b. Contraseña password
3. En el menú de navegación izquierdo seleccionamos SQL injection.
4. En el campo User ID, ingresamos lo siguiente:
  - a. 1' OR '1'='1
5. Clic en Submit
6. La aplicación devuelve la lista de los usuarios existentes en la base de datos:



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left is a navigation menu with various security exercises. The 'SQL Injection' option is highlighted in green. The main content area is titled 'Vulnerability: SQL Injection'. It features a 'User ID:' input field with the value '1' OR '1'='1' and a 'Submit' button. Below the input field, the application displays the results of the query in red text, showing a list of users: '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'; and 'ID: 1' OR '1'='1', 'First name: Bob', 'Surname: Smith'. At the bottom, there is a 'More Information' section with links to external resources.

**DVWA**

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

**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://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://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

## **Impacto del Incidente**

- La vulnerabilidad permite el acceso a información sensible (nombre y apellido)
- Una vulnerabilidad de inyección que ha funcionado da pie a que se prueben otras como la de ingresar datos a la base de datos.

## **Recomendaciones**

- Implementar consultas preparadas (prepared statements) para prevenir inyecciones SQL.
- Validar y sanitizar entradas del usuario utilizando funciones como `mysqli_real_escape_string` o filtros de tipo.
- Aumentar el nivel de seguridad de DVWA a High o Impossible.
- Ejecutar pruebas regulares de seguridad automatizadas y revisiones de código

## **Conclusión**

El incidente identificado corresponde a una vulnerabilidad en la validación de entradas en el módulo SQL de DVWA. Corresponde a una vulnerabilidad crítica debido a que su explotación es de fácil utilización, y que deja vulnerables datos importantes de la base de datos como son los datos personales.