




## Ejercicio Práctico

 **Título:** Explotación controlada de una inyección SQL y documentación de hallazgo en entorno DVWA

---

### Objetivo:

Simular una auditoría real sobre una aplicación vulnerable, identificar una falla de tipo **Inyección SQL (SQLi)**, validarla manualmente con herramientas profesionales y generar un informe técnico claro y profesional del hallazgo.

---

### Escenario:

La organización te ha pedido realizar una auditoría interna sobre su aplicación web de pruebas, **DVWA**, la cual corre localmente en un entorno controlado. Debes encontrar si la sección de usuarios es vulnerable a SQL Injection y documentar tus hallazgos como lo harías en un entorno profesional.

---

### Actividades:

---

#### Paso 1 – Configuración inicial

1. Accede a DVWA en tu navegador: <http://localhost/dvwa>
2. Inicia sesión con:
  - Usuario: [admin](#)
  - Contraseña: [password](#)
3. Configura el **Security Level** en “Low”.

---

## ✓ Paso 2 – Análisis del módulo vulnerable

1. Navega al módulo “**SQL Injection**”.
2. Usa **Burp Suite** o **OWASP ZAP** para interceptar la petición al enviar un **User ID**.
3. Analiza la estructura del parámetro enviado (**id=**) en la URL o cuerpo de la solicitud.

---

## ✓ Paso 3 – Prueba manual de inyección

Usa el siguiente payload como prueba:

1' OR '1'='1

- 1.
2. Observa si el sistema retorna más resultados de lo habitual (usuarios adicionales, errores de base de datos, etc.).

Intenta un payload más avanzado:

1' UNION SELECT null, database(), null --

- 3.

---

## ✓ Paso 4 – Validación en Burp Suite (opcional)

1. Usa **Repeater** para reenviar la misma solicitud varias veces con payloads distintos.
2. Observa cómo responde el servidor a cada uno de ellos.
3. Documenta los cambios en la respuesta (HTML modificado, nuevos resultados, errores SQL visibles, etc.).

---

## ✓ Paso 5 – Documentación profesional del hallazgo

Elabora un informe estructurado con los siguientes apartados:

1. Título del Hallazgo

2. Descripción del Problema
  3. Evidencia Técnica (payloads, respuestas, capturas)
  4. Evaluación de Riesgo
  5. Recomendación Técnica
  6. Referencias (CVSS, OWASP, etc.)
- 

### **Entregables:**

1. Capturas de pantalla del entorno antes y después de la explotación.
  2. Detalle de los payloads utilizados.
  3. Resumen técnico del comportamiento observado.
  4. Informe técnico redactado en estilo profesional.
- 

### **Reflexión final:**

- ¿Por qué la inyección funcionó?
  - ¿Cómo podrías evitar que estas consultas SQL sean manipuladas?
  - ¿Qué hubiera pasado si el sistema estuviera en producción?
-