> BARRSEC_

REPORTE EJECUTIVO DE LA AUDITORÍA

OWASP Testing Guide v4.2 · CVSS v3.1 · Black-box Methodology

CLIENTE	Institución Educativa (Anonimizado — Caso de Portafolio)	VERSIÓN	v1.0
FECHA	Marzo 2026	CONSULTOR	Diego B. — BARRSEC
CLASIFICACIÓN	CONFIDENCIAL	COBERTURA	Black-box · Infraestructura pública e IP perimetral

01

SECCIÓN 01

Resumen Ejecutivo

Se realizó una evaluación de seguridad en modalidad black-box sobre la infraestructura pública del objetivo. Los portales principales, incluyendo el sistema central de autenticación SAML, cuentan con una postura de seguridad robusta, fuertemente defendida por un Firewall de Aplicaciones Web (WAF) corporativo que mitiga eficazmente ataques automatizados y manipulación manual de parámetros. Sin embargo, durante la fase de reconocimiento de subdominios se identificó un endpoint secundario crítico — perteneciente a un entorno paralelo de e-commerce/marketing con protección considerablemente menor que el dominio principal — que expone a la infraestructura a un riesgo severo de compromiso del servidor por una vulnerabilidad de subida de archivos sin restricciones.

3	9.8	1	3-5d
HALLAZGOS TOTALES	CVSS MÁS ALTO	HALLAZGOS CRÍTICOS	DURACIÓN AUDITORÍA

Rating de riesgo general: CRÍTICO. El hallazgo crítico permanece abierto. Remediación recomendada dentro de 24-72 horas dado que es explotable por un atacante no autenticado.

02

SECCIÓN 02

Metodología

01

Reconocimiento y Mapeo de Superficie

Escaneo de puertos TCP SYN con evasión de firewall perimetral (Nmap sin descubrimiento de host, manipulación de puerto de origen simulando tráfico DNS).

02

Descubrimiento de Subdominios y Fingerprinting

Enumeración pasiva de subdominios y fingerprinting de tecnologías, identificando entornos paralelos con menor nivel de protección que el dominio principal.

03

Pruebas Activas y Explotación

Pruebas de fuerza bruta, fuzzing y parameter tampering sobre los formularios de autenticación, con validación de las defensas del WAF.

04

Análisis de Configuración

Escaneo de cabeceras de seguridad, configuración TLS y vulnerabilidades conocidas sobre los subdominios secundarios identificados.

05

Reporte + Remediación

Matriz de riesgo, hallazgos priorizados, y recomendaciones de remediación por hallazgo.

SECCIÓN 03

Stack Tecnológico Identificado

- Portal SSO corporativo (SAML / Novell Access Manager)
- WAF corporativo Imperva Incapsula
- Infraestructura web distribuida en múltiples subdominios
- Subdominio secundario de e-commerce/marketing (entorno paralelo)

04

SECCIÓN 04

Resumen de Hallazgos

#	HALLAZGO	SEVERIDAD	CVSS	ESTADO
1	Subida de Archivos sin Restricciones (RCE) — CVE-2025-54236	CRÍTICO	9.8	Abierto
2	Falta de Cabeceras de Seguridad y Exposición de Versión TLS	BAJO	3.1	Abierto
3	Anomalía en Envío de Credenciales (parámetro de respaldo codificado)	INFORMATIVO	2.0	Mitigado (WAF)

La tabla resume los hallazgos documentados en esta evaluación. El detalle técnico completo de cada uno — descripción, evidencia, impacto y remediación — se presenta en la Sección de Hallazgos Detallados.

HALLAZGO 1

[CRÍTICO]

9.8

Subida de Archivos sin Restricciones (RCE) — CVE-2025-54236

ACTIVO AFECTADO

Subdominio secundario de e-commerce/marketing — endpoint de carga de archivos

CATEGORÍA OWASP

A05:2021 — Security Misconfiguration / CWE-434

DESCRIPCIÓN

Mediante escaneo automatizado sobre la infraestructura secundaria descubierta durante el reconocimiento de subdominios, se detectó que un endpoint de carga de archivos en un entorno paralelo de e-commerce/marketing es vulnerable a CVE-2025-54236, la cual permite subir archivos evadiendo las restricciones de tipo/extensión esperadas.

EVIDENCIA / POC

```
nmap -p 80,443,8000,8080,8443 -sS -Pn -g 53 [IP_ANONIMIZADA]
-> Puertos 80/443/8000/8080/8443 abiertos (evasión de firewall vía
spoofing de puerto de origen 53/DNS)
Endpoint vulnerable identificado: /customer/address_file/upload
[CVE-2025-54236] [http] [critical] confirmado por escáner automatizado
```

IMPACTO

Un atacante no autenticado podría evadir los filtros de subida y alojar scripts maliciosos (web shells) para lograr Ejecución Remota de Código (RCE), comprometiendo el servidor del subdominio afectado y, potencialmente, sirviendo como pivote hacia el resto de la infraestructura.

