




Ejercicio Práctico

 **Título:** Identificación, explotación y documentación de una inyección de comandos en DVWA

Objetivo:

Simular una auditoría de seguridad en el entorno DVWA para detectar y explotar una vulnerabilidad de **inyección de comandos del sistema operativo**, documentando técnicamente el hallazgo y generando recomendaciones para su mitigación.

Escenario:

Se ha solicitado una auditoría ética a la aplicación vulnerable **DVWA**, que corre en un entorno de laboratorio. Tu objetivo será evaluar si el módulo "Command Injection" permite la ejecución de comandos arbitrarios y documentar el impacto potencial de esta falla.

Instrucciones:

Paso 1 – Acceso y configuración

1. Ingresa a DVWA desde <http://localhost/dvwa>.
 2. Inicia sesión con las credenciales:
 - Usuario: [admin](#)
 - Contraseña: [password](#)
 3. Cambia el nivel de seguridad a **Low** desde "DVWA Security".
-

✓ Paso 2 – Ingreso al módulo vulnerable

1. Accede a la sección “**Command Injection**” desde el menú lateral.
 2. El módulo solicita una dirección IP para hacer ping. Este campo es vulnerable si no se filtran correctamente los datos ingresados.
-

✓ Paso 3 – Prueba de vulnerabilidad

Ingresa una dirección IP válida seguida de un separador de comandos. Ejemplo (en Linux):

127.0.0.1; whoami

- 1.
 2. Envía el formulario.
 3. Observa si en la respuesta se muestra el resultado del comando `whoami`, lo cual indicaría que se ejecutó desde el sistema operativo del servidor.
-

✓ Paso 4 – Prueba avanzada

Repite el proceso utilizando otros comandos controlados como:

127.0.0.1; uname -a

127.0.0.1 && id

- 1.
 2. Analiza los resultados devueltos.
-

✓ Paso 5 – Documentación profesional del hallazgo

Prepara un informe con el siguiente formato:

1. Título del hallazgo
 2. Descripción técnica del problema
 3. Evidencia (capturas, comandos utilizados, resultados)
 4. Evaluación del riesgo
 5. Recomendación de mitigación
 6. Referencias (OWASP, CWE, CVSS)
-

Entregables esperados:

1. Capturas del comportamiento del sistema ante los comandos.
 2. Resumen técnico de los payloads y resultados.
 3. Informe estructurado del hallazgo.
 4. Reflexión sobre los riesgos reales de este tipo de falla.
-

Preguntas de reflexión:

- ¿Por qué el sistema ejecutó comandos desde un campo de formulario?
 - ¿Qué consecuencias tendría esta falla si el sistema estuviera en producción?
 - ¿Qué soluciones pueden evitar que las aplicaciones ejecuten código no autorizado?
-