M7 – P1: Elaboración de informe técnico y ejecutivo

Elaborar un **informe demo** copiando los bloques que aparecen aquí, **pegándolos en tu editor** (*Word/LibreOffice/Google Docs/Markdown*).

El informe final contendrá: portada, control de versiones, alcance/limitaciones/cronograma/disclaimer, resumen ejecutivo**,** tabla de hallazgos**,** 1 hallazgo técnico completo**,** conclusiones y anexos con evidencias.

La estructura y el tono siguen OWASP WSTG que separa claramente resumen ejecutivo y hallazgos técnicos, incluye control de versiones y anexos con evidencias limpias.

Nota: NIST SP 800-115 subraya que el informe incluye análisis de hallazgos y mitigación y el manejo adecuado de evidencias; úsalo como referencia de buenas prácticas.

Estándares y referencias

- **OWASP WSTG – Reporting**: estructura del informe: portada, control de versiones, alcance/limitaciones, resumen ejecutivo, tabla de hallazgos, hallazgos técnicos, anexos y recomendación de proteger el informe.
- **PTES – Reporting**: define *Reporting* como la fase final del estándar de pentesting.
- **NIST SP 800-115**: guía técnica para planificar, ejecutar, analizar hallazgos, proponer mitigación y manejar evidencias.
- **FIRST / CVSS**: **CVSS v4.0** (especificación y calculadora oficial).

Nota: *CVSS es una **medida de severidad**, no un análisis de riesgo completo; el riesgo requiere contexto adicional (negocio, exposición real, controles, etc.). Esto lo subrayan tanto v3.1 como v4.0.*

Diferencias de enfoque: informe ejecutivo vs. técnico

- **Ejecutivo (dirección)**: breve, en lenguaje de negocio. Incluye objetivo, hallazgos clave a alto nivel, impacto de negocio, recomendaciones estratégicas y próximos pasos (retest). Esto está alineado con OWASP WSTG/Reporting.
- **Técnico (IT/Seguridad)**: detalles reproducibles: descripción, pasos, evidencia sanitizada, CVSS (v4.0 preferente), mitigación y referencias. OWASP recomienda incluir anexos con evidencias limpias.

Requisitos previos

1. Abre tu editor y crea un documento vacío llamado: **Informe_Pentest_Demo**.
2. Configura fuente legible (11–12 pt) y estilos de Título/Encabezado/Tabla.
3. Ten a mano la **calculadora CVSS v4.0**.

Paso 1 — Portada

Copia y pega:

```
Informe de Pruebas de Seguridad (Pentest)
Cliente: ComercioX
Proyecto: Evaluación Web + BD
Fecha: 27/09/2025
Equipo: Alumno Demo
```

Formato y presencia de portada/metadata conforme a OWASP WSTG/Reporting.

Paso 2 — Control de versiones

Inserta una tabla 4×2 y rellena así, ya que OWASP recomienda control de versiones en el informe:

Versión	Descripción	Fecha	Autor
1.0	Informe inicial	27/09/2025	Alumno Demo

https://owasp.org/www-project-web-security-testing-guide/latest/5-Reporting/01-Reporting_Structure

Paso 3 — Alcance, limitaciones, cronograma, disclaimer

Pega este bloque bajo el título "Alcance y condiciones" OWASP WSTG indica incluir alcance, limitaciones, cronograma y un **disclaimer point-in-time.** NIST 800-115 aconseja documentar supuestos y restricciones de las pruebas:

```
Alcance:
- Host 10.10.10.5 (servidor web de catálogo).
- Host 10.10.10.6 (servidor de base de datos).

Limitaciones:
- Sin pruebas de denegación de servicio (DoS).
- No se incluyeron pruebas autenticadas con rol administrador.

Cronograma:
- Trabajo de campo: 20–21/09/2025
- Análisis y consolidación: 22/09/2025

Disclaimer (point-in-time):
Este informe refleja el estado de seguridad en el momento de las pruebas; el
entorno puede haber cambiado desde entonces.
```

https://owasp.org/www-project-web-security-testing-guide/latest/5-Reporting/01-Reporting_Structure

