

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://info.realoviedo.es
Dominio info.realoviedo.es
Fecha 10 de junio de 2026 a las 09:57

Checks 9 pruebas
Hallazgos 44 totales
Problemas 7 detectados

B

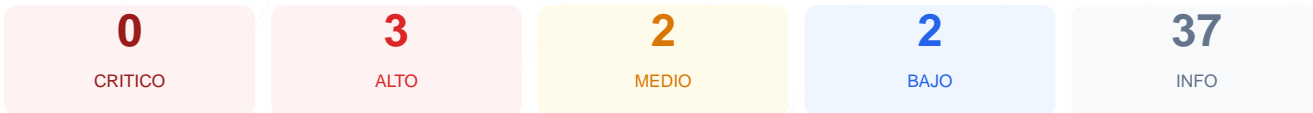
75/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el sitio web arroja una puntuación de 75/100, lo que equivale a una nota B. Se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue calificado como fallo. Los hallazgos principales revelan deficiencias críticas en la redirección de tráfico seguro y en la implementación de políticas de transporte estricto. Aunque el cifrado base es correcto, la configuración del servidor web presenta riesgos de exposición de infraestructura. En conclusión, el sitio se considera moderadamente seguro, pero es vulnerable a ataques de intermediario y posee una superficie de ataque innecesariamente ampliada.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 76 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 76 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
76 dias restantes (expira: 2026-08-25T11:01:04.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-05-27T10:01:15.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

- BAJO **Server header expuesto**
Server: cloudflare — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
Presente: default-src 'none'; script-src 'nonce-BUChCRBQIbYdkTAATdsGu5' 'unsafe-eval' http...
- INFO **X-Frame-Options**
Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
Presente: nosniiff
- INFO **Referrer-Policy**
Presente: same-origin
- INFO **Permissions-Policy**
Presente: accelerometer=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),g...

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
HTTP 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
HTTPS responde con status 403

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
Presente (1738 bytes)
- INFO **Reglas robots.txt**
9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
No encontrado (HTTP 403)
- BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[ALTA] Redirección HTTPS inexistente: El sitio no redirige el tráfico HTTP hacia HTTPS, respondiendo con un error 403 en lugar de forzar una conexión segura.

[ALTA] Falta de Strict-Transport-Security: La ausencia de la cabecera HSTS impide que el navegador fuerce conexiones cifradas, facilitando ataques de degradación de protocolo.

[MEDIA] Puerto 8080 (HTTP-Alt) abierto: La presencia de este puerto alternativo expone un posible servidor proxy o servicio administrativo que no debería ser accesible públicamente.

[MEDIA] Bloqueo total en robots.txt: El archivo configurado con Disallow: / impide el rastreo legítimo y sugiere una configuración restrictiva que podría estar ocultando endpoints sin protección adicional.

[BAJA] Cabecera Server expuesta: El servidor revela el uso de Cloudflare, proporcionando información técnica a potenciales atacantes sobre la infraestructura de red.

[BAJA] Falta de sitemap.xml: No se encontró el mapa del sitio (HTTP 403), lo que dificulta la auditoría de rutas y la indexación controlada del contenido.