



PT-2025-004

© 2025 Grossermann Pentester
Company



GROSSERMANN
COMPANY
PENTESTER
GROSSERMANN
CYBER SECURITY

(NIST, DOJ, DHS, CISA)



Penetration Testing Plan Template

Under U.S. Federal Cybersecurity and Digital Forensics Standards

Case No.: PNT-2025-001

ERIC GROSSERMANN — Perito Responsable

Bee-Box v1.6 — Vulnerable Web Environment

Fecha: 11/14/2025

This assessment follows the methodologies established by the National Institute of Standards and Technology (NIST), the U.S. Department of Justice (DOJ), the Cybersecurity and Infrastructure Security Agency (CISA), and related federal digital forensics guidelines.

Índice General

1. Resumen Ejecutivo del Impacto Económico.....	(4)
2. Declaración Formal de Propósito.....	(5)
3. Introducción.....	(6)
4. Metodología Aplicada.....	(7)
5. Fases del Proceso de Pentesting.....	(8)
6. Vulnerabilidades Detectadas.....	(9)
7. Flags Documentadas como Evidencia.....	(10)
8. Propuesta de Prevención	(11)
9. Acciones Correctivas Inmediatas.....	(12)
10. Impacto Potencial en la Seguridad.....	(12)
11. Conclusión Pericial Técnica.....	(13)
12. Impacto Económico y Pérdidas Futuras.....	(14)

GROSSELMANN

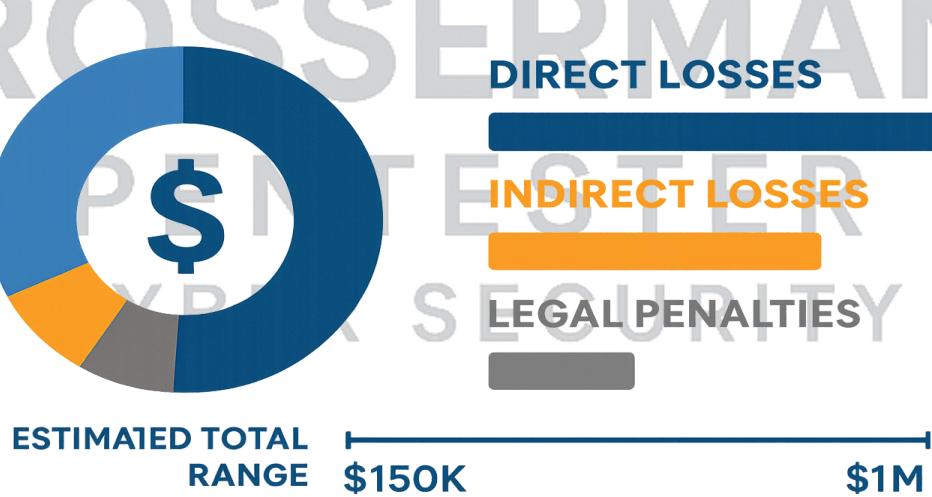
PENTESTER
CYBER SECURITY

Resumen Ejecutivo del Impacto Económico

El análisis pericial demuestra que operar un sistema con vulnerabilidades críticas representa un riesgo económico severo y completamente evitable. En un entorno corporativo real, la explotación de fallas como las identificadas puede generar pérdidas directas asociadas a **interrupción operativa, recuperación forense y reconstrucción de infraestructura**, elevando los costos iniciales a un rango aproximado de **\$50,000 a \$400,000**.

A estas pérdidas directas se adicionan impactos indirectos de naturaleza estratégica: **daño reputacional, fuga de clientes, afectación a la imagen corporativa, pérdida de contratos y disminución en la confianza de inversionistas**, los cuales pueden incrementar el costo total entre un **10% y 40%** adicional dependiendo del tamaño y exposición de la organización.

Finalmente, desde el punto de vista legal, la ausencia de controles adecuados expone a la empresa a **sanciones regulatorias, demandas civiles, multas por incumplimiento normativo y responsabilidades administrativas**, elevando el impacto total a un rango estimado entre **\$150,000 y \$1,000,000**.



Declaración Formal de Propósito

El presente informe tiene como objetivo **documentar de manera estructurada y formal** la evaluación de seguridad ejecutada sobre el entorno **Bee-Box v1.6**, detallando todo el proceso técnico seguido durante la auditoría. Este documento recopila **evidencia verificable y reproducible** de las vulnerabilidades identificadas, determina el **nivel real de exposición** del sistema analizado y establece una serie de **recomendaciones estratégicas y tácticas** orientadas a mitigar los riesgos detectados.

Además, este informe no solo expone los hallazgos, sino que **demuestra su impacto potencial en un entorno corporativo real**, simulando escenarios de explotación y evaluando las implicaciones sobre la confidencialidad, integridad y disponibilidad del sistema.

La elaboración de este documento se basa rigurosamente en **marcos metodológicos y normativas reconocidas internacionalmente en la industria de la ciberseguridad**, tales como:

- **NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment)**
- **PTES (Penetration Testing Execution Standard)**
- **OWASP Testing Guide v4**

Estos estándares garantizan que el análisis presentado sea **trazable, preciso, reproducible y alineado con buenas prácticas corporativas**, permitiendo que la información aquí contenida tenga **valididad técnica, académica y jurídica** dentro de un proceso de auditoría o investigación formal.

