
Día 1: Del hallazgo al reporte

Michel Faúndez

Fecha: 20.11.2025

Agenda



Sección 1

INTRODUCCIÓN Y CONTEXTO



Sección 2

MARCO LEGAL Y PREPARACIÓN (EL ESCUDO)



Sección 3

ESTRATEGIA Y METODOLOGÍA (EL MAPA)



Sección 4

EJECUCIÓN TÉCNICA (LA ACCIÓN)



Sección 5

EL REPORTE (EL PRODUCTO)



Sección 6

MÁS ALLÁ DEL REPORTE (SOFT SKILLS)



Sección 7

PRÁCTICA (MANOS A LA OBRA)



Sección 8

REFERENCIAS

SECCIÓN 1: INTRODUCCIÓN Y CONTEXTO


The background is a vibrant, abstract digital scene. It features a dark blue and black space filled with glowing, colorful light trails in shades of red, orange, yellow, and blue. These trails curve and flow across the frame, creating a sense of motion and depth. Scattered throughout the scene are numerous binary digits (0s and 1s) in various colors, some appearing to float or move along the light trails. The overall effect is a high-tech, futuristic aesthetic that suggests data, technology, and digital communication.

1 Introducción

A todos nos gusta encontrar información e informar , sin embargo siempre todo tiene reglas claras, y un contexto



SECCIÓN 2: MARCO LEGAL Y PREPARACIÓN (EL ESCUDO)

The background is a vibrant, abstract digital composition. It features a dark blue base with streaks of bright orange, red, and yellow light that create a sense of motion and depth. Scattered throughout are binary digits (0s and 1s) in various colors, some appearing to float or move. The overall aesthetic is high-tech and futuristic, typical of digital or cyber-themed presentations.



Normativas y Compliance (El "Por qué")

- El pentesting ayuda a cumplir con normativas internacionales exigidas en Chile.
Destacamos
- **ISO 27001:2013:** El control A.12.6.1 exige la gestión de vulnerabilidades técnicas.
En la actualidad Evidenciamos este control como anexo en el punto 8.8 de la ISO 27002:2022
- **NIST CSF 2.0:** Identificar y Proteger son funciones core que requieren evaluación continua.
- **PCI DSS:** Obligatorio para procesar tarjetas. Exige pentests anuales y tras cambios significativos.



Marco Legal Chileno (Lo crítico)

- **Ley N° 21.459 (Delitos):** Sanciona el acceso ilícito (Art. 2), interceptación y daño a datos. Es la base penal.
- **Ley N° 21.663 (Marco):** Establece obligaciones de reporte para servicios esenciales.

Otros:

La Ley de Fraude y Abuso Informático
(CFAA, por sus siglas en inglés) (EEUU)

- The Computer Misuse Act 1990
(CMA) (Reino Unido)

Documentación Previa 1 (Contratos)



Acuerdo de Confidencialidad (NDA)

Definición de Información confidencial: ¿ Qué datos están protegidos ?

Plazos de vigencia: Duración de la obligación de secreto.

Exclusiones: Información que no está protegida.

Jurisdicción: Ley que rige el acuerdo.



Master Service Agreement (MSA)

Alcance del trabajo: Qué se va a hacer (y qué no).

Límites de responsabilidad: Hasta dónde te cubres.

Seguros profesionales: Requisitos de cobertura.

Documentación Previa 2: Tu "Salvoconducto"



- Jamás inicies pruebas sin la documentación firmada. Esto distingue al pentester del cibercriminal.
- **NDA (Acuerdo de Confidencialidad):** Protege la información sensible del cliente.
- **Acuerdo de Servicios (MSA):** Define términos comerciales y legales.
- **Autorización de Pruebas** Documento técnico explícito que autoriza el ataque a IPs/Dominios específicos durante una ventana de tiempo definida.

Scoping: Definiendo los Límites



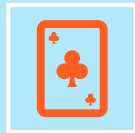
Un alcance mal definido puede resultar en problemas legales o pérdida de dinero.



¿Qué SÍ se toca?: IPs, URLs, aplicaciones móviles específicas.



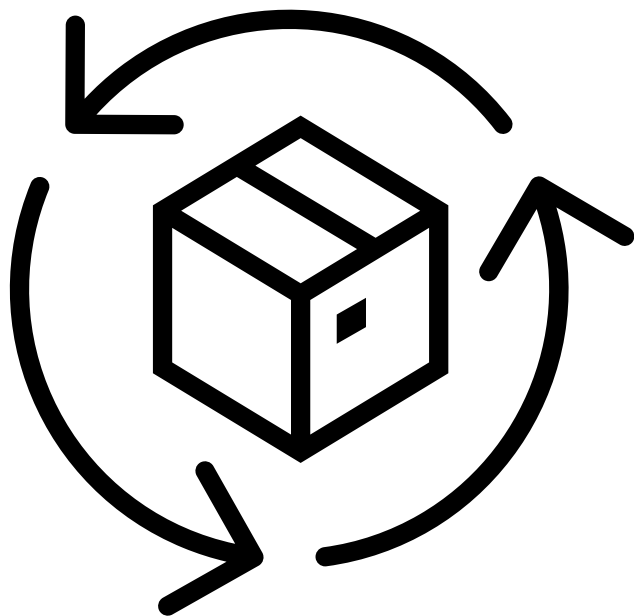
¿Qué NO se toca?: Servidores de terceros, infraestructura crítica en producción, bases de datos legadas frágiles.



Reglas de Juego (ROE): ¿Se permite Ingeniería Social? ¿DoS? ¿Horarios de prueba?

SECCIÓN 3: ESTRATEGIA Y METODOLOGÍA (EL MAPA)

The background is a vibrant, abstract digital scene. It features a dark blue and black space filled with glowing, colorful light trails in shades of red, orange, yellow, and blue. These trails curve and flow across the frame, creating a sense of motion and depth. Scattered throughout the scene are numerous binary digits (0s and 1s) in various colors, some appearing to float or move. The overall aesthetic is futuristic and high-tech, typical of digital or data-themed presentations.



Ciclo de vida (fase) Pentesting

- **Planificación:** Definición del alcance y reglas de juego (ROE).
- **Descubrimiento:** Recolección de información y escaneo.
- **Ataque/Explotación:** Confirmación de vulnerabilidades.
- **Reporte:** El producto final que recibe el cliente.



