EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.uci.es	Checks	9 pruebas
Dominio	www.uci.es	Hallazgos	65 totales
Fecha	25 de mayo de 2026 a las 14:49	Problemas	6 detectados

A

93/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de ciberseguridad realizado al sitio web ha arrojado una puntuacion de 93/100, lo que otorga una calificacion final de grado A. Durante el proceso se ejecutaron 9 comprobaciones pasivas, obteniendo 7 resultados satisfactorios y 2 advertencias, sin registrarse fallos criticos. Aunque la infraestructura base es solida y cumple con los estandares de cifrado, existen omisiones en las cabeceras de seguridad y en la configuracion de cookies de sesion. Se concluye que el sitio es mayoritariamente seguro, aunque presenta vulnerabilidades de severidad alta y media que deben ser mitigadas para evitar ataques de inyeccion.

Resumen de Riesgos

0	3	1	2	59
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 250 dias
Cabeceras de Seguridad	75	AVISO	5/6 presentes. Faltan: Content-Security-Policy
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	83	AVISO	ucies#lang: falta HttpOnly; shell#lang: falta Ht...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 250 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  250 dias restantes (expira: 2027-01-30T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-06T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-Policy

- BAJO **Server header expuesto**
  Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(self)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.uci.es/
- 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
- 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 — 83/100

Estado: AVISO

ucies#lang: falta HttpOnly; shell#lang: falta HttpOnly; ARRAffinity: falta SameSite

- INFO **Cookies detectadas**
  6 cookie(s) encontrada(s)
- ALTO **Cookie: ucies#lang — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: ucies#lang — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ucies#lang — SameSite**
  SameSite=none
- ALTO **Cookie: shell#lang — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: shell#lang — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: shell#lang — SameSite**
  SameSite=none
- INFO **Cookie: ASP.NET_SessionId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ASP.NET_SessionId — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ASP.NET_SessionId — SameSite**
  SameSite=none
- INFO **Cookie: SC_ANALYTICS_GLOBAL_COOKIE — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: SC_ANALYTICS_GLOBAL_COOKIE — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: SC_ANALYTICS_GLOBAL_COOKIE — SameSite**
  SameSite=none
- INFO **Cookie: ARRAffinity — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ARRAffinity — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ARRAffinity — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: ARRAffinitySameSite — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ARRAffinitySameSite — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ARRAffinitySameSite — SameSite**
  SameSite=none

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (516 bytes)

- INFO **Reglas robots.txt**
  16 Disallow, 2 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://uci.es/sitemap_index.xml/
- 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 ejecucion de ataques XSS y la inyeccion de contenido malicioso al no restringir las fuentes de scripts.
[HIGH] Cookies sin atributo HttpOnly: Las cookies ucies#lang y shell#lang carecen de esta proteccion, permitiendo que sean accesibles mediante scripts de navegador, lo que facilita el robo de sesiones.
[MEDIUM] Cookie sin atributo SameSite: La cookie ARRAffinity no implementa esta politica, dejando el sitio expuesto a posibles ataques de falsificacion de peticiones en sitios cruzados (CSRF).
[LOW] Server header expuesto: La cabecera revela el uso de Microsoft-IIS/10.0, informacion que un atacante puede utilizar para buscar vulnerabilidades especificas de esa version de software.
[LOW] Ruta sensible en robots.txt: El archivo incluye una referencia al directorio config, lo cual podria guiar a usuarios malintencionados hacia rutas que deberian ser privadas.