



Redacción de Reportes de vulnerabilidades



\$WhoAmI

- ➔ **Security Consultant | Penetration Tester**
- ➔ Application Security
- ➔ Auditor TI
- ➔ Speaker
- ➔ GWEB, CEH
- ➔ Podcaster “Hack, Talk and Drink” Coming Soon

 @arturo_io  arturo_sustaita  4sus_  @4sus_00

Antes de empezar...



Índice

- Entender la importancia de un buen reporte.
- Aprender a estructurar hallazgos claros y accionables.
- Consejos prácticos de redacción.
- Importancia de tomar notas
- Debrief

"Report writing is fun,"
said no one ever.





¿Por qué importa el reporte?

- Es el entregable principal
- Comunica hallazgos a diferentes audiencias (técnicos, gerencia, cumplimiento).
- Genera conversaciones incómodas.
- Puede evitar (o provocar) vulnerabilidades persistentes.

Un mal reporte...



- Genera dudas.
- Incumplimientos de auditorías.
- Mitigaciones incorrectas.



Defined Approach Requirements

11.4.2 Internal penetration testing is performed:

- Per the entity's defined methodology,
- At least once every 12 months
- After any significant infrastructure or application upgrade or change
- By a qualified internal resource or qualified external third-party
- Organizational independence of the tester exists (not required to be a QSA or ASV).

Defined Approach Testing Procedures

11.4.2.a Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed in accordance with all elements specified in this requirement.

11.4.2.b Interview personnel to verify that the internal penetration test was performed by a qualified internal resource or qualified external third-party and that organizational independence of the tester exists (not required to be a QSA or ASV).



(260) IV. Contratar a un tercero independiente, con personal que cuente con capacidad técnica comprobable mediante certificaciones especializadas de la industria en la materia, para la realización de pruebas de penetración en los diferentes sistemas y aplicativos de la Institución con la finalidad de detectar errores, vulnerabilidades, funcionalidad no autorizada o cualquier código que ponga o pueda poner en riesgo la información y patrimonio de los clientes y de la propia Institución. Tal revisión deberá incluir la verificación de la integridad de los componentes de hardware y software que permitan detectar alteraciones a estos. Dichas pruebas deberán considerar, al menos lo siguiente:

(260) a) Su alcance y metodología, debiendo ser validados por el oficial en jefe de seguridad de la información.

(260) b) Ser realizadas al menos dos al año sobre sistemas y aplicativos distintos, o bien, cuando lo ordene la Comisión habiendo detectado factores que puedan afectar los sistemas y aplicativos o la información recibida, generada, procesada, almacenada o transmitida en estos. En este último caso, la Comisión determinará el alcance de las pruebas, así como los plazos para realizarlas.

(260) Se podrán efectuar pruebas adicionales a juicio del director general, con opinión del oficial en jefe de seguridad de la información, cuando existan cambios significativos en los sistemas y aplicativos, o realizarlas sobre sistemas y aplicativos previamente revisados cuando existan vulnerabilidades críticas.

(260) El director general de la Institución deberá enviar a la Comisión, dentro de los 20 días hábiles de haber sido finalizadas las pruebas, un informe con las conclusiones de estas. En el envío que se realice, se deberá procurar el uso de mecanismos que impidan el acceso al contenido de este informe por personal no autorizado.

Construyendo el reporte...



Toma de notas





- Escribe para tu yo del futuro
- Genera evidencias (durante las pruebas)
- Capturas de pantalla, request, parametros.
- Detallado, especifico estructurado
- Ayuda para el retest



CherryTree

→ **Nombre Pentest**

- ◆ **Info**
- ◆ **Suspicious**
- ◆ **Findings**
 - Finding 1
 - Finding 2
- ◆ **Retest**



WOMCY
LATAM Women in Cybersecurity

Armando el reporte



Estructura

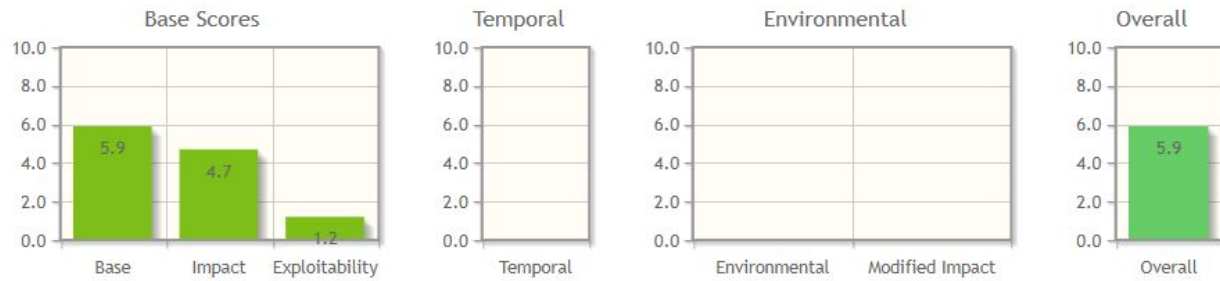
1. Portada y resumen ejecutivo
2. Alcance y metodología
3. Hallazgos priorizados
4. Evidencia + Recomendaciones

- TCM Report
- DSecure Report





Severidad



CVSS Base Score: 5.9
 Impact Subscore: 4.7
 Exploitability Subscore: 1.2
CVSS Temporal Score: NA
 CVSS Environmental Score: NA
 Modified Impact Subscore: NA
Overall CVSS Score: 5.9

Show Equations

CVSS v3.1 Vector
 AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:L

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) High (AC:H)

Privileges Required (PR)*

None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*

None (UI:N) Required (UI:R)

Scope (S)*

Unchanged (S:U) Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) High (C:H)

Integrity Impact (I)*

None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) High (A:H)

* All base metrics are required to generate a base score

Hallazgo

- Título descriptivo
- Descripción clara del problema
- Riesgo e impacto real
- Evidencia suficiente
- Recomendación/mitigación



Palabras

- ~~Muchos, pocos~~ -> 10 usuarios, usuarios con rol X.
- ~~Probablemente, podría, parece~~ -> De acuerdo con, Es evidente, se comprueba,



Incorrecto

Encontré una vulnerabilidad XSS y
mostré un alert() en la pantalla



Correcto



Se identificó la posibilidad de inyectar código Javascript a través del campo de búsqueda de productos, dicha vulnerabilidad es conocida como Cross Site Scripting (XSS) reflejado y permitiría a una atacante ejecutar código malicioso en el navegador del usuario permitiéndole realizar acciones tales como el robo de sesión.