RECOMENDACIÓN / REMEDIACIÓN

Aplicar el parche de seguridad correspondiente del proveedor a la brevedad (ventana de 24-72h dado que es explotable sin autenticación). Adicionalmente: validar el tipo de archivo por contenido real (magic bytes) y no solo por extensión, almacenar los archivos subidos fuera del webroot, y deshabilitar la ejecución de scripts en el directorio de subidas.

HALLAZGO 2

[BAJO]

3.1

Falta de Cabeceras de Seguridad y Exposición de Versión TLS

ACTIVO AFECTADO

Subdominio secundario (portal de biblioteca/recursos)

CATEGORÍA OWASP

A05:2021 — Security Misconfiguration

DESCRIPCIÓN

Los escaneos automatizados sobre el subdominio secundario revelaron la ausencia de cabeceras de seguridad estrictas (Content-Security-Policy, Strict-Transport-Security) y expusieron información sobre la versión de TLS en uso.

EVIDENCIA / POC

```
Escaneo automatizado: headers ausentes [content-security-policy,
strict-transport-security]. Escáner agresivo complementario bloqueado
exitosamente por WAF genérico tras 20 errores de conexión consecutivos.
```

IMPACTO

Superficie de ataque incrementada ante clickjacking y degradación de protocolo; riesgo bajo de forma aislada, pero incrementa la efectividad de otros vectores si se combina con hallazgos futuros.

RECOMENDACIÓN / REMEDIACIÓN

Implementar Content-Security-Policy y Strict-Transport-Security de forma estricta en todos los subdominios, no solo en el portal principal. Deshabilitar versiones obsoletas de TLS.

HALLAZGO 3

[INFORMATIVO]

2.0

Anomalía en Envío de Credenciales (parámetro de respaldo codificado)

ACTIVO AFECTADO

Portal SSO corporativo (SAML / Novell Access Manager)

CATEGORÍA OWASP

A02:2021 — Cryptographic Failures (uso de codificación como sustituto de cifrado)

DESCRIPCIÓN

El formulario de inicio de sesión del portal SSO envía la contraseña en texto plano junto con una copia adicional codificada en Base64 en un parámetro separado — una práctica de diseño redundante, ya que Base64 no constituye cifrado ni aporta protección real.

EVIDENCIA / POC

```
Parameter Tampering en Burp Suite Repeater: al eliminar/alterar el
parámetro codificado en Base64, el WAF corporativo bloqueó la
transacción devolviendo HTTP/1.1 403 Forbidden.
```

IMPACTO

Ninguno explotable de forma directa gracias al WAF; sin embargo, la mitigación depende de un control de terceros (el WAF) para compensar una debilidad de diseño propia del formulario.

RECOMENDACIÓN / REMEDIACIÓN

Refactorizar la lógica del formulario para eliminar el parámetro Base64 redundante del lado del cliente. No depender exclusivamente del WAF como única capa de defensa para una debilidad de diseño conocida.

05

SECCIÓN 05

Matriz de Riesgo y Priorización

TIER 1 · ATENDER DENTRO DE 24-72 HORAS

Explotabilidad alta

- Subida de Archivos sin Restricciones (RCE) — CVE-2025-54236

TIER 3 · MEJORES PRÁCTICAS CONTINUAS

Fortalecimiento a largo plazo

- Auditorías de seguridad trimestrales
- Capacitación de seguridad al equipo de desarrollo
- Implementación de Web Application Firewall (WAF)
- Testing de seguridad integrado al pipeline de CI/CD

06

SECCIÓN 06

Conclusiones y Recomendaciones

La infraestructura evaluada demuestra una madurez de seguridad desigual: el portal principal de autenticación SSO está sólidamente defendido — se validó resistencia efectiva a ataques de fuerza bruta y a enumeración de usuarios, con el WAF corporativo bloqueando consistentemente intentos automatizados y manipulación manual de parámetros. Sin embargo, esta fortaleza no se replica en los entornos paralelos (subdominios secundarios de e-commerce/marketing y biblioteca), donde se concentra el riesgo real: la vulnerabilidad crítica de subida de archivos sin restricciones representa una vía de compromiso total del servidor. Se recomienda extender la misma rigurosidad de seguridad del dominio principal a todos los entornos paralelos, y realizar revisiones periódicas de superficie de ataque en subdominios, ya que estos suelen ser el eslabón más débil de la infraestructura.

ESTADO ACTUAL

CRÍTICO

→

POST-REMEDIACIÓN

BAJO

El riesgo no se reduce solo, se remedia.

Cada hallazgo de este reporte es una puerta abierta hasta que se cierra.