

Escanear Vulnerabilidades

Informe de Seguridad Web

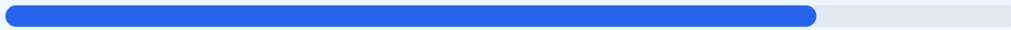
URL https://elisdecodetalles.eu
Dominio elisdecodetalles.eu
Fecha 10 de julio de 2026 a las 05:00

Checks 9 pruebas
Hallazgos 44 totales
Problemas 8 detectados

B

80/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 80/100 con una calificación de nota B. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 7 resultaron satisfactorias y 2 presentaron fallos críticos en la configuración de cabeceras y archivos de indexación. Al no haberse realizado un pentest activo, el análisis se centra en la superficie de exposición pública y la robustez de la infraestructura actual. Aunque la base de cifrado es sólida, la ausencia de políticas de seguridad en el servidor clasifica al sitio como vulnerable ante ataques de inyección y suplantación. El estado general es aceptable, pero requiere correcciones inmediatas en la configuración del servidor para alcanzar un nivel de protección profesional.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 88 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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 88 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
88 dias restantes (expira: 2026-10-06T14:02:40.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-07-08T14:02:41.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

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

- BAJO **Server header expuesto**
Server: Netlify — 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
- **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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redireccion**
HTTP 301 redirige a <https://elisdecodetalles.eu/>
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000
- **BAJO** **HSTS includeSubDomains**
HSTS no 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

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

- **INFO** **Archivo /readme.html**
No accesible (correcto)
- **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 **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 permite la ejecución de scripts maliciosos y ataques XSS al no restringir el origen del contenido.

[HIGH] X-Frame-Options: Al faltar esta directiva, el sitio es susceptible a ataques de clickjacking, donde un atacante puede cargar la web en un marco invisible para engañar al usuario.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, lo que facilita ataques de sniffing de MIME-type.

[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación enviada a otros sitios, lo que podría exponer rutas internas o datos sensibles en las URLs.

[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs críticas del navegador como la cámara, el micrófono o la geolocalización, aumentando el riesgo de privacidad.

[LOW] Server header expuesto: El servidor revela el uso de la tecnología Netlify, lo que ayuda a posibles atacantes a perfilar la infraestructura y buscar vulnerabilidades específicas.

[LOW] Ausencia de robots.txt y sitemap.xml: El servidor responde con errores 404 para estos archivos, lo que dificulta la indexación correcta y el control de acceso para rastreadores web.