Tipos de Pruebas

- **Black Box (Caja Negra):** Simula un atacante externo real. Sin información previa. Mayor esfuerzo de reconocimiento.
- **Grey Box (Caja Gris):** Acceso parcial (ej. credenciales de usuario). Balance ideal costo-beneficio.
- **White Box (Caja Blanca):** Acceso total (código fuente, diagramas). Auditoría exhaustiva.

Metodologías

PTES

Penetration Testing Execution Standard. Cubre desde la pre-interacción hasta el reporte.

OWASP WSTG

Guía paso a paso para probar vulnerabilidades web*.

OSSTMM

Manual de Metodología Abierta de Testeo de Seguridad. Enfoque científico y métrico.

Metodologías *

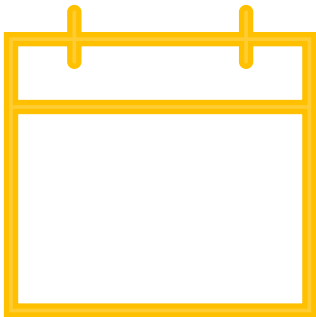
ISSAF

Information
System Security
Assessment
Framework

NIST

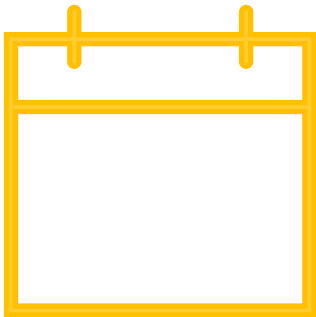
Publicación
especial 800-115
del NIST

Tiempos Referenciales**




METODOLOGÍA	FASES CLAVE	DURACIÓN TÍPICA	ENTREGABLES
OWASP Testing Guide	<ol style="list-style-type: none">1. Configuración/Despliegue2. Gestión de Sesión/Autenticación3. Pruebas de inyección4. Lógica de Negocio	2-4 semanas	Informe de Vulnerabilidades Web (incluyendo OWASP Top 10), Calificación de Riesgo por Vulnerabilidad, Recomendaciones de Remediación Específicas del código.
PTES	<ol style="list-style-type: none">1. Interacción Previa (Definición de Alcance)2. Recolección de Inteligencia (Footprinting)3. Modelado de Amenazas4. Análisis de Vulnerabilidades5. Explotación6. Post-Explotación (Elevación de Privilegios/Persistencia)7. Reporte	3-6 semanas	Informe Final con Resumen Ejecutivo, Listado de Vulnerabilidades con Pruebas de Concepto (PoC), Calificación de Riesgo (CVSS/Similar), Plan de Remediación Detallado.
OSSTM	<ol style="list-style-type: none">1. Pre-análisis (Definición de Alcance y Reglas)2. Testing de los 5 Canales (Data, Human, Physical, Wireless, Telecom)3. Análisis de Resultados (Cálculo de RAVs)4. Elaboración del Reporte	Depende de la cantidad de "Canales" a evaluar. 2-8 semanas (base 1 semana)	Certificado de Seguridad (con puntaje RAV o Risk Assessment Values), Informe Detallado de las Capacidades de Defensa, Métricas Cuantificables de riesgo por canal. Puede ser adaptable dependiendo del Canal.

Tiempos Referenciales**



METODOLOGÍA	FASES CLAVE	DURACIÓN TÍPICA	ENTREGABLES
ISSAF	1. Planificación y Preparación (Alcance, Reglas) 2. Evaluación (Recolección de Información, Mapeo, Identificación de Vulnerabilidades, Penetración, Escalada de Privilegios, Mantenimiento de Acceso). 3. Reporte, Limpieza y Destrucción de Artefactos (Cubrir Huellas).	4-8 semanas (Debido a su profundidad y detalle).	Resumen Ejecutivo para la Gestión, Informe Técnico Detallado (incluyendo herramientas y <i>exploits</i> usados), Lista de Vulnerabilidades Priorizadas con Recomendaciones de Mitigación
NIST SP 800-115	1 . Planificación 2. Ejecución (Descubrimiento, Análisis de Vulnerabilidades, Explotación) 3. Post-Ejecución (Reporte y Limpieza)	4 a 8 semanas	Plan de Pruebas de Seguridad Aprobado, Documentación de los hallazgos con base en los objetivos del negocio, Recomendaciones alineadas con políticas y estándares de seguridad.

SECCIÓN 4: Ejecución Técnica (La Acción)

The background is a vibrant, abstract digital scene. It features a dark blue and black space filled with glowing, colorful light trails in shades of red, orange, yellow, and blue. These trails curve and flow across the frame, creating a sense of dynamic movement. Scattered throughout the scene are numerous binary digits (0s and 1s) in various colors, some appearing to float or be part of the light trails. The overall effect is one of high-tech, digital energy and data flow.

El Toolbox del Pentester



Escáner de puertos



Escáner de vulnerabilidad



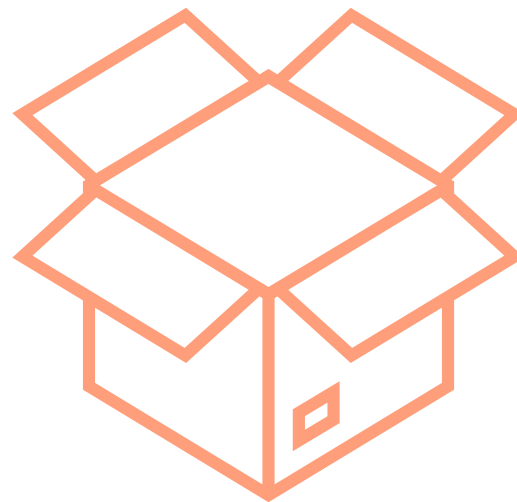
Proxy web



Recuperación avanzada de contraseña



Sniffer de red



"Las mejores herramientas a las que puede recurrir el líder para mejorar su desempeño son: el estudio, el pensamiento crítico, la reflexión, la acción compartida, el ejemplo".

SECCIÓN 5: EL REPORTE (EL PRODUCTO)

The background is a vibrant, abstract digital scene. It features a dark blue and black space filled with glowing orange, yellow, and red light trails that curve and sweep across the frame, suggesting high-speed data flow or network activity. Scattered throughout are numerous binary digits (0s and 1s) in various colors (white, blue, orange) and sizes, some appearing to float or move. The overall effect is one of dynamic, futuristic technology.

