EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://comerciallucy.codeplex.vip/pages/login	Checks	9 pruebas
Dominio	comerciallucy.codeplex.vip	Hallazgos	43 totales
Fecha	31 de julio de 2026 a las 20:46	Problemas	16 detectados

D

58/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio comerciallucy.codeplex.vip ha resultado en una puntuación de 58/100, lo que otorga una calificación de grado D. Se realizaron 9 checks pasivos, de los cuales 5 fueron satisfactorios y 4 detectaron fallos críticos en la configuración de la infraestructura y el servidor web. La ausencia de un pentest activo limita la profundidad del hallazgo, pero los datos obtenidos revelan una superficie de ataque considerablemente expuesta. Debido a la apertura de puertos de bases de datos y la falta de cabeceras de protección esenciales, el sitio se considera vulnerable y con un nivel de riesgo elevado.

Resumen de Riesgos

1	5	9	1	27
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 41 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 41 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  41 dias restantes (expira: 2026-09-11T05:27:38.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-13T05:27:39.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: frame-ancestors *
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto
- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos es accesible desde internet, lo que permite ataques directos de fuerza bruta o explotación de vulnerabilidades del motor de base de datos.
[HIGH] Puerto 21 (FTP) abierto: Este servicio transmite archivos y credenciales sin cifrado, permitiendo la interceptación de datos sensibles en la red.
[HIGH] X-Frame-Options ausente: La falta de esta cabecera permite que el sitio sea cargado en iframes maliciosos, facilitando ataques de secuestro de clic o clickjacking.
[HIGH] Strict-Transport-Security (HSTS) ausente: El servidor no instruye al navegador para usar exclusivamente conexiones seguras, permitiendo ataques de degradación de protocolo.

[HIGH] Redirección HTTPS no configurada: El tráfico que entra por el puerto 80 no se redirige automáticamente al puerto seguro, dejando la comunicación inicial expuesta.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de administración remota está expuesto públicamente, aumentando el riesgo de ataques dirigidos contra el acceso al servidor.
[MEDIUM] X-Content-Type-Options ausente: Facilita ataques de MIME-sniffing, donde un navegador podría interpretar archivos de texto como scripts ejecutables maliciosos.
[MEDIUM] Archivos informativos accesibles: La presencia de archivos como readme.html y README.txt, junto a rutas administrativas expuestas, facilita la fase de reconocimiento para un atacante.
[MEDIUM] Referrer-Policy y Permissions-Policy ausentes: Falta de control sobre la información de navegación compartida y sobre el acceso del navegador a periféricos como cámara o micrófono.
[LOW] Cabecera de servidor expuesta: El servidor informa explícitamente que utiliza Apache, proporcionando información valiosa para buscar exploits específicos de dicha tecnología.