EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.uchceu.es/universidad-castellon	Checks	9 pruebas
Dominio	www.uchceu.es	Hallazgos	49 totales
Fecha	1 de julio de 2026 a las 12:31	Problemas	10 detectados

B

83/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre la plataforma arroja una puntuación de 83/100, lo que otorga una calificación de grado B. Se han ejecutado un total de 9 verificaciones pasivas, de las cuales 7 resultaron satisfactorias, se registró 1 advertencia por puertos abiertos y 1 fallo crítico relacionado con la ausencia de cabeceras de seguridad. El cifrado de datos es robusto y las redirecciones HTTPS funcionan correctamente, pero existen deficiencias importantes en la configuración de políticas del navegador. En conclusión, el sitio se considera generalmente seguro para el usuario, aunque presenta vulnerabilidades de configuración que deben corregirse para prevenir ataques de inyección y secuestro de clics.

Resumen de Riesgos

0	2	5	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 87 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 87 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  87 dias restantes (expira: 2026-09-26T11:20:10.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-28T10:20:12.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=2592000; includeSubDomains
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.uchceu.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=2592000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- MEDIO **HSTS max-age**
  max-age=2592000 (30 dias) — Recomendado minimo 180 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, Astro, ASP.NET

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (4433 bytes)
- INFO **Reglas robots.txt**
  63 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.uchceu.es/sitemap_index.xml
- 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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) y otras inyecciones de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a ataques de clickjacking, donde un atacante puede engañar al usuario para que realice acciones no deseadas dentro de un marco invisible.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo aumenta la superficie de ataque al revelar servicios que podrían no estar debidamente protegidos.
[MEDIUM] HSTS max-age insuficiente: El tiempo de persistencia de la política de seguridad de transporte es de solo 30 días, por debajo del estándar recomendado de 180 días.
[MEDIUM] Referrer-Policy: No se detectó esta cabecera, lo que puede provocar la fuga de información sensible en las URLs de referencia hacia sitios externos.
[MEDIUM] Permissions-Policy: La falta de esta política permite que el navegador acceda a APIs potencialmente sensibles sin restricciones explícitas.
[MEDIUM] Robots.txt con rutas sensibles: El archivo revela la ubicación de directorios como "admin", proporcionando información valiosa a posibles atacantes sobre la estructura del sitio.
[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, lo que facilita las labores de reconocimiento tecnológico para un atacante.
[LOW] X-Powered-By expuesto: Se detectó la cabecera ASP.NET, informando directamente sobre el framework utilizado y permitiendo la búsqueda de vulnerabilidades específicas para dicha tecnología.