Estructura del Reporte Profesional



-
- El reporte tiene dos audiencias muy distintas. No las mezcles.
 - **Resumen Ejecutivo**
 - Dirigido a Gerentes/Directorio. Enfocado en riesgo de negocio, impacto financiero y reputacional. Sin jerga técnica.
 - **Informe Técnico**
 - Dirigido a TI/Desarrollo. Evidencia detallada, pasos de reproducción (PoC), CVSS y remediación técnica específica.

Resumen ejecutivo



Es la parte más leída del reporte.

Debe responder en tres frases:

- **Qué encontramos:** El problema crítico.
- **Qué riesgo representa:** El impacto en el negocio.
- **Qué hacer primero:** La acción inmediata.

Informe técnico

Estructura de una Vulnerabilidad (CVSS)

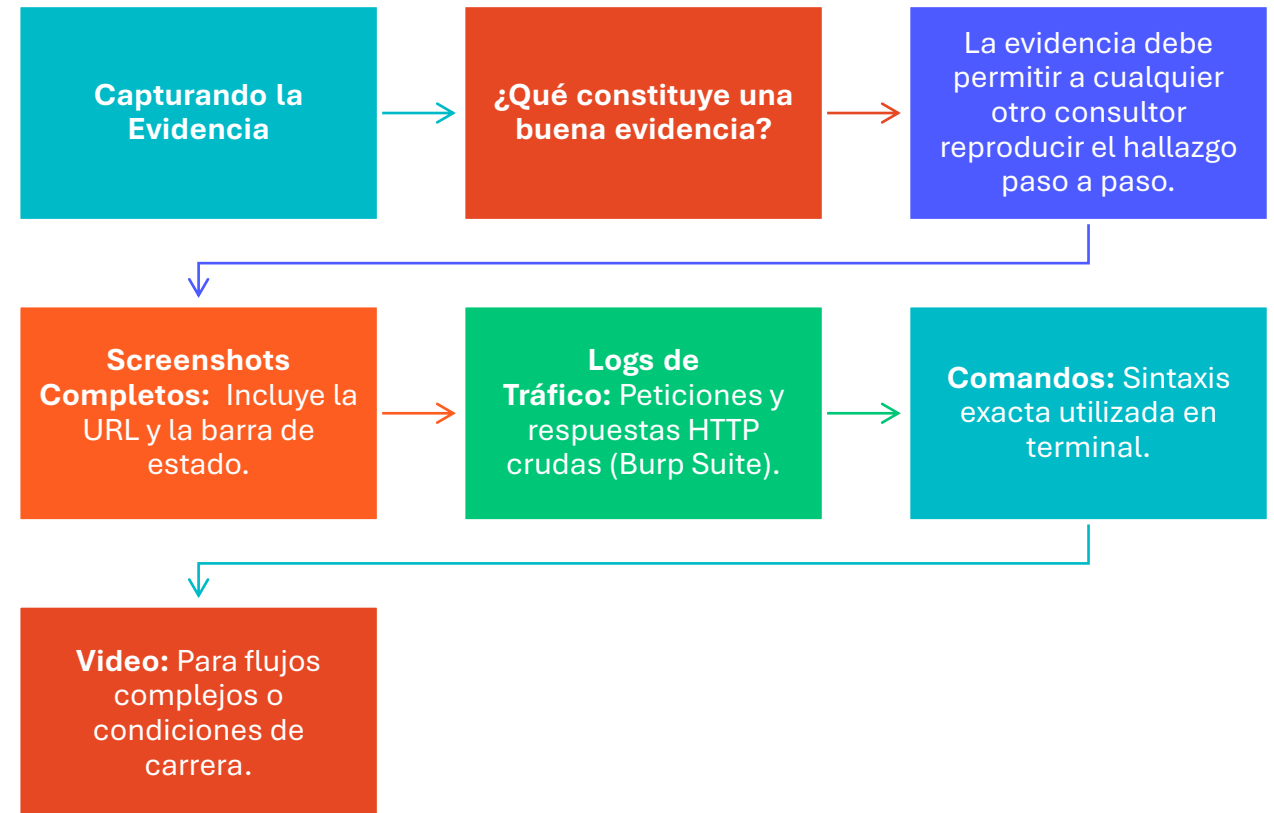
- 🔧 **Descripción:** Qué es el problema.
- 💣 **Impacto:** Qué tan malo es.
- 🔄 **Reproducibilidad:** Pasos para replicarlo.
- 🛡️ **Mitigación:** Cómo solucionarlo.

Evidencias

- 📷 **Capturas de pantalla:** Antes y después.
- 📄 **Logs y salidas de comandos:** Prueba técnica.
- >_ **Comandos ejecutados:** Para la reproducibilidad.



Del Hallazgo al Papel



SECCIÓN 6: MÁS ALLÁ DEL REPORTE (SOFT SKILLS)

The background is a vibrant, abstract digital scene. It features a dark blue base with streaks of bright yellow, orange, and red light that create a sense of motion and depth. Scattered throughout are glowing binary digits (0s and 1s) in various colors, some appearing to float or move. The overall effect is one of high-tech, data-driven energy.

Habilidades Blandas y Manejo de Cliente



- El Rol del Traductor:**

- Tu trabajo es traducir *Riesgo Técnico* (SQL Injection) a *Riesgo de Negocio* (Pérdida financiera/reputacional).

- Gerencia no habla TCP/IP; habla dinero y continuidad operativa.

- Gestión de la Negación ("Es un falso positivo"):**

- Es común que el cliente se ponga a la defensiva.

- Solución:** No entres en discusiones de ego. Responde con la **Prueba de Concepto (PoC)** en mano. Los datos matan el relato.

Habilidades Blandas y Manejo de Cliente

- **Manejo de Expectativas y Scope Creep:**
- Cliente: *"¿Ya que estás ahí, puedes revisar también este otro servidor?"*
- Pentester: *"Eso excede el alcance (Scope) firmado. Podemos revisarlo en una nueva iteración."* (Protege tu tiempo y el contrato).

Empatía con el Desarrollador:

- No eres un juez, eres un consultor.
- Evita el tono: "Mira lo mal que hiciste esto".
- Usa el tono: "Aquí hay una oportunidad de mejora para blindar el sistema".



