EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://web.archive.org/	Checks	9 pruebas
Dominio	web.archive.org	Hallazgos	42 totales
Fecha	20 de mayo de 2026 a las 21:41	Problemas	9 detectados

C

66/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada a web.archive.org arroja una puntuación de 66/100, lo que corresponde a una calificación de grado C. El análisis se basó exclusivamente en 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos críticos. Aunque el sitio posee un cifrado de transporte válido, carece de protecciones esenciales contra ataques comunes de la web moderna. Debido a la falta de cabeceras de seguridad y errores en la redirección de tráfico, se concluye que el sitio es actualmente vulnerable.

Resumen de Riesgos

0	5	2	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 265 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 265 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  265 dias restantes (expira: 2027-02-09T22:02:42.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-08T22:02:42.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: nginx — 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
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- INFO **Permissions-Policy**
  Presente: interest-cohort=()

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
- INFO **Tecnologias detectadas**
  React

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
- INFO **Archivo /README.txt**
  No accesible (correcto)
- 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

- BAJO **robots.txt**
  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: Falta — La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options: Falta — El sitio es susceptible a ataques de clickjacking al no restringir cómo se muestra la página en marcos o iframes.
[HIGH] Strict-Transport-Security: Falta — No se obliga al navegador a usar conexiones cifradas, facilitando ataques de degradación de SSL.
[HIGH] Redirección HTTP a HTTPS: No ejecutada — El servidor permite conexiones inseguras a través del puerto 80 sin redirigir automáticamente al puerto seguro 443.
[MEDIUM] X-Content-Type-Options: Falta — El navegador podría intentar adivinar el tipo de contenido, lo que permite ataques de MIME-sniffing.
[MEDIUM] Archivo /readme.html accesible: Este archivo se encuentra expuesto públicamente y puede revelar detalles técnicos internos del sistema.
[LOW] Cabecera de servidor expuesta: Se detectó el valor "Server: nginx", lo que facilita a un atacante identificar la tecnología y buscar exploits específicos.
[LOW] Ausencia de archivos de indexación: No se encontraron los archivos robots.txt ni sitemap.xml, lo que impide un control adecuado sobre el rastreo del sitio.