Acción + vulnerabilidad + Riesgo



WOMCY
LATAM Women in Cybersecurity

Referencias

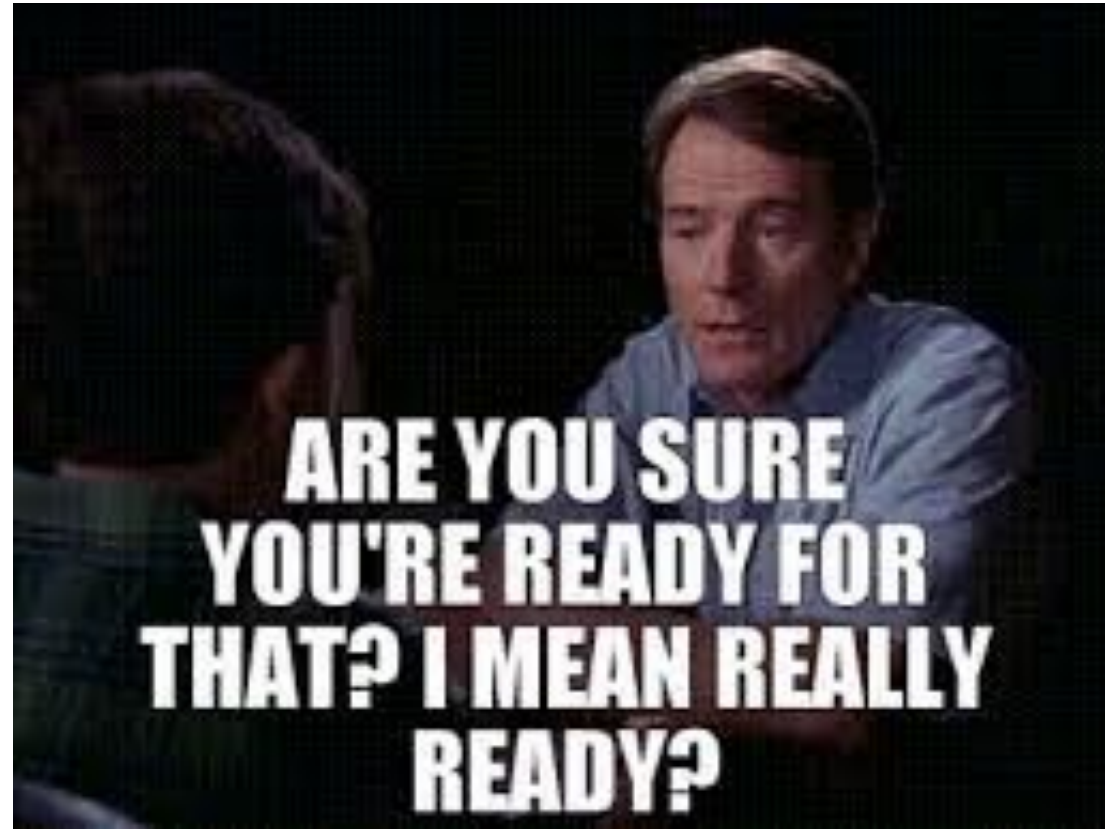
- [OWASP ASVS 5.0](#)
- [OWASP Top 10 2021](#)
- [OWASP Cheat Sheet](#)
- [OWASP Testing Guide 4.2](#)
- [CWE](#)
- [Portswigger Academy](#)



Debrief

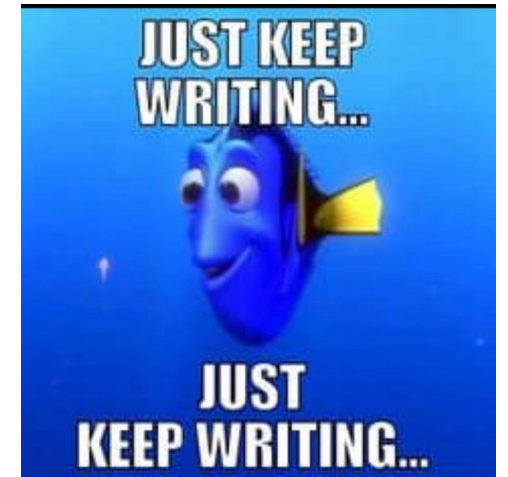
- Presentación informe técnico y ejecutivo.
- Enfoque en el impacto en lenguaje de negocio.
- Prepárate para defender tu criterio técnico.
- Mantén postura profesional.
- Aceptación del riesgo.






Consejos finales...

- ★ Buenas notas = Buenas evidencias = Buen reporte.
- ★ Escribe, escribe, escribe, corrige.
- ★ Riesgo presente.
- ★ Dudas? Vuelve a probar
- ★ Técnica del pato



Gracias

X @arturo_io

 arturo_sustaita

 4sus_

 @4sus_00



WOMCY
LATAM Women in Cybersecurity



WOMCY

LATAM Women in Cybersecurity