Paso 4 — Metodología

Añade este breve párrafo para dejar trazabilidad y manejo de evidencias - WSTG y PTES para el marco y NIST 800-115 para informe y manejo de evidencias:

```
Metodología
Se siguió el OWASP Web Security Testing Guide y se referenció PTES (incluye una
fase de Reporting).
El informe, análisis y custodia de evidencias se alinearon con NIST SP 800-115.
```

PTES define 7 fases e incluye **Reporting** como la fase final.

https://owasp.org/www-project-web-security-testing-guide/v41/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

Paso 5 — Resumen ejecutivo – no técnico

Pega el siguiente bloque: lenguaje de negocio, sin jerga técnica, OWASP pide que el informe sea claro para directivos y técnicos:

```
Objetivo
Evaluar la seguridad de la aplicación web y la base de datos de ComercioX para
reducir riesgo de exposición de datos y fraude.

Hallazgos clave (alto nivel)
1) Entrada de búsqueda vulnerable a XSS → posible secuestro de sesión.
2) Cookie de sesión sin atributo HttpOnly → incrementa el impacto del XSS.
3) Configuración TLS del servidor mejorable → comunicaciones más expuestas.

Impacto de negocio
Posible afectación a confidencialidad de datos de clientes y reputación.

Recomendaciones estratégicas
- Validar/encodear las entradas y aplicar Content Security Policy (CSP).
- Establecer atributos de sesión seguros (HttpOnly y Secure).
- Revisar configuración TLS y realizar un retest tras aplicar correcciones.
```

Estructura coherente con WSTG: claridad para directivos

https://owasp.org/www-project-web-security-testing-guide/latest/5-Reporting/01-Reporting_Structure

Paso 6 — Tabla resumen de hallazgos

Inserta esta tabla, OWASP recomienda un **Findings Summary** antes del detalle:

ID	Título	Severidad (Base)	Activo	Estado
H-01	XSS reflejado en `/buscar`	(a calcular)	10.10.10.5	Nuevo

ID	Título	Severidad (Base)	Activo	Estado
H-02	Cookie de sesión sin `HttpOnly` (a estimar)		10.10.10.5	Nuevo

https://owasp.org/www-project-web-security-testing-guide/latest/5-Reporting/01-Reporting_Structure

Paso 7 — Hallazgo técnico H-01 (XSS reflejado)

Completarás un hallazgo **reproducible**, con evidencia **sanitizada**, **vector CVSS** y mitigación, estructura alineada con WSTG.

Copia y pega:

```
Título

XSS reflejado en /buscar

Descripción

El parámetro q en /buscar refleja la entrada del usuario sin codificación,
permitiendo la ejecución de JavaScript en el navegador (XSS reflejado).

Pasos de reproducción

1) Solicitud:
GET /buscar?q=%22%3E%3Cscript%3Ealert(1)%3C/script%3E HTTP/1.1
Host: 10.10.10.5

2) Respuesta (extracto del cuerpo):
<div>Resultados para: "><script>alert(1)</script></div>

Resultado esperado: el navegador ejecutaría el script (alerta).
```

Documentar paso a paso y con evidencia **sanitizada** es consistente con WSTG y NIST 800-115

```
Impacto

Un atacante podría ejecutar JavaScript en el navegador de la víctima para
secuestrar sesiones, manipular la interfaz o capturar credenciales.

Severidad (CVSS v4.0)
```

1. Abre la **calculadora oficial CVSS v4.0**. https://www.first.org/cvss/calculator/4-0
2. Asigna métricas **Base** típicas para un XSS reflejado **(ilustrativas; valida en tu entorno)**:
   - **AV:N**, **AC:L**, **AT:N**, **PR:N**, **UI:A**.
   - Impactos al **sistema vulnerable**: **VC:L**, **VI:L**, **VA:N**.
   - Impactos a **sistemas subsiguientes** (p. ej., navegador/usuario): **SC:L**, **SI:L**, **SA:N**.
     Esto generará un **vector v4.0** del tipo:

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N` *(ejemplo orientativo; obtén el **score Base** en la calculadora y documenta vector + puntuación). (Métricas y orden obligatorios en v4.0 según especificación oficial).*

3. Si tu cliente exige **v3.1**, usa la calculadora v3.1 y un vector típico para XSS reflejado (ajusta a contexto): `AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N`.

