🛠️ Ejercicio Práctico

📌 **Título:** Redacción inicial de un hallazgo de seguridad en formato estructurado

---

🎯 Objetivo del ejercicio:

El estudiante aplicará los **principios de claridad, precisión y estructura** para redactar un hallazgo de seguridad básico y organizarlo dentro de un informe técnico simulado.

🧱 Escenario:

Has realizado una auditoría web básica utilizando OWASP ZAP y encontraste una vulnerabilidad de tipo **XSS (Cross-Site Scripting)** en el campo de comentarios de un blog institucional. Tu misión es redactar este hallazgo utilizando un esquema profesional de documentación, siguiendo los principios vistos en la lección.

📋 Actividad:

A partir del siguiente hallazgo detectado, completa las secciones requeridas de un informe técnico:

Hallazgo técnico:
Al ingresar el código `<script>alert("XSS")</script>` en el campo de comentarios, el navegador ejecuta el script sin filtrar. El contenido queda almacenado y se muestra a otros usuarios.

📌 Formato sugerido de respuesta:

1. **Título del hallazgo**

2. **Resumen técnico breve** (1 a 2 líneas)

3. **Impacto potencial** (explica qué podría ocurrir si no se corrige)
4. **Evidencia técnica** (describir herramienta y prueba realizada)
5. **Recomendación de mitigación** (una acción concreta que elimine el riesgo)

✍️ Ejemplo de estructura a completar:

Sección	Contenido (completar)
Título del hallazgo	
Resumen técnico	
Impacto potencial	
Evidencia técnica	
Recomendación de mitigación	

🧠 Instrucciones:

- Utiliza un lenguaje **claro y directo**, evitando adornos o explicaciones vagas.
- Aplica el formato y estilo recomendado en la lección.
- No es necesario justificar metodologías complejas; enfócate en la forma más profesional de comunicar lo esencial.

✅ Ejemplo de Solución – Redacción de Hallazgo Técnico

Sección	Contenido
Título del hallazgo	Vulnerabilidad XSS almacenado en campo de comentarios del blog
Resumen técnico	Se identificó una ejecución no controlada de scripts en el campo de comentarios, permitiendo ataques XSS almacenados.

Impacto potencial	Un atacante podría inyectar scripts maliciosos que se ejecuten en los navegadores de otros usuarios, lo que permitiría robo de sesiones, redirecciones o ejecución de código arbitrario.
Evidencia técnica	Se utilizó OWASP ZAP para insertar el payload `<script>alert("XSS")</script>` en el formulario de comentarios. Tras enviar el formulario, el script se almacenó y fue ejecutado al visitar la publicación, confirmando la vulnerabilidad.
Recomendación de mitigación	Implementar sanitización y escape de entradas de usuario antes de renderizar contenido. Utilizar funciones como `htmlspecialchars()` en entornos PHP, y validar/filtrar entradas en el backend. Adicionalmente, aplicar políticas de seguridad de contenido (CSP).