Disclosure y Vulnerabilidades



¿Qué pasa cuando encuentras algo crítico? El manejo de la información es vital.



Coordinated Vulnerability Disclosure (CVD): Reportar al vendor/dueño y dar un tiempo razonable para el parche antes de publicar.



Ley Marco (21.663): Obliga a operadores de servicios esenciales a reportar incidentes significativos al CSIRT Nacional.



Uso de CVSS v4.0: Estándar objetivo para puntuar la severidad (Base, Amenaza, Ambiental).

Checklist

Final: Antes de Entregar



Scope firmado y adjunto



Reporte generado en un formato que pueda ser abordado (docx, pdf)



Resumen ejecutivo revisado



Recomendaciones Priorizadas
Evidencias (capturas, logs) guardadas



CVSS calculado para cada hallazgo



Gráficos de riesgo incluidos**



Compliance mapeado (ej. ISO 27001)



Cliente notificado y copia de seguridad en repositorio interno

SECCIÓN 7: PRÁCTICA (MANOS A LA OBRA)

The background is a vibrant, abstract digital composition. It features a dark blue base with streaks of bright yellow, orange, and red light that create a sense of motion and depth. Scattered throughout are glowing binary digits (0s and 1s) in various colors, including cyan, yellow, and red. The overall effect is one of high-tech energy and digital connectivity.



Ejercicio Práctico (Introducción)

Antes de llegar y ejecutar una vulnerabilidad, es importante conocer cada escenario y realidad

El Escenario

1



2



3



La Tarea

1

2

3

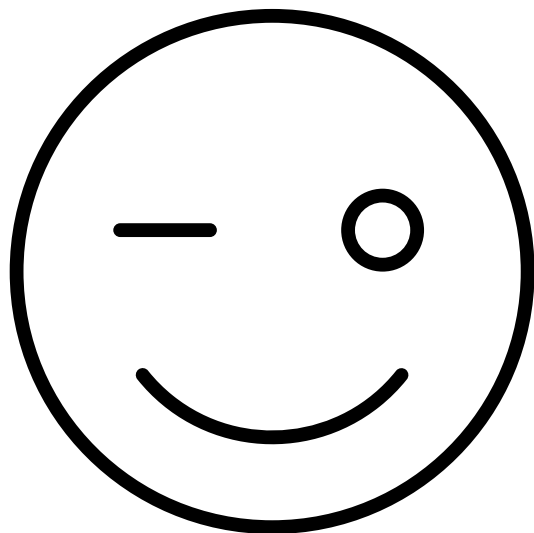
Encontraste una vulnerabilidad de SQL Injection en un formulario de login.

La URL afectada es `/login.php`. La payload `' OR '1'='1` te permite bypassar la autenticación.

Tienes una captura de pantalla mostrando acceso a datos de administrador.

- Actividad:
- 1. Calcula CVSS (Base score ?)
- 2. Redacta Impacto (1 párrafo)
- 3. Propone una Mitigación (Acción Inmediata)
- 4. ¿Que número(s) representa la vulnerabilidad presentada?

Conclusión



Más allá de la Vulnerabilidad

- **El Reporte es el Producto:** El cliente no paga por el exploit, paga por el entendimiento del riesgo y la solución. Si el hallazgo no se comunica bien, el trabajo técnico pierde su valor.
- **La Firma es la Frontera:** La diferencia entre un ciberdelincuente y un pentester profesional es la autorización escrita. Sin documentos firmados (NDA, MSA, Autorización), no hay ética ni legalidad.
- **Traductor de Riesgos:** Nuestro rol es traducir fallas técnicas complejas (como una inyección SQL) en impactos de negocio comprensibles para la gerencia, entender riesgos y vulnerabilidades, va de la mano a saber abordarlas de forma efectiva.
- **Metodología sobre Herramientas:** Las herramientas cambian, pero una metodología sólida (OWASP, PTES, NIST) garantiza consistencia y calidad profesional.

Palabras Finales

Gracias

Muchas gracias por su atención

SECCIÓN 8: Referencias

The background is a vibrant, abstract digital composition. It features a dark blue and black base, overlaid with numerous glowing, curved lines in shades of orange, red, and yellow. Scattered throughout the scene are various binary digits (0s and 1s) in white and light blue, some appearing to float or move. The overall effect is one of high-tech, data-driven energy.

Referencia

Contacto : Michel Faúndez

- Mi camino en ciberseguridad comenzó con una base en Matemática de la Universidad del Bío-Bío, la cual he complementado intensamente con especializaciones en seguridad. Cuento con un Diplomado en Red Team de Capacitación USACH y certificaciones como eJPT (Penetration Testing) de INE y CEHP de EC-Council. Además, he profundizado en Gestión de Incidentes como Implementador Líder ISO 27035, entre otras formaciones y enseñanzas.
- Actualmente, me desempeño como Consultor de Ethical Hacking y DevSecOps en PentestSPA, donde mi rol como Pentester me permite aplicar conocimientos tanto ofensivos como defensivos. Soy un colaborador activo en comunidades clave de ciberseguridad como Fundación Sochisi, Partyhack y Blueteam Latam, y he tenido la oportunidad de ser speaker en diversas instancias.
- Me considero un profesional autodidacta y proactivo, siempre buscando el crecimiento constante y el perfeccionamiento en ciberseguridad. Valoro mucho el trabajo en equipo y me gusta compartir mis conocimientos técnicos con respeto y empatía, tanto en entornos colaborativos como formativos.
- **Mi LinkedIn:** <https://www.linkedin.com/in/mfaundez/>

