[2025-11-21 XX:XX] - Explotación de OS Command Injection (Medium)

URL:
http://192.168.56.1/vulnerabilities/exec/

Payload utilizado:
127.0.0.1 | ls

Resultado:
El servidor ejecutó comandos del sistema operativo y mostró archivos internos de la aplicación (`help`, `index.php`, `source`). Esto confirma la presencia de OS Command Injection en nivel Medium.

Evidencias:
 Evidencia Command_exploit_01

- Petición Burp: `command_injection_request.txt`

Clasificación preliminar:

- OWASP: A03 – Injection
- CWE: CWE-78
- Severidad: CVSS 9.8 (Critical)

[2025-11-22 XX:XX] - File Upload Bypass (Medium)

URL:
http://192.168.56.1/vulnerabilities/upload/

Acción realizada:
Se creó un archivo PHP malicioso camuflado como PNG para evadir el filtro del módulo de carga.

Payload empleado:

- Archivo: `fake.png`
- Contenido: Código PHP incrustado dentro de un archivo con encabezado válido de PNG para bypass del filtro de DVWA Medium.

Proceso:

1. Se generó el archivo en Kali Linux con una cabecera PNG y contenido PHP.
2. DVWA Medium validó superficialmente el tipo de archivo y permitió la subida.
3. El archivo se almacenó correctamente en el directorio: `/hackable/uploads/`.
4. Al acceder a la URL del archivo, el navegador reportó que la imagen contiene errores, confirmando que se subió un archivo manipulado.

Evidencia — Archivo subido en `/hackable/uploads/`

 Evidencia File Upload

📸 Evidencia 2 — Intento de ejecución (error de imagen)

Al acceder al archivo subido mediante la URL:

`http://192.168.56.1/hackable/uploads/fake.png?cmd=ls`

el navegador muestra un error indicando que la imagen no puede visualizarse.
Esto confirma que el archivo **sí fue almacenado**, pero **no ejecuta código PHP en nivel Medium**, lo cual es el comportamiento esperado según la configuración de DVWA.

Impacto preliminar:

- Validación insuficiente de archivos.
- Se permite subir archivos manipulados.
- Riesgo de escalamiento si se combina con otras vulnerabilidades (File Inclusion, XSS, etc.).

Clasificación:

- **OWASP:** A08 — Software and Data Integrity Failures
- **CWE:** CWE-434 — Unrestricted File Upload
- **Severidad:** CVSS 7.5 (High)