

M2-A3: Fingerprinting de tecnologías web

Objetivo: identificar tecnologías de una aplicación web y comprobar si están afectadas por vulnerabilidades públicas.

1. Ejecuta WhatWeb contra un dominio de prueba (ej. `testphp.vulnweb.com`):

```
whatweb -a 3 -v http://testphp.vulnweb.com
```

2. Usa Wappalyzer en el navegador para validar los resultados.
3. Con Nmap, extrae cabeceras HTTP:

```
nmap -p80 --script http-headers testphp.vulnweb.com
```

4. Toma una tecnología detectada (ej. Apache 2.4.29, PHP 7.2.24, WordPress 5.4) y búscala en:
 - CVE Details
 - Exploit-DB

Entregar:

- Lista de tecnologías detectadas con versiones.
- Para al menos una tecnología, referencia de un CVE real (ID, año, impacto).
- Conclusión: ¿qué riesgo supondría para la empresa dejar esa versión en producción?