EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://lucsam.cl/	Checks	9 pruebas
Dominio	lucsam.cl	Hallazgos	54 totales
Fecha	27 de mayo de 2026 a las 04:23	Problemas	19 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 68/100, lo que corresponde a una calificación de Grado C. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 5 aprobados, 1 advertencia y 3 fallos críticos en configuraciones de red y aplicación. Aunque el certificado SSL es válido, la ausencia de cabeceras de seguridad esenciales y la presencia de contenido mixto comprometen la integridad de la plataforma. Debido a la exposición de versiones de software y falta de protección contra ataques comunes, se concluye que el sitio es actualmente vulnerable. El riesgo detectado es moderado-alto y requiere intervención técnica inmediata para mitigar posibles vectores de explotación.

Resumen de Riesgos

0	4	11	4	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 dias
Cabeceras de Seguridad	40	FALLO	Solo 2/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 6.9.4 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	7 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-08-08T00:46:28.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-10T00:46:29.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 2/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.30 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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
- INFO **Permissions-Policy**
  Presente: private-state-token-redemption=(self "https://www.google.com" "https://www.gstat...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://lucsam.cl/
- 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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  PHP/8.3.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 20/100

Estado: FALLO

7 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://lucsam.cl/wp-content/uploads/2026/03/Logo-LucsamTech-...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://lucsam.cl/wp-content/uploads/2026/03/Logo-LucsamTech-...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://lucsam.cl/wp-content/uploads/2026/03/Logo-LucsamTech-...
- MEDIO **Recurso HTTP (CSS url())**
  http://lucsam.cl/wp-content/uploads/2026/03/LUcsam-IA-1.png
- MEDIO **Recurso HTTP (CSS url())**
  http://lucsam.cl/wp-content/uploads/2022/05/card-lines-backg...
- MEDIO **Recurso HTTP (CSS url())**
  http://lucsam.cl/wp-content/uploads/2022/05/card-lines-backg...
- MEDIO **CSS url()**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (110 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://lucsam.cl/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- INFO **Puerto 22 (SSH)**
  Cerrado — 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
- INFO **Puerto 3306 (MySQL)**
  Cerrado — 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

[HIGH] WordPress version 6.9.4 expuesta: Permite a atacantes identificar vulnerabilidades específicas y CVEs conocidos para esta versión.
[HIGH] Falta de X-Frame-Options: La ausencia de esta cabecera hace que el sitio sea susceptible a ataques de Clickjacking.
[HIGH] Falta de Strict-Transport-Security (HSTS): No se fuerza la conexión segura en el navegador, permitiendo ataques de degradación de protocolo.
[MEDIUM] Contenido Mixto (7 recursos): El sitio carga imágenes y scripts mediante HTTP en una página HTTPS, lo que debilita el cifrado.
[MEDIUM] Ruta /wp-login.php accesible: El panel de administración está expuesto a ataques de fuerza bruta y escaneo automatizado.
[MEDIUM] Archivo /readme.html accesible: Este archivo revela información técnica sobre el CMS que debería ser privada.
[MEDIUM] Falta de X-Content-Type-Options: El sitio es vulnerable a ataques de sniffing de tipos MIME por parte del navegador.
[MEDIUM] Falta de Referrer-Policy: No existe control sobre la información de referencia enviada a otros dominios durante la navegación.
[LOW] Cabecera Server expuesta (hcdn): Revela la tecnología del servidor facilitando el reconocimiento para un atacante.
[LOW] Cabecera X-Powered-By expuesta (PHP/8.3.30): Expone la versión exacta del lenguaje de programación utilizado.
[LOW] Meta generator WordPress expuesto: Facilita la identificación rápida del CMS y su versión actual.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a directorios de administración en un archivo público.