

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://familia.edu.gva.es
Dominio familia.edu.gva.es
Fecha 7 de octubre de 2026 a las 23:49

Checks 9 pruebas
Hallazgos 50 totales
Problemas 9 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el portal web ha resultado en una puntuación de 85/100 con una calificación de B. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 7 finalizaron con éxito y 2 registraron fallos de configuración en las cabeceras y archivos de indexación. Aunque el cifrado de datos es excelente, la ausencia de cabeceras de protección específicas y la visibilidad de archivos internos representan riesgos moderados. En conclusión, el sitio web presenta un estado de seguridad aceptable, pero se considera vulnerable frente a ataques de suplantación de interfaz y reconocimiento de sistema.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 138 dias
Cabeceras de Seguridad	45	FALLO	Solo 2/6 presentes. Faltan: X-Frame-Options, X-C...
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	2 cookies, todas con flags correctos
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	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 138 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
138 dias restantes (expira: 2027-02-22T12:52:25.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-07T12:52:26.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

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

- INFO Content-Security-Policy
Presente: upgrade-insecure-requests; frame-ancestors 'self' https://*.edu.gva.es/; connect...

- ALTO

X-Frame-Options
Falta — Protege contra clickjacking
- INFO

Strict-Transport-Security
Presente: max-age=157680000; includeSubDomains
- MEDIO

X-Content-Type-Options
Falta — Evita MIME-type sniffing
- 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 307 redirige a https://familia.edu.gva.es/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=157680000; includeSubDomains
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=157680000 (1825 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

- MEDIO

Archivo /readme.html
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Archivo /README.txt
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Ruta /wp-login.php
Panel de login accesible publicamente
- MEDIO

Ruta /administrator/
Panel de login accesible publicamente

- MEDIO

Ruta /user/login
Panel de login accesible publicamente
- INFO

Version CMS
No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

2 cookies, todas con flags correctos

- INFO

Cookies detectadas
2 cookie(s) encontrada(s)
- INFO

Cookie: JSESSIONID — HttpOnly
HttpOnly activo — No accesible via JavaScript
- INFO

Cookie: JSESSIONID — Secure
Flag Secure activo — Solo se envia por HTTPS
- INFO

Cookie: JSESSIONID — SameSite
SameSite=none
- INFO

Cookie: NSC_mc2_fev_kcptt_2_jubdb_7101 — HttpOnly
HttpOