

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cel.gob.sv	Checks	9 pruebas
Dominio	cel.gob.sv	Hallazgos	51 totales
Fecha	4 de octubre de 2026 a las 19:27	Problemas	12 detectados

C

70/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio cel.gob.sv ha resultado en una puntuación de 70/100, otorgando una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron correctos, 1 presentó advertencias y 3 fallaron significativamente. El portal demuestra un manejo adecuado del cifrado de datos y redirecciones seguras, pero presenta deficiencias críticas en la configuración de cabeceras de seguridad y protección de cookies. Debido a la exposición de versiones de software y la falta de políticas contra ataques de inyección, el sitio se considera vulnerable a amenazas dirigidas que podrían comprometer la integridad de la plataforma.

Resumen de Riesgos

0	4	5	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 41 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.8.10 expuesta, WordPress 2 expuesta
Seguridad de Cookies	50	AVISO	__wpdm_client: falta SameSite; cookiesession1: f...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

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: 2026-11-14T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-04-30T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

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

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

- ALTO

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO

X-Frame-Options
Falta — Protege contra clickjacking
- INFO

Strict-Transport-Security
Presente: max-age=31536000; includeSubDomains; preload
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://cel.gob.sv:443/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=31536000 (365 dias)
- INFO

Respuesta HTTPS
HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO

WordPress
Detectado via HTML body
- INFO

Joomla
No detectado
- INFO

Drupal
No detectado
- INFO

Magento
No detectado
- INFO

Shopify
No detectado
- INFO

PrestaShop
Detectado via HTML body
- INFO

Wix
No detectado
- INFO

Squarespace
No detectado
- BAJO

Meta generator
Expone: WordPress 6.8.10
- INFO

Tecnologias detectadas
Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.8.10 expuesta, WordPress 2 expuesta

- ALTO

WordPress version
Version 6.8.10 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)

Seguridad de Cookies — 50/100

Estado: AVISO

__wpdm_client: falta SameSite; cookiesession1: falta Secure; cookiesession1: falta SameSite

- INFO

Cookies detectadas
2 cookie(s) encontrada(s)
- INFO

Cookie: __wpdm_client — HttpOnly
HttpOnly activo — No accesible via JavaScript
- INFO

Cookie: __wpdm_client — Secure
Flag Secure activo — Solo se envia por HTTPS
- MEDIO

Cookie: __wpdm_client — SameSite
Falta SameSite — Vulnerable a CSRF
- INFO

Cookie: cookiesession1 — HttpOnly
HttpOnly activo — No accesible via JavaScript
- ALTO

Cookie: cookiesession1 — Secure
Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO

Cookie: cookiesession1 — SameSite
Falta SameSite — Vulnerable a CSRF

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

- BAJO

sitemap.xml
No encontrado (HTTP 404)
- 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] Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.

[HIGH] X-Frame-Options: Al no estar presente, el sitio web permite ser cargado en marcos externos, facilitando ataques de clickjacking.

[HIGH] WordPress version: La versión 6.8.10 se encuentra expuesta públicamente, permitiendo a posibles atacantes identificar vulnerabilidades específicas para ese motor.

[HIGH] Cookie: cookiesession1 - Secure: Esta cookie carece del flag de seguridad, lo que permite su transmisión a través de conexiones HTTP no cifradas.

[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos no autorizados.

[MEDIUM] Referrer-Policy: No se han definido controles sobre la información de referencia enviada a otros dominios, lo que compromete la privacidad del usuario.

[MEDIUM] Archivo /readme.html: Este archivo es accesible de forma pública y suele revelar detalles técnicos internos del sistema de gestión de contenidos.

[MEDIUM] Cookie: __wpdm_client - SameSite: La falta de este atributo hace que la cookie sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).

[MEDIUM] Cookie: cookiesession1 - SameSite: La ausencia de la política SameSite incrementa el riesgo de acciones no autorizadas mediante CSRF.

[LOW] Server header expuesto: El servidor revela el uso de Apache, proporcionando pistas sobre la infraestructura tecnológica subyacente.

[LOW] Meta generator: Se detectó la etiqueta que expone la versión exacta de WordPress utilizada por el portal.

[LOW] sitemap.xml: No se encontró el archivo de mapa del sitio, lo que dificulta la auditoría de estructura y el indexado correcto.