Bibliografía Metodologías y Frameworks

- [20] OWASP Foundation - "Penetration Testing Methodologies"
- URL: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies
- [21] Sapphire.net - "OWASP Methodology Security Testing Phases" (2024-05-20)
- URL: <https://www.sapphire.net/blogs-press-releases/owasp-methodology/>
- [23] GeeksforGeeks - "Penetration Testing Execution Standard (PTES)" (2019-10-24)
- URL: <https://www.geeksforgeeks.org/software-engineering/penetration-testing-execution-standard-ptes/>
- [24] LinkedIn - "Penetration Testing Methodologies: OWASP, OSSTMM, PTES" (2024-05-29)
- Author: Maxwell Ferreira
- URL: <https://www.linkedin.com/pulse/penetration-testing-methodologies-owasp-osstmm-ptes-maxwell-ferreira-norrc>
- [26] Datami - "Penetration Testing Execution Standard: 7 PTES Stages" (2025-06-02)
- URL: <https://datami.ee/blog/penetration-testing-execution-standard-7-ptes-stages/>
- [27] VikingCloud - "What is the Penetration Testing Execution Standard (PTES)?" (2025-09-01)
- URL: <https://www.vikingcloud.com/blog/what-is-penetration-testing-execution-standard>
- [28] OWASP Foundation - "Penetration Testing Methodologies v4.1" (2011-12-31)
- URL: https://owasp.org/www-project-web-security-testing-guide/v41/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies
- [30] PTES - "The Penetration Testing Execution Standard"
- URL: http://www.pentest-standard.org/index.php/Main_Page

Bibliografía Metodologías y Frameworks

-
- [31] OWASP - "OWASP Web Security Testing Guide"
 - URL: <https://owasp.org/www-project-web-security-testing-guide/>
 - [79] DataGuard - "An overview of penetration testing methodologies" (2024-10-14)
 - URL: <https://www.dataguard.com/blog/penetration-testing-methodologies/>
 - [80] Sprinto - "List of Penetration testing methodologies" (2025-01-09)
 - URL: <https://sprinto.com/blog/penetration-testing-methodologies/>
 - [85] IBM - "Top Penetration Testing Methodologies" (2024-01-23)
 - URL: <https://www.ibm.com/think/insights/pen-testing-methodology>
 - [93] Indusface - "Complete Guide to Penetration Testing Methodology" (2025-08-12)
 - URL: <https://www.indusface.com/blog/penetration-testing-methodologies/>
 - [99] Qualysec - "Top 10 Penetration Testing Methodologies (Expert Guide)" (2025-05-19)
 - URL: <https://qualysec.com/penetration-testing-methodologies/>
 - [102] Datami - "Pen Testing Methodology: Top 5 Methodologies" (2025-06-02)
 - URL: <https://datami.ee/blog/top-5-methodologies/>
 - [104] N-ix - "Top 4 penetration testing methodologies to use in 2025" (2025-04-24)
 - URL: <https://www.n-ix.com/penetration-testing-methodologies/>

Bibliografía

Estructura de Reportes

- [1] TCM Security - "What is a Penetration Testing Report?" (2024-10-24)
URL: <https://tcm-sec.com/what-is-a-penetration-testing-report/>
- [4] Offensive Security - "Penetration Test Report for Internal Lab and Exam" (PWK Example Report v1)
URL: <https://www.offsec.com/pwk-online/PWK-Example-Report-v1.pdf>
- [10] PurpleSec - "Sample Penetration Test Report - Example Institute"
URL: <https://purplesec.us/wp-content/uploads/2019/12/Sample-Penetration-Test-Report-PurpleSec.pdf>
- [19] HackTheBox - "Penetration testing reports: A powerful template and guide" (2025-08-19)
URL: <https://www.hackthebox.com/blog/penetration-testing-reports-template-and-guide>
- [83] Terra Security - "The Essential Penetration Test Report Template" (2025-05-26)
URL: <https://www.terra.security/blog/the-essential-penetration-test-report-template>
- [84] Scytale - "How to Create an Effective Plan for Penetration Testing Reports" (2025-06-24)
URL: <https://scytale.ai/resources/how-to-create-an-effective-plan-for-penetration-testing-reports/>
- [89] eSecurity Planet - "How to Write a Pentesting Report - With Checklist" (2023-11-28)
URL: <https://www.esecurityplanet.com/networks/pentest-report/>
- [92] PentestPad - "What to Include in a Professional Pentest Report" (2025-04-04)
URL: <https://www.pentestpad.com/blog/what-to-include-in-a-professional-pentest-report-a-complete-guide>
- [95] Microminder CS - "Penetration Testing Report: Key Elements and Best Practices" (2025-08-24)
URL: <https://www.micromindercs.com/blog/penetration-testing-report>

Bibliografía

Reportes en Español

- [39] RINKU - "Cómo hacer un informe de PENTESTING para el eCPPTv2"
- URL: <https://rinku.tech/informe-ecpptv2/>
- [42] RINKU - "Cómo hacer un informe de PENTESTING (PLANTILLA GRATIS)" (Video, 2024-04-10)
- URL: https://www.youtube.com/watch?v=vW3C_0BFtAU
- [45] RINKU - "Cómo hacer tu primer informe de PENTESTING" (2025-04-30)
- URL: <https://rinku.tech/mi-primer-informe-pentesting/>
- [48] 4Geeks - "Informe de Resultados de Pruebas de Penetración (con ejemplos)" (2025-04-24)
- URL: <https://4geeks.com/es/lesson/como-hacer-reporte-pruebas-de-penetracion-con-ejemplos-y-plantilla>
- [54] Hacker Mentor - "Modelo de Informe de Resultados Pentesting"
- URL: <https://www.hacker-mentor.com/modeloinformepentesting>
- [57] Hacknoid - "¿Cómo presentar un informe de Ethical Hacking?" (2023-02-26)
- URL: <https://www.hacknoid.com/hacknoid/presentar-informe-ethical-hacking-plantilla-descargable/>

Bibliografía

Marco Legal y Ético

-
- [152] PixelQA - "Ethical & Legal Considerations in Penetration Testing" (2025-03-23)
 - URL: <https://www.pixelqa.com/blog/post/ethical-legal-considerations-penetration-testing>
 - [155] Sentrion - "Legal requirements and compliance for penetration testing" (2025-07-06)
 - URL: <https://www.sentrion.co.uk/insights/what-are-the-legal-aspects-of-penetration-testing>
 - [158] PlusClouds - "Legal Aspects of Penetration Tests: Legal Processes and Permissions" (2023-07-24)
 - URL: <https://plusclouds.com/us/blogs/legal-aspects-of-penetration-tests-legal-processes-and-permissions-1>
 - [161] Roubin - "Legal and Ethical Considerations in Penetration Testing" (2025-09-01)
 - URL: <https://www.roubin.co.uk/blog/legal-and-ethical-considerations-in-penetration-testing>
 - [164] CarbonSec - "The Legal Aspects of Ethical Hacking"
 - URL: <https://www.carbonsec.com/legal-aspects-of-ethical-hacking/>
 - [167] Vertex Cybersecurity - "The Legal and Ethical Considerations of Penetration Testing" (2024-07-23)
 - URL: <https://www.vertexcybersecurity.com.au/the-legal-and-ethical-considerations-of-penetration-testing/>

