EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ih.csic.es/es	Checks	9 pruebas
Dominio	ih.csic.es	Hallazgos	47 totales
Fecha	18 de mayo de 2026 a las 08:22	Problemas	10 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio ih.csic.es/es ha resultado en una puntuación de 80/100, otorgando una calificación de grado B. De los 9 checks pasivos ejecutados, 6 se completaron con éxito, 2 presentaron advertencias de riesgo bajo y 1 falló debido a carencias en la configuración del servidor. El portal demuestra una gestión correcta del cifrado de datos mediante certificados actualizados, pero presenta debilidades en la protección contra ataques de inyección de código. En su estado actual, el sitio se considera mayormente seguro para el usuario final, aunque vulnerable ante ataques técnicos dirigidos que aprovechen la falta de cabeceras de seguridad modernas.

Resumen de Riesgos

0	3	2	5	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 130 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: Drupal, PrestaShop
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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 130 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  130 dias restantes (expira: 2026-09-25T10:00:13.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-25T10:00:13.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache/2.4.38 (Debian) — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://ih.csic.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: Drupal, PrestaShop

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  Detectado via HTML body
- 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: Drupal 9 (https://www.drupal.org)
- INFO **Tecnologias detectadas**
  Next.js

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1706 bytes)
- INFO **Reglas robots.txt**
  26 Disallow, 18 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — 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] Falta de Content-Security-Policy: La ausencia de esta cabecera permite que el sitio sea susceptible a ataques de Cross-Site Scripting (XSS) y secuestro de clics.
[HIGH] Ausencia de Strict-Transport-Security: No se obliga a los navegadores a conectar exclusivamente vía HTTPS, permitiendo ataques de interceptación de tráfico o downgrade.
[MEDIUM] Falta de Referrer-Policy: El sitio no controla qué información de navegación se envía a terceros cuando se hace clic en enlaces externos.
[MEDIUM] Ausencia de Permissions-Policy: No existen restricciones sobre qué APIs del navegador (como geolocalización o cámara) pueden ser invocadas por scripts alojados.
[LOW] Exposición de cabecera Server: Se revela la versión exacta del servidor Apache/2.4.38 y el sistema operativo Debian, facilitando la búsqueda de vulnerabilidades específicas.
[LOW] Meta generator expuesto: El código fuente revela el uso de Drupal 9, lo que reduce el tiempo de reconocimiento para un atacante potencial.
[LOW] Rutas sensibles en robots.txt: Se listan directorios como admin y config, lo que expone puntos de entrada administrativos a herramientas de escaneo automatizado.
[LOW] Falta de sitemap.xml: La ausencia de este archivo dificulta la auditoría de la estructura completa del sitio y la indexación correcta de contenidos.