EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://fepade.org.sv	Checks	9 pruebas
Dominio	fepade.org.sv	Hallazgos	43 totales
Fecha	21 de abril de 2026 a las 16:09	Problemas	11 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El portal fepade.org.sv ha obtenido una puntuación de seguridad de 72/100, lo que representa una nota C en nuestra auditoría. Este resultado se deriva de la ejecución de 9 checks pasivos, de los cuales 5 fueron exitosos, 2 generaron advertencias y 1 se registró como fallo debido a un tiempo de espera agotado. Aunque el cifrado de datos básico está presente, se detectaron deficiencias críticas en la configuración de las cabeceras de seguridad y la exposición de puertos de red innecesarios. En su estado actual, el sitio se considera vulnerable a ataques de intermediario y secuestro de clics debido a la falta de políticas de protección modernas.

Resumen de Riesgos

0	5	3	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 57 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 57 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  57 dias restantes (expira: 2026-06-18T01:26:38.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-20T01:26:39.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, 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
- 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://fepade.org.sv/
- 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, 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: Site Kit by Google 1.176.0
- INFO **Tecnologias detectadas**
  Next.js

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (472 bytes)
- INFO **Reglas robots.txt**
  7 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://fepade.org.sv/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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 permite ataques de scripts cruzados (XSS) y la inyección de contenido malicioso en el navegador del usuario.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar a los visitantes.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el servidor obligue al navegador a usar siempre conexiones cifradas, facilitando ataques de degradación de SSL.
[HIGH] Puerto 21 (FTP): Este puerto está abierto y es peligroso porque transmite credenciales y archivos en texto plano, sin ningún tipo de cifrado.
[MEDIUM] X-Content-Type-Options: La falta de esta configuración permite que los navegadores intenten adivinar el tipo de contenido, lo que puede ser aprovechado para ejecutar archivos maliciosos disfrazados de imágenes.
[MEDIUM] Referrer-Policy: No se controla la información de navegación que se envía a otros sitios web externos, lo que podría filtrar rutas internas.
[MEDIUM] Puerto 22 (SSH): La exposición de este puerto de administración remota aumenta la superficie de ataque, permitiendo intentos de acceso por fuerza bruta.
[LOW] Server header expuesto: El servidor revela el nombre de la tecnología (Apache), proporcionando información valiosa para que un atacante busque vulnerabilidades específicas de esa versión.
[LOW] Meta generator: Se exponen detalles de la versión de plugins como Site Kit by Google, lo que facilita el reconocimiento de la arquitectura interna del sitio.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a directorios como admin, orientando a posibles atacantes hacia áreas administrativas que deberían permanecer ocultas.