Bibliografía NDAs y Contratos

- [151] Template.net - "Cybersecurity NDA (Non-Disclosure Agreement) Template" (2025-03-10)
- URL: <https://www.template.net/editable/148052/cybersecurity-nda-non-disclosure-agreement>
- [154] GoNitro - "NDA Template" (2016-03-09)
- URL: <https://www.gonitro.com/resources/nda-template>
- [157] Portant - "International NDA Template - Easy, Online & Free"
- URL: <https://www.portant.co/contract-templates/international-nda-template>
- [160] GenieAI - "Cyber Security Non Disclosure Agreement - India"
- URL: <https://www.genieai.co/en-in/template/cyber-security-non-disclosure-agreement>
- [163] eSign - "Free Cyber Security Non-Disclosure Agreement (NDA) | PDF" (2024-06-07)
- URL: <https://esign.com/nda/cyber-security/>
- [166] NDA Template - "Non-Disclosure Agreement (NDA) Template – Sample"
- URL: <https://nondisclosureagreement.com>
- [169] LegalZoom - "Non-Disclosure Agreement Templates" (2023-11-05)
- URL: <https://www.legalzoom.com/templates/agreements/non-disclosure-agreements>
- [170] Penetration Testing - "MSA - Master Service Agreement" (2025-05-08)
- URL: <https://www.penetration-testing.com/legal+-documents/msa>

Bibliografía Documentos de Alcance (Scope)

- [171] ClickUp - "Penetration Testing Scope of Work Template" (2025-03-19)
 - URL: <https://clickup.com/templates/scope-of-work/penetration-testing>
- [174] Saudi NCA - "Penetration Testing Standard Template"
 - URL: https://cdn.nca.gov.sa/api/files/public/upload/3a098671-bd77-4d76-a24d-7518ae9ac953_STANDARD_Penetration_Testing_Template_en-.pdf
- [177] Trio.so - "Free Penetration Testing Policy Template for Your Organization" (2024-10-08)
 - URL: <https://www.trio.so/blog/penetration-testing-policy-template/>
- [180] Timeless IMS - "Penetration Test Scoping Document"
 - URL: <https://www.timelessims.co.uk/wp-content/uploads/Timeless%20IMS%20Security%20Pen%20Testing%20and%20Scoping%20document%20v1.0.pdf>
- [183] PurpleSec - "Sample Penetration Testing Policy Template" (2025-07-23)
 - URL: <https://purplesec.us/resources/cyber-security-policy-templates/penetration-testing/>
- [186] SANS - "Pen Test Scope Worksheet" (2025-09-10)
 - URL: <https://www.sans.org/posters/pen-test-scope-worksheet>

Bibliografía

Vulnerability

Disclosure

- [172] OWASP - "Vulnerability Disclosure Cheat Sheet" (2019-12-31)
- URL: https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html
- [175] Fortinet - "Vulnerability Disclosure: Risks, Significance, and Best Practices"
- URL: <https://www.fortinet.com/resources/cyberglossary/vulnerability-disclosure>
- [178] Arçelik - "Vulnerability Disclosure Procedure"
- URL: <https://www.arcelikglobal.com/en/vulnerability-disclosure-procedure/>
- [181] CISA - "Coordinated Vulnerability Disclosure Program" (2025-04-30)
- URL: <https://www.cisa.gov/resources-tools/programs/coordinated-vulnerability-disclosure-program>
- [184] HHS - "Vulnerability Disclosure Policy" (2021-01-07)
- URL: <https://www.hhs.gov/vulnerability-disclosure-policy/index.html>
- [187] US Commerce - "Vulnerability Disclosure Policy" (2023-06-28)
- URL: <https://www.commerce.gov/vulnerability-disclosure-policy>
- [189] European Commission - "Vulnerability Disclosure Policy"
- URL: https://commission.europa.eu/legal-notice/vulnerability-disclosure-policy_en

Bibliografía Gestión de Incidentes

-
- [173] DataGuard - "Cyber Security Incident Response Plan" (2024-01-31)
- URL: <https://www.dataguard.com/cyber-security/incident-response-plan/>
- [176] Balbix - "The Comprehensive Cybersecurity Incident Response Guide" (2025-03-23)
- URL: <https://www.balbix.com/insights/cybersecurity-incident-response-a-comprehensive-guide-for-security-leaders/>
- [179] Microsoft - "Incident response overview" (2024-11-05)
- URL: <https://learn.microsoft.com/en-us/security/operations/incident-response-overview>
- [182] NIST - "Computer Security Incident Handling Guide" (SP 800-61r2)
- URL: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>
- [185] Australian Cyber Security Centre - "Cyber Incident Response Plan"
- URL: https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf
- [188] CREST - "Cyber Security Incident Response Guide"
- URL: <https://www.crest-approved.org/wp-content/uploads/2022/04/CSIR-Procurement-Guide-1.pdf>

Bibliografía Compliance NIST Cybersecurity Framework

- ##### [22] SBS CyberSecurity - "NIST CSF Risk Assessment Services" (2025-09-03)
- URL: <https://sbscyber.com/services/nist-cybersecurity-framework-assessment>
- [25] CyberSaint - "NIST Cybersecurity Assessment Tool" (2024-04-22)
- URL: <https://www.cybersaint.io/blog/nist-cybersecurity-framework-assessment-tool>
- [32] NIST - "The NIST Cybersecurity Framework (CSF) 2.0"
- URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- [35] NIST - "Assessment & Auditing Resources" (2025-04-01)
- URL: <https://www.nist.gov/cyberframework/assessment-auditing-resources>
- [156] Cymulate - "NIST Compliance Checklist & Guide" (2025-08-31)
- URL: <https://cymulate.com/blog/nist-compliance-checklist/>
- [162] LegitSecurity - "NIST Compliance Checklist: A Guide" (2025-02-05)
- URL: <https://www.legitsecurity.com/aspm-knowledge-base/nist-compliance-checklist-step-guide>
- [168] XM Cyber - "NIST Cybersecurity Framework (CSF) Checklist for 2024" (2025-06-17)
- URL: <https://xmcyber.com/the-nist-cybersecurity-framework-2-0-checklist/>

