🛠️ Ejercicio Práctico

📌 **Título:** Redacción de Informe Técnico Completo sobre una Vulnerabilidad Confirmada

---

🎯 Objetivo del ejercicio:

Simular una situación real de pentesting donde, tras identificar y validar una vulnerabilidad, debes **documentarla como un hallazgo profesional**, incluyendo todos los elementos clave: evidencia, riesgo, impacto, y recomendación técnica.

📝 Escenario:

Durante una prueba de seguridad en un entorno controlado, identificaste una vulnerabilidad de tipo **Cross-Site Scripting (XSS)** en un campo de comentarios de una aplicación web. Tu tarea es redactar un informe técnico estructurado que pueda ser presentado tanto al equipo de desarrollo como a la gerencia.

🔍 Tu tarea:

✅ Paso 1 – Identificación del hallazgo

1. Describe el tipo de vulnerabilidad encontrada
2. Ubicación exacta del fallo dentro de la aplicación
3. Indica cómo se detectó (herramienta o análisis manual)

✅ Paso 2 – Evidencia técnica

1. Muestra el payload utilizado (por ejemplo: `<script>alert("XSS")</script>`)

2. Explica el comportamiento del sistema al ejecutar el código
3. Describe cómo este fallo puede ser reproducido paso a paso

---

✅ Paso 3 – Análisis de impacto y riesgo

1. Evalúa la severidad del hallazgo (puedes usar una escala como **CVSS** estimada)
2. Menciona qué activos están en riesgo (usuarios, sesión, cookies, datos sensibles)
3. Clasifica el riesgo como Bajo, Medio o Alto

✅ Paso 4 – Recomendación técnica

1. Indica al menos **dos acciones concretas** que permitan mitigar el fallo
2. Si corresponde, incluye prácticas seguras de desarrollo (por ejemplo: sanitización de entradas, uso de CSP)

✅ Paso 5 – Presentación del hallazgo en formato profesional

Utiliza el siguiente formato para entregar tu informe:

1. Título del Hallazgo
2. Descripción
3. Evidencia Técnica
4. Evaluación de Impacto y Riesgo
5. Recomendaciones Técnicas
6. Referencias (si corresponde)

🧪 Resultado esperado:

- Documento completo, técnico, comprensible y accionable
- Evidencia bien explicada

- Riesgo argumentado con lógica
- Recomendaciones aplicables en contexto real

🧠 Reflexión Final:

¿Cómo se diferencia un informe profesional de una simple alerta técnica?
¿Qué aprendiste sobre la importancia del lenguaje y la estructura en un reporte de seguridad?
