M7 – P3: Redacción de un informe a partir de un caso simulado

Objetivos

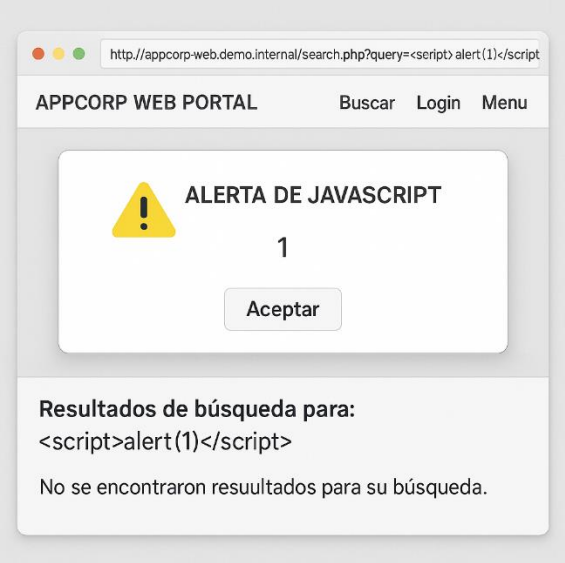
- Elaborar un informe profesional a partir de notas y outputs brutos.
- Redactar tanto la parte ejecutiva como la técnica de forma completa.

Desarrollo paso a paso

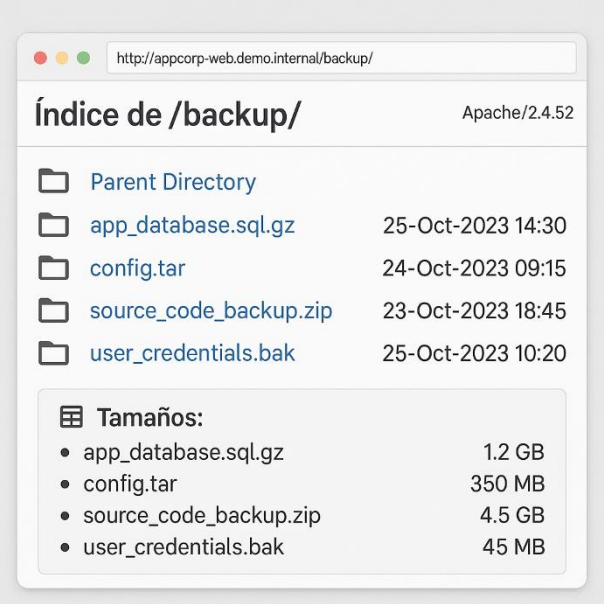
1. **Presentación del caso** "paquete de evidencias":
    - XML de Nmap (hosts con servicios). `nmap_scan_results.txt`

```
# Escaneo Nmap 7.93 ejecutado el Wed Oct 25 14:16:50 2023
# Objetivo: 192.168.1.50 (appcorp-web.demo.internal)

Nmap scan report for appcorp-web.demo.internal (192.168.1.50)
Host is up (0.045s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.52 ((Ubuntu))
3306/tcp open  mysql   MySQL 8.0.31
Device type: general purpose
Running: Linux 5.4-5.10
OS CPE: cpe:/o:linux:linux_kernel:5.4
OS details: Linux 5.4 - 5.10

Service detection performed. Please report any incorrect results.
```

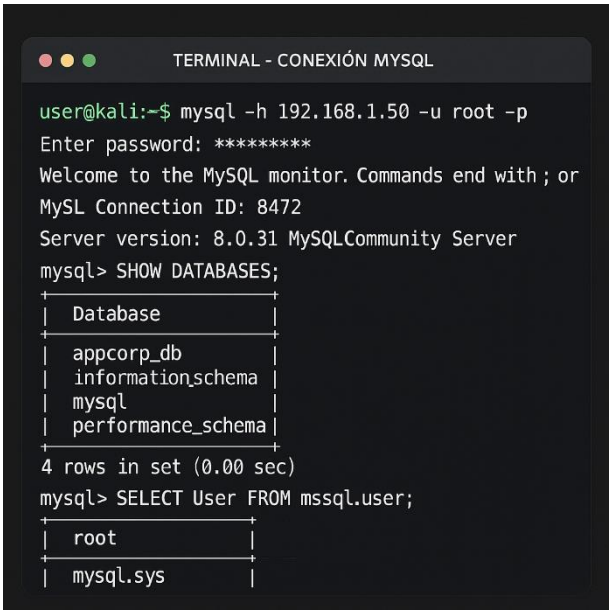
    - Capturas de un XSS (`alert(1)` en búsqueda).



- Captura de directorio `/backup/` accesible.



- Credenciales débiles para MySQL (solo en entorno controlado).



2. **Redacción del Resumen Ejecutivo**
   - Objetivo: en 1 página, explicar los **3 riesgos clave** en lenguaje sencillo.
   - Ejemplo: *"Un atacante podría acceder a copias de seguridad expuestas en el servidor web, lo que pondría en riesgo información sensible de clientes."*

3. **Redacción técnica de hallazgos**

   Cada alumno desarrolla 3 hallazgos con la plantilla:
   - **Título**
   - **Descripción** (qué es, dónde se encontró).
   - **Impacto** (qué podría pasar si se explota).
   - **Evidencia** (captura limpia).
   - **Severidad CVSS** (usar calculadora online).
   - **Recomendación** (acción concreta: "aplicar validación en servidor" mejor que "arreglar XSS").

4. **Conclusiones y Anexos (5 min)**
   - Conclusión: postura de seguridad global y próximos pasos (retest, parches, capacitación).
   - Anexar outputs de Nmap, capturas y criterios de severidad.

Entregable

- Informe final (5–8 páginas) con:
  - Resumen ejecutivo.
  - 3 hallazgos técnicos.
  - Conclusión y anexos.