Bibliografía Compliance ISO 27001

-
- [60] Scrut.io - "Understanding ISO 27001 penetration testing: Scope, controls, and compliance" (2025-08-21)
 - URL: <https://www.scrut.io/hub/iso-27001/penetration-testing>
 - [63] BlazeInfosec - "ISO 27001 Penetration Testing - The Complete Guide" (2025-05-19)
 - URL: <https://www.blazeinfosec.com/post/iso-27001-penetration-testing/>
 - [66] Qualysec - "ISO 27001 Penetration Testing – A Comprehensive Guide" (2025-01-15)
 - URL: <https://qualysec.com/iso-27001-penetration-testing-a-comprehensive-guide-2023/>
 - [72] HackerOne - "ISO 27001 and Pentesting: What You Need to Know" (2024-04-30)
 - URL: <https://www.hackerone.com/blog/iso-27001-and-pentesting-what-you-need-know>

Bibliografía Frameworks Generales

- [153] Security Compass - "15 Essential Regulatory and Security Compliance Frameworks" (2025-06-22)
 - URL: <https://www.securitycompass.com/blog/regulatory-security-compliance-frameworks-standards/>
- [159] Cynomi - "8 Key Cybersecurity Compliance Standards and Frameworks" (2025-08-26)
 - URL: <https://cynomi.com/learn/cyber-security-compliance-standards-and-frameworks/>
- [165] FINRA - "Small Firm Cybersecurity Checklist" (2023-11-30)
 - URL: <https://www.finra.org/compliance-tools/cybersecurity-checklist>

Bibliografía

Categorías

testing

- [82] BlueVoyant - "Penetration Testing: Complete Guide to Process, Types, and Tools" (2025-01-21)
 - URL: <https://www.bluevoyant.com/knowledge-center/penetration-testing-complete-guide-to-process-types-and-tools>
- [96] Redscan - "Types of Penetration Testing: Black Box, White Box & Grey Box" (2024-01-23)
 - URL: <https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/>
- [97] Qualysec - "Types of Pen Testing in Cyber Security: A Comprehensive Guide" (2025-02-12)
 - URL: <https://qualysec.com/types-of-pen-testing/>
- [100] N-ix - "Types of penetration testing: A comprehensive guide" (2024-11-04)
 - URL: <https://www.n-ix.com/types-of-penetration-testing/>
- [101] Sprocket Security - "Top 8 Penetration Testing Types, Techniques, and Best Practices" (2024-11-20)
 - URL: <https://www.sprocketsecurity.com/blog/pentesting-types-2>
- [103] BrightSec - "9 Penetration Testing Types" (2025-03-24)
 - URL: <https://brightsec.com/blog/penetration-testing-types/>
- [110] Coursera - "What Are the Different Types of Penetration Testing?" (2025-06-04)
 - URL: <https://www.coursera.org/articles/types-of-penetration-testing>

Bibliografía

Categorías

testing

-
- [98] CyberSapiens - "Which tools should be used to perform a wireless infrastructure penetration test" (2025-06-05)
 - URL: <https://cybersapiens.com.au/high-tools-should-be-used-to-perform-a-wireless-infrastructure-penetration-test/>
 - [105] VikingCloud - "What is Wireless Penetration Testing?" (2025-09-08)
 - URL: <https://www.vikingcloud.com/blog/what-is-wireless-penetration-testing>
 - [111] Threat Intelligence - "What is Wireless Penetration Testing?" (2024-11-06)
 - URL: <https://www.threatintelligence.com/blog/wireless-penetration-testing>

Bibliografía Physical & Social Engineering

-
- [112] ISACA - "Physical Penetration Testing" (White Paper, 2023-09-04)
 - URL: <https://www.isaca.org/resources/white-papers/2023/physical-penetration-testing>
 - [115] Sprocket Security - "Social Engineering Penetration Testing: A Practical Guide" (2024-09-26)
 - URL: <https://www.sprocketsecurity.com/blog/social-engineering-penetration-testing-a-practical-guide>
 - [118] University of Twente - "Two methodologies for physical penetration testing using social engineering"
 - URL: https://research.utwente.nl/files/5468345/ACSAC_pentesting_methodology_%5B1%5D.pdf
 - [121] Ares Security - "A Deep Dive into Physical Penetration Testing" (2024-10-31)
 - URL: <https://aressecuritycorp.com/2024/11/01/physical-penetration-testing/>
 - [124] Tesserent - "What Is Physical Penetration Testing? Pen testing explained" (2024-12-10)
 - URL: <https://tesserent.com/resources/what-is-physical-penetration-testing-pentests-explained>
 - [127] PurpleSec - "Social Engineering Penetration Testing: Attacks, Methods, and Tools" (2025-07-17)
 - URL: <https://purplesec.us/learn/social-engineering-penetration-testing/>
 - [130] PurpleSec - "13 Physical Penetration Testing Methods That Work" (2025-07-17)
 - URL: <https://purplesec.us/learn/physical-penetration-testing/>

Bibliografía

Categorías

testing

- ##### Cloud & IoT Testing
- [113] Passcurity - "Penetration Testing in 2025: New Focus on Cloud and IoT Security" (2025-04-28)
- URL: <https://passcurity.com/penetration-testing-2025-cloud-iot-security/>
- [116] Haxoris - "IoT and Embedded Device Penetration Testing" (2024-10-31)
- URL: <https://haxoris.com/services/penetration-testing/iot>
- [119] Integrity360 - "What is IoT penetration testing and why do you need It?" (2024-09-15)
- URL: <https://insights.integrity360.com/what-is-iot-penetration-testing-and-why-do-you-need-it>
- [122] Praetorian - "IoT Penetration Testing that Identifies Security Risks" (2024-06-30)
- URL: <https://www.praetorian.com/services/iot-penetration-testing/>
- [125] Bright Defense - "What is IoT Penetration Testing?" (2025-06-25)
- URL: <https://www.brightdefense.com/resources/iot-penetration-testing/>
- [128] CloudTribe - "What Is IoT Penetration Testing?"
- URL: <https://cloudtri.be/pentest/iot/>
- [131] Microminder CS - "IoT Penetration Testing: Why It Matters and How It's Done" (2025-07-30)
- URL: <https://www.micromindercs.com/blog/iot-penetration-testing>

