🛠️ Ejercicio Práctico

📌 **Título:** Documentar un Hallazgo de Seguridad a Nivel Inicial

---

🎯 Objetivo del ejercicio:

Aprender a estructurar y redactar la documentación básica de un hallazgo de seguridad encontrado durante una prueba de penetración, aplicando un formato profesional claro, comprensible y accionable.

📝 Escenario:

Durante una auditoría de seguridad en una aplicación web en entorno de laboratorio (como DVWA o WebGoat), identificaste una vulnerabilidad de tipo **SQL Injection** en un campo de búsqueda. Ahora, debes **documentar este hallazgo como si formaras parte del equipo de pentesting**.

🔍 Tu tarea:

✅ Paso 1 – Descripción del hallazgo

1. Redacta una descripción breve del hallazgo:
    - ¿Qué tipo de vulnerabilidad encontraste?
    - ¿Dónde se ubica en la aplicación?
    - ¿Qué comportamiento anómalo observaste?

✅ Paso 2 – Evidencia técnica

1. Especifica:
    - El parámetro o campo vulnerable
    - El payload utilizado (ej. `' OR '1'='1`)
    - El comportamiento de la aplicación ante ese payload
2. Agrega (si puedes) una **captura de pantalla simulada** o describe visualmente qué debería verse.

✅ Paso 3 – Evaluación del riesgo

1. Clasifica la vulnerabilidad usando términos simples:
    - Riesgo: Bajo / Medio / Alto
    - ¿Qué consecuencias puede tener si no se mitiga?

✅ Paso 4 – Recomendación

1. Proporciona una recomendación técnica para solucionar el problema:
    - ¿Qué cambios se deberían hacer en el código?
    - ¿Qué controles pueden evitar futuras apariciones?

✅ Paso 5 – Estructura final del informe

Entrega tu respuesta final con este formato:

1. Título del Hallazgo
2. Descripción
3. Evidencia Técnica
4. Evaluación del Riesgo
5. Recomendación Técnica

🧪 Resultado esperado:

- Un informe corto, claro y bien estructurado
- Redacción profesional adecuada al nivel técnico
- Identificación de riesgo y propuesta de solución realista

🧠 Reflexión Final:

¿Cómo ayuda una buena documentación al equipo de desarrollo?
¿Por qué es importante adaptar el lenguaje al público lector del informe?

🛠️ Solución – Ejercicio Práctico

📌 Documentar un Hallazgo de Seguridad a Nivel Inicial

---

1. Título del Hallazgo:

Inyección SQL en el campo de búsqueda de usuarios – Módulo "User Info"

---

2. Descripción:

Durante la evaluación de seguridad en el entorno de pruebas **DVWA (Damn Vulnerable Web Application)**, se detectó una vulnerabilidad de tipo **SQL Injection** en el parámetro `id` del módulo “SQL Injection”.
El sistema no valida correctamente las entradas del usuario, lo que permite modificar las consultas SQL enviadas al servidor.

---

3. Evidencia Técnica:

- **Campo vulnerable:** `id` (parámetro GET)

Payload utilizado:

1' OR '1'='1

-
- **Comportamiento observado:**
  Al enviar este valor, la aplicación retorna información de **todos los usuarios** en lugar de uno solo, evidenciando que la lógica de la consulta SQL fue alterada.

- **Descripción visual:**

  Después de enviar el payload, la aplicación mostró una tabla con múltiples registros de usuario, en lugar de mostrar los datos del ID específico solicitado.

---

4. Evaluación del Riesgo:

- **Nivel de riesgo: 🔴 Alto**
- **Impacto potencial:**
  - Exposición de información sensible
  - Posible extracción de datos de usuarios
  - Riesgo de escalación hacia compromisos más críticos (bases de datos completas)

---

5. Recomendación Técnica:

🔧 **Medidas de mitigación sugeridas:**

- Implementar **consultas SQL parametrizadas (prepared statements)** en el backend para evitar la manipulación de sentencias.
- Validar y sanitizar **todas las entradas del usuario** en formularios, URLs y cabeceras.
- Aplicar un **WAF (Web Application Firewall)** que detecte y bloquee patrones comunes de inyección.
- Realizar pruebas de seguridad periódicas con herramientas como Sqlmap, Burp Suite y análisis manual.

🧠 Reflexión Final (opcional para el estudiante):

Documentar correctamente este hallazgo permite al equipo de desarrollo entender **exactamente qué corregir**, sin necesidad de ser expertos en seguridad. Además, usar un lenguaje claro ayuda a comunicar el riesgo de forma efectiva a perfiles no técnicos, como gerentes o clientes.