Importante: CVSS expresa **severidad** (Base/Threat/Environmental/Supplemental en v4.0) **no** es un análisis de **riesgo** completo, eso requiere contexto adicional. Para priorizar, en v4.0 etiqueta si publicas **CVSS-B**, **CVSS-BT**, **CVSS-BE** o **CVSS-BTE** según las métricas aplicadas.

https://www.first.org/cvss/v3-1/cvss-v31-user-guide_r1.pdf

https://owasp.org/www-project-web-security-testing-guide/latest/5-Reporting/01-Reporting_Structure

Inserta la evidencia **sanitizada** , sin PII (Personally Identifiable Information) ni cookies reales. Copia este bloque en tu Anexo C y referencia aquí “ver Anexo C, Fig. 1”:

```
Evidencia

Fig. 1 — Evidencia XSS (extracto de respuesta):
<div>Resultados para: "><script>alert(1)</script></div>
(Nota: sin datos de usuario; solo prueba mínima alert(1))
```

NIST 800-115 enfatiza manejo adecuado de evidencias; WSTG sugiere anexarlas sanitizadas

Copia y pega:

```
Mitigación

- Validar y codificar la entrada en servidor (HTML/atributos/JS).
- Implementar una Content Security Policy restrictiva.
- Añadir a cookies de sesión: HttpOnly y Secure.
- Pruebas de regresión y retest tras aplicar correcciones.
```

Buenas prácticas coherentes con WSTG/Reporting

Copia y pega:

```
Referencias

- OWASP WSTG – Sección de Reporting y formato de hallazgos.
- FIRST/CVSS v3.1 – Especificación y calculadora oficial.
- FIRST / CVSS v4.0 – Especificación y calculadora.
- NIST SP 800-115 – análisis/mitigación y evidencias.
```

https://owasp.org/www-project-web-security-testing-guide/latest/5-Reporting/01-Reporting_Structure

Paso 8 — Hallazgo técnico H-02 (cookie sin HttpOnly)

Título

```
Cookie de sesión sin HttpOnly
```

Descripción

```
La cookie de sesión no incluye el atributo HttpOnly, lo que permite que sea
accesible desde JavaScript, incrementando el impacto de XSS y el riesgo de robo de
sesión.
```

Evidencia (cabeceras HTTP sanitizadas)

Copia esto en **Anexo B** y referencia "ver Anexo B, Listado 1":

```
HTTP/1.1 200 OK
Set-Cookie: sessionid=abc123; Path=/; Secure
Content-Type: text/html; charset=UTF-8
Observación: Falta el atributo HttpOnly en la cookie de sesión.
```

Severidad (breve, orientativa)

- Como **endurecimiento de sesión** que **eleva** el impacto de XSS, puedes puntuarlo en v4.0 considerando que por sí solo no siempre afecta C/I/A; **evalúa en tu contexto** (exposición, rol, controles). Usa la calculadora v4.0 y documenta vector + score.
- Si usas v3.1, deja claro que es una **condición que agrava** otras vulnerabilidades (no necesariamente un impacto directo sin vector explotable).

https://www.first.org/cvss/v3-1/cvss-v31-user-guide_r1.pdf

Mitigación

```
Configurar la cookie de sesión con HttpOnly y Secure; revisar SameSite según caso.
```

Estructura de mitigación según WSTG/Reporting.

Paso 9 — Conclusiones

Copia y pega:

Conclusiones

```
La evaluación identificó una vulnerabilidad XSS y configuraciones de sesión
mejorables que afectan a la seguridad de las sesiones y potencialmente a datos de
clientes. Se recomienda priorizar la corrección del XSS y reforzar los atributos de
sesión (HttpOnly, Secure). Tras los cambios, realizar un retest y evaluar mejoras
en la configuración TLS.
```

En línea con WSTG: cerrar con próximas acciones y retest.