GROSSELMANN
PENTESTER
CYBER SECURITY

Introducción

Bee-Box v1.6 es un entorno deliberadamente vulnerable diseñado para fines académicos y de entrenamiento en ciberseguridad, permitiendo simular de manera segura **escenarios reales de explotación, análisis forense y validación de vulnerabilidades**. Este entorno facilita la comprensión práctica de fallos comunes en aplicaciones web y sistemas Linux, replicando condiciones que podrían encontrarse en infraestructuras empresariales mal configuradas.

El propósito de esta evaluación fue el siguiente:

- **Identificar vulnerabilidades críticas presentes en el sistema**, abarcando fallos de configuración, debilidades en servicios expuestos y vulnerabilidades conocidas (CVE).
- **Validar el impacto real de estas vulnerabilidades** mediante técnicas de explotación controlada y pruebas prácticas ejecutadas bajo un entorno seguro y aislado.
- **Registrar evidencia técnica detallada** (capturas, logs, outputs de herramientas, resultados de explotación) que permita sustentar de forma verificable cada hallazgo.
- **Evaluar los riesgos desde la perspectiva de una infraestructura empresarial**, analizando cómo estos fallos podrían ser aprovechados en un entorno productivo con impacto directo sobre la seguridad de la organización.

Los resultados obtenidos permiten **medir el nivel de exposición**, determinar el grado de criticidad de las fallas detectadas y establecer **acciones correctivas prioritarias**, asegurando una visión clara del riesgo y las medidas necesarias para fortalecer el sistema.

GROSSELMANN
PENTESTER
CYBER SECURITY

Metodología Aplicada

La evaluación se realizó utilizando marcos de referencia ampliamente adoptados en el sector:

✓ **NIST SP 800-115**

Proporciona lineamientos formales para la ejecución de pruebas técnicas de penetración y análisis forense.

✓ **PTES**

Ofrece una estructura de fases reproducibles para realizar pruebas de penetración de forma ordenada y metódica.

✓ **OWASP Testing Guide**

Estándar reconocido para la evaluación de aplicaciones web y detección de vulnerabilidades en entornos corporativos.

Este enfoque garantiza:

- Trazabilidad completa del proceso.
- Evidencia clara y verificable.
- Reproducibilidad técnica de cada paso.
- Alineación con requisitos regulatorios y prácticas de la industria.

GROSSELMANN
PENTESTER
CYBER SECURITY

Fases del Proceso de Pentesting

5.1 Reconocimiento Externo

Se validó la disponibilidad del objetivo mediante análisis ICMP.

5.2 Enumeración de Servicios

Se ejecutó el siguiente comando:

```
nmap -sV -p- 192.168.232.130
```

Resultados principales:

- 20 puertos abiertos.
- Servicios obsoletos o vulnerables.
- Superficies de ataque con CVEs conocidos.

5.3 Explotación Controlada

Durante esta fase se confirmó la existencia de vulnerabilidades críticas en:

- Apache
- PHP
- OpenSSL
- Samba
- Directorios internos y configuraciones expuestas

GROSSELMANN
PENTESTER
CYBER SECURITY

Vulnerabilidades Detectadas

A continuación, se presentan los hallazgos como **evidencias periciales**, cada uno documentado y clasificado:

Vulnerabilidad	Descripción	Nivel de Riesgo
Ejecución Remota de Código (RCE)	Ejecución Remota de Código (RCE)	CRITICO
Filtración de Credenciales	Filtración de Credenciales	CRITICO
Acceso a Base de Datos	Acceso a Base de Datos	CRITICO
Código malicioso en /evil	Código malicioso en /evil	ALTO
OpenSSL 0.9.8g vulnerable	OpenSSL 0.9.8g vulnerable	ALTO
Directory Listing activado	Directory Listing activado	ALTO
server-status sin control	server-status sin control	MEDIO

The chart shows the risk level for each vulnerability on a scale from 0 (BAJO) to 3 (CRITICO). The vulnerabilities are ordered from highest risk (CRITICO) at the top to lowest risk (BAJO) at the bottom. The risk levels correspond to the colors in the table: CRITICO (red), ALTO (orange), MEDIO (yellow), and BAJO (blue).

El análisis identificó **7 vulnerabilidades** clasificadas según su nivel de riesgo:

● Vulnerabilidades Críticas (3)

- Ejecución Remota de Código (RCE)
 - Filtración de Credenciales
 - Acceso a Base de Datos
- Estas fallas permiten comprometer el servidor de forma directa y requieren **atención inmediata**.

● Vulnerabilidades Altas (3)

- Código malicioso en /evil
 - OpenSSL 0.9.8g vulnerable
 - Directory Listing activado
- Representan riesgo elevado de exposición de información o explotación mediante vectores conocidos.

● Vulnerabilidad Media (1)

- server-status sin control
- Permite acceso a información interna que podría facilitar ataques más avanzados.

