EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ieselrincon.es	Checks	9 pruebas
Dominio	ieselrincon.es	Hallazgos	47 totales
Fecha	15 de septiembre de 2026 a las 18:00	Problemas	15 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio ieselrincon.es ha arrojado una puntuación de 57/100, lo que equivale a una calificacion de grado D. De los 9 checks pasivos ejecutados, solo 3 resultaron satisfactorios, mientras que se identificaron 4 advertencias y 2 fallos criticos de seguridad. Los problemas principales radican en la exposicion de versiones desactualizadas del CMS y una ausencia total de cabeceras de proteccion en el servidor. Debido a estas deficiencias tecnicas, se concluye que el sitio es actualmente vulnerable a diversos vectores de ataque conocidos.

Resumen de Riesgos

0	5	6	4	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 17 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 7.1 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 17 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  17 dias restantes (expira: 2026-10-02T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-18T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-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
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://ieselrincon.es/
- 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 7.1
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.1 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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www3.gobiernodecanarias.org/medusa/eforma/campus/

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (67 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- 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: Falta esta cabecera esencial para prevenir ataques de inyeccion de codigo y XSS.
[HIGH] X-Frame-Options: La ausencia de esta proteccion permite que el sitio sea cargado en iframes, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no fuerza conexiones seguras de forma automatica.
[HIGH] WordPress version: Se expone publicamente el uso de la version 7.1, permitiendo a atacantes buscar vulnerabilidades especificas para ese motor.
[MEDIUM] X-Content-Type-Options: Falta la cabecera que evita que el navegador realice MIME-type sniffing, lo que puede derivar en ejecucion de scripts.
[MEDIUM] Referrer-Policy: No se controla la informacion de navegacion que se envia a otros sitios web mediante el referer.
[MEDIUM] Permissions-Policy: No hay restricciones sobre el uso de APIs del navegador como la camara, el microfono o la geolocalizacion.
[MEDIUM] Archivo /readme.html: El archivo de instalacion es accesible publicamente y revela informacion tecnica innecesaria del CMS.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario en internet.
[MEDIUM] Contenido Mixto: Se detecto un recurso cargado mediante HTTP inseguro dentro de la pagina protegida por HTTPS.
[LOW] Server header expuesto: La cabecera revela que se utiliza el servidor Apache, facilitando el reconocimiento del entorno.
[LOW] Meta generator: La etiqueta meta del codigo fuente confirma la version exacta de WordPress utilizada.
[LOW] Ruta sensible en robots.txt: Se menciona la ruta admin en el archivo de indexacion, guiando a posibles atacantes a zonas sensibles.
[LOW] sitemap.xml: El archivo no fue localizado, lo que indica una falta de estructura de indexacion estandar.