Paso 10 — Anexos con evidencias

OWASP sugiere incluir **evidencias sanitizadas** y criterios de severidad en anexos, evitando volcados completos. Crea los siguientes anexos y **pega tal cual**:

https://owasp.org/www-project-web-security-testing-guide/latest/5-Reporting/01-Reporting_Structure

Anexo A — Extracto Nmap (sanitizado)

```
# nmap -sV -oX nmap_scan.xml 10.10.10.5 10.10.10.6

<host>
  <address addr="10.10.10.5" addrtype="ipv4"/>
  <ports>
    <port protocol="tcp" portid="80">
      <state state="open"/>
      <service name="http" product="nginx" version="1.20.0"/>
    </port>
    <port protocol="tcp" portid="443">
      <state state="open"/>
      <service name="https" product="nginx" version="1.20.0" tunnel="ssl"/>
    </port>
  </ports>
</host>
<host>
  <address addr="10.10.10.6" addrtype="ipv4"/>
  <ports>
    <port protocol="tcp" portid="3306">
      <state state="open"/>
      <service name="mysql" product="MySQL" version="5.7.33"/>
    </port>
  </ports>
</host>
```

Anexo B — Cabeceras HTTP (cookie sin HttpOnly)

```
HTTP/1.1 200 OK
Set-Cookie: sessionid=abc123; Path=/; Secure
Content-Type: text/html; charset=UTF-8
```

Anexo C — Evidencia XSS (extracto HTML)

```
<div>Resultados para: "><script>alert(1)</script></div>
```

Anexo D — Criterios de severidad (CVSS)

```
La severidad se determina con base en CVSS v4.0 (Common Vulnerability Scoring
System, versión 4.0).

El vector y la puntuación Base deben documentarse en cada hallazgo utilizando la
calculadora oficial de FIRST: https://www.first.org/cvss/calculator/4.0
```

```
Recordatorio: el score Base representa únicamente la severidad intrínseca de la
vulnerabilidad; no sustituye un análisis de riesgo completo, que requiere
considerar factores de contexto, exposición y controles existentes.

De acuerdo con FIRST CVSS v4.0 User Guide, CVSS mide la severidad técnica, mientras
que el riesgo real depende del entorno organizacional y operativo.

Referencia oficial:
FIRST, CVSS v4.0 Specification Document(2023).
https://www.first.org/cvss/v4.0/specification-document
FIRST, CVSS v4.0 Calculator (2023). https://www.first.org/cvss/calculator/4.0
```

Paso 11 — Checklist final

Marca estos puntos alineados con WSTG Reporting:

https://owasp.org/www-project-web-security-testing-guide/latest/5-Reporting/01-Reporting_Structure

- ✓ Portada y control de versiones.
- ✓ Alcance/limitaciones/cronograma + disclaimer.
- ✓ Resumen ejecutivo claro para dirección.
- ✓ Tabla de hallazgos.
- ✓ Hallazgo técnico con reproducción, evidencia limpia, CVSS v4.0 (vector + score), mitigación.
- ✓ Conclusiones.
- ✓ Anexos con evidencias sanitizadas y criterios CVSS.

Paso 12 — Proteger el informe

Antes de compartir, **protege/cifra** el documento/PDF, WSTG recomienda asegurar el informe.

https://owasp.org/www-project-web-security-testing-guide/latest/5-Reporting/01-Reporting_Structure

Fuentes para consulta y justificación de la práctica

- **OWASP WSTG – Reporting**: estructura, público mixto, resumen ejecutivo, hallazgos, anexos y recomendaciones de asegurar el informe. https://owasp.org/www-project-web-security-testing-guide/latest/5-Reporting/01-Reporting_Structure
- **PTES – Reporting**: fase final del estándar, también referenciado desde OWASP. https://www.pentest-standard.org/index.php/Reporting
- **NIST SP 800-115**: guía técnica, planificación, ejecución, análisis de hallazgos/mitigación e informe. https://csrc.nist.gov/pubs/sp/800/115/final
- **FIRST / CVSS v4.0**: especificación y calculadora oficial, "CVSS mide severidad, no riesgo". https://www.first.org/cvss/v4.0/specification-document