

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://crece.uca.es
Dominio crece.uca.es
Fecha 21 de mayo de 2026 a las 09:24

Checks 9 pruebas
Hallazgos 44 totales
Problemas 5 detectados

A

91/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad del sitio web ha dado como resultado una puntuación de 91/100, lo que otorga una nota de A. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios, 1 presentó advertencias y 1 fue calificado como fallo. El portal demuestra una implementación sólida en términos de cifrado y protocolos de transporte seguro, aunque carece de ciertas configuraciones de endurecimiento en sus cabeceras. En conclusión, crece.uca.es es un sitio seguro que requiere ajustes técnicos menores para alcanzar la excelencia en su postura de seguridad.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 197 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
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 197 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
197 dias restantes (expira: 2026-12-04T11:56:19.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-05-19T11:56:20.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
Presente: default-src Cache-Control Content-Location http: https: data: 'unsafe-inline' 'u...
- INFO **X-Frame-Options**
Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
Presente: max-age=31500000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
Presente: nosniiff
- 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 302 redirige a https://crece.uca.es
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31500000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
HSTS cubre subdominios
- INFO **HSTS max-age**
max-age=31500000 (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

[MEDIUM] Falta de cabecera Referrer-Policy: La ausencia de esta directiva impide controlar la cantidad de información que el navegador envía al seguir enlaces hacia otros sitios.
[MEDIUM] Falta de cabecera Permissions-Policy: No se están restringiendo de forma explícita las capacidades del navegador, como el acceso a la cámara o micrófono, lo que aumenta la superficie de riesgo.

[LOW] Cabecera de servidor expuesta: El sistema revela que utiliza Apache, información que puede ser aprovechada por atacantes para buscar vulnerabilidades específicas de esa versión o software.

[LOW] Ausencia de archivo robots.txt: No se ha encontrado este fichero, lo que dificulta la gestión del comportamiento de los rastreadores y la protección de rutas que no deberían ser indexadas.

[LOW] Ausencia de archivo sitemap.xml: El sitio carece de un mapa estructurado, lo que afecta negativamente al rastreo técnico y a la organización de la información pública.