Bibliografía API & Mobile Testing

-
- [114] SecureIdeas - "API and Mobile App Penetration Testing"
 - URL: <https://www.secureideas.com/api-and-mobile-app-penetration-testing>
 - [117] Appknox - "What is API Security for Mobile Apps? Why Is It Important?" (2025-03-11)
 - URL: <https://www.appknox.com/blog/complete-guide-on-api-security-for-mobile-apps>
 - [120] Akamai - "What Is API Penetration Testing?" (2025-03-18)
 - URL: <https://www.akamai.com/glossary/what-is-api-penetration-testing>
 - [123] VeraSafe - "Mobile App and API Penetration Testing Service"
 - URL: <https://verasafe.com/cybersecurity-solutions/mobile-app-penetration-testing/>
 - [126] Qualysec - "Mobile App Security Testing" (2025-06-19)
 - URL: <https://qualysec.com/mobile-app-security-testing/>
 - [129] Datami - "Mobile Application Penetration Testing Services" (2025-08-31)
 - URL: <https://datami.ee/services/pentest/mobile-app-penetration-testing/>

Bibliografía Herramientas de Pentesting

- [59] Campus Ciberseguridad - "Burp Suite una herramienta de pentesting" (2025-06-15)
- URL: <https://www.campusciberseguridad.com/blog/burp-suite-una-herramienta-de-pentesting/>
- [62] Logic Solutions - "Explorando las herramientas más eficaces para el pentesting en 2024" (2024-09-18)
- URL: <https://www.logicsolutions.es/es/blog/explorando-las-herramientas-mas-eficaces-para-el-pentesting-en-2024>
- [65] Campus Ciberseguridad - "Metasploit. La herramienta esencial en Ciberseguridad" (2025-08-11)
- URL: <https://www.campusciberseguridad.com/blog/metasploit-herramienta-esencial-ciberseguridad/>
- [68] Check Point - "Las 19 mejores herramientas para pruebas de penetración" (2024-03-27)
- URL: <https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-penetration-testing/top-19-penetration-testing-tools/>
- [71] Metasploit - "Metasploit | Penetration Testing Software" (2025-06-05)
- URL: <https://www.metasploit.com>
- [74] Tecnógrafos - "Las 13 herramientas más usadas para pentesting y hacking" (2022-05-11)
- URL: <https://tecnografos.es/2022/05/12/las-13-herramientas-mas-usadas-para-pentesting-y-hacking-por-los-profesionales/>
- [77] HackMetrix - "Penetration Testing: 5 herramientas que ayudan a su ejecución" (2024-08-08)
- URL: <https://blog.hackmetrix.com/penetration-testing/>

Bibliografía Templates

- ##### GitHub Repositories - Templates
- [16] Julio Cesar Fort - "public-pentesting-reports"
- URL: <https://github.com/juliocesarfort/public-pentesting-reports>
- [190] MTK911 - "pentest-report-template" (2020-04-01)
- URL: <https://github.com/MTK911/pentest-report-template>
- [191] Heath Adams (TCM Security) - "TCM-Security-Sample-Pentest-Report" (2019-05-26)
- URL: <https://github.com/hmaverickadams/TCM-Security-Sample-Pentest-Report>
- [192] h0tPlug1n - "Web-Penetration-Testing-Report-Sample" (2021-09-02)
- URL: <https://github.com/h0tPlug1n/Web-Penetration-Testing-Report-Sample>
- [196] cyber-cfreg - "Penetration-Test-Report-Template" (2022-02-28)
- URL: <https://github.com/cyber-cfreg/Penetration-Test-Report-Template>
- [199] Reconmap - "pentest-reports" (2020-08-27)
- URL: <https://github.com/reconmap/pentest-reports>
- [202] Ryan Sapone - "Web-Pentest-Report" (2024-04-25)
- URL: <https://github.com/Ryan-Sapone/Web-Pentest-Report>
- [205] PwnDoc - "pwndoc: Pentest Report Generator" (2025-08-25)
- URL: <https://github.com/pwndoc/pwndoc>

Bibliografía

Checklists

- [194] Harshinsecurity - "web-pentesting-checklist" (2020-10-24)
- URL: <https://github.com/harshinsecurity/web-pentesting-checklist>
- [197] Hrishikesh7665 - "Android-Pentesting-Checklist" (2022-12-30)
- URL: <https://github.com/Hrishikesh7665/Android-Pentesting-Checklist>
- [203] OWASP - "OWASP Web Application Penetration Checklist v1.1"
- URL: https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Web_Application_Penetration_Checklist_v1_1.pdf
- [206] Indusface - "API PenTesting Checklist (XLSX)"
- URL: <https://www.indusface.com/downloads/api-pen-testing-checklist-indusface.xlsx>
- [200] A-Lign - "A Comprehensive Checklist for Penetration Testing" (2025-05-29)
- URL: <https://www.a-lign.com/articles/penetration-testing-checklist>

Bibliografía Reportes Públicos

- [Assessment-Report-Template.pdf](#)
- [193] PentestReports.com - "Free Penetration Test Report Templates"
- URL: <https://pentestreports.com/templates>
- [195] PurpleSec - "Sample Vulnerability Assessment Report - Example Institute"
- URL: <https://purplesec.us/wp-content/uploads/2019/12/Sample-Vulnerability-Assessment-Report-PurpleSec.pdf>
- [198] PurpleSec - "Sample Network Vulnerability Assessment Report"
- URL: <https://purplesec.us/wp-content/uploads/2019/03/Sample-Network-Security-Vulnerability-Assessment-Report-Purplesec.pdf>
- [201] MaxAPEX - "Vulnerability Assessment Report Template"
- URL: <https://www.maxapex.com/wp-content/uploads/2024/07/Vulnerability->
- [204] Indusface - "Vulnerability Assessment Report"
- URL: https://www.indusface.com/images/download/Vulnerability_Assessment_Sample_Report.pdf
- [207] Invia - "Vulnerability Assessment and Penetration Testing Report"
- URL: <https://invia.com.au/App/media/sample%20vapt%20report.pdf>
- [208] Overleaf - "Penetration Test Report Template (LaTeX)" (2025-09-30)
- URL: <https://www.overleaf.com/latex/templates/penetration-test-report-template/gbzgfgsnqyvq>