**Informe Técnico**

**Inyección de Comandos en el Módulo “Command Injection” – DVWA (entorno controlado)**

**1. Título del Hallazgo**

**Vulnerabilidad de Inyección de Comandos del Sistema Operativo en DVWA**

**2. Descripción Técnica del Problema**

Durante una auditoría de seguridad realizada en el entorno de laboratorio **DVWA (Damn Vulnerable Web Application)**, se detectó que el módulo “Command Injection” es vulnerable a **OS Command Injection**.  
El campo que solicita una dirección IP para ejecutar un comando ping no valida ni sanitiza la entrada, lo que permite a un atacante inyectar instrucciones adicionales del sistema operativo y obtener información del servidor.

**3. Evidencia Técnica**

**Herramientas utilizadas:**

* Navegador web con acceso a DVWA en http://localhost/dvwa
* **Burp Suite** para interceptar y modificar solicitudes

**Comandos de prueba utilizados:**  
1.

127.0.0.1; whoami

✔ Resultado: la respuesta mostró el usuario con el que corre el servidor web.

127.0.0.1; uname -a

✔ Resultado: se obtuvo información del kernel del sistema operativo.

127.0.0.1 && id

✔ Resultado: se devolvió el identificador de usuario y grupos.

**Evidencia (resumen):**

* El servidor ejecutó comandos arbitrarios concatenados desde el campo del formulario.
* Se confirmó que no existen filtros de validación en la entrada.

**4. Evaluación del Riesgo**

* **Clasificación:** Crítico
* **Impacto:**
  + Ejecución remota de comandos.
  + Acceso no autorizado a información sensible del servidor.
  + Posible escalada a compromiso total del sistema.
* **Severidad (CVSS v3.1):** 9.8 (Critical)
* **Referencia CWE:** CWE-78 – Improper Neutralization of Special Elements in OS Command

**5. Recomendación de Mitigación**

1. Implementar **validación estricta de entradas**, limitando la entrada a valores esperados (ej. solo direcciones IP válidas).
2. Usar funciones seguras que no ejecuten comandos directamente, sino librerías propias del lenguaje (ej. funciones de red).
3. Configurar el servidor para ejecutar procesos web con usuarios de privilegios mínimos.
4. Aplicar un **WAF (Web Application Firewall)** para detectar patrones de inyección de comandos.
5. Realizar pruebas periódicas con herramientas de análisis dinámico y estático.

**6. Referencias**

* OWASP Testing Guide – Command Injection
* CWE-78: Improper Neutralization of OS Command Elements
* OWASP Top 10 – A03:2021 Injection

**7. Reflexión Final**

El sistema ejecutó comandos porque el formulario envía datos directamente al intérprete del sistema operativo sin validación. En un entorno productivo, esta falla permitiría a un atacante comprometer el servidor completo, robar información o instalar malware.  
La solución radica en **validar y sanear entradas, restringir privilegios y aplicar controles de seguridad adicionales**, asegurando que el software siga el principio de **seguridad por diseño**.