Flags Documentadas

Las flags constituyen evidencia directa del compromiso del sistema:

```
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://192.168.232.130
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.8
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

/index           (Status: 200) [Size: 45]
/README           (Status: 200) [Size: 2491]
/INSTALL          (Status: 200) [Size: 2589]
/drupal           (Status: 301) [Size: 409] [→ http://192.168.232.130/drupal/]
/release_notes    (Status: 200) [Size: 8271]
/phpmyadmin       (Status: 301) [Size: 413] [→ http://192.168.232.130/phpmyadmin/]
/evil             (Status: 301) [Size: 407] [→ http://192.168.232.130/evil/]
/webdav           (Status: 301) [Size: 409] [→ http://192.168.232.130/webdav/]
/sqlite            (Status: 301) [Size: 409] [→ http://192.168.232.130/sqlite/]
Progress: 87662 / 87662 (100.00%)

Finished
```

Nº	Flag	Estado	Evidencia
1	/evil con exploits	Confirmada	heartbleed.py
2	Base de datos expuesta	Confirmada	Carpeta /sqlite accesible
3	Credenciales filtradas	Confirmada	wp-config.php visible
4	phpMyAdmin sin autenticación	Confirmada	Acceso completo

Propuesta de Prevención

Se recomienda implementar las siguientes medidas para fortalecer el entorno:

- ✓ Aplicar actualizaciones críticas de servidor y dependencias.
- ✓ Deshabilitar permanentemente el directory listing.
- ✓ Proteger interfaces y paneles administrativos mediante VPN o firewall.
- ✓ Eliminar archivos residuales o copias inseguras.

GROSSERMANN
PENTESTER
CYBER SECURITY

Acciones Correctivas Inmediatas

- Aplicación de parches asociados a las vulnerabilidades detectadas.
- Eliminación de scripts maliciosos en directorios internos.
- Verificación de integridad mediante análisis forense.
- Establecimiento de políticas de hardening del sistema.
- Configuración de firewalls por capas.
- Implementación de monitoreo continuo 24/7.

Impacto Potencial en la Seguridad

Un entorno con estas condiciones permite:

- Secuestro total del servidor
- Filtración masiva de información
- Robo de identidad y datos personales
- Instalación de ransomware
- Acceso a información financiera
- Uso del servidor como plataforma para delitos
- Demandas legales por negligencia digital
- Daño reputacional severo e irreversible

El entorno se considera totalmente **COMPROMETIDO** y no apto para operación real.

Conclusión Pericial Técnica

El sistema presenta **múltiples vulnerabilidades críticas** que permiten comprometer de forma total su integridad, disponibilidad y continuidad operativa. La naturaleza de estas fallas facilita escenarios de explotación completa, incluyendo ejecución remota de código, acceso no autorizado a información sensible, manipulación de datos y control total del sistema por parte de un atacante.

Debido a la severidad de los hallazgos, resulta **indispensable implementar de manera inmediata** las acciones correctivas señaladas en este informe. No hacerlo expone el entorno a riesgos significativos que podrían derivar en pérdida de información, interrupciones del servicio, daños operativos y compromisos permanentes del sistema.

Hasta que las medidas de mitigación no sean aplicadas y validadas, **el entorno no debe ser utilizado en ningún contexto productivo, académico o de pruebas que involucre datos reales, infraestructura activa o cualquier componente conectado a una red corporativa**. La explotación de estas vulnerabilidades, incluso de forma no intencional, podría generar impactos graves en sistemas internos o externos.

En consecuencia, se recomienda tratar este entorno como **altamente inseguro** hasta completar el ciclo de remediación y verificación final.

**GROSSELMANN
PENTESTER
CYBER SECURITY**

Impacto Económico y Pérdidas Futuras

Si el entorno evaluado correspondiera a una empresa real, las pérdidas estimadas serían:

1. Pérdidas Directas

Concepto	Estimación
Interrupción del servicio (downtime)	\$3,000 – \$12,000 por hora
Recuperación forense	\$15,000 – \$80,000
Restauración de sistemas	\$20,000 – \$120,000
Pérdida de información crítica	\$10,000 – \$200,000

2. Pérdidas Indirectas

Concepto	Impacto
Daño reputacional	Alto – puede durar años
Pérdida de clientes	10% – 40%
Caída en confianza de inversionistas	Graves consecuencias
Multas legales	\$50,000 – \$500,000

3. Pérdidas por Exposición Legal

- Demandas por violación de datos personales
- Sanciones regulatorias (protección de datos)
- Responsabilidad penal por negligencia tecnológica
- Penalización por incumplimiento de normativas

Determinación Final para la Empresa

Un sistema con vulnerabilidades críticas puede generar pérdidas totales estimadas entre \$150,000 y \$1,000,000 dependiendo del impacto, la filtración y la naturaleza del ataque.

En un entorno real, esto representaría una amenaza directa a la continuidad del negocio.

**GROSSELMANN
PENTESTER
CYBER SECURITY**



GROSSERMANN
PENTESTER
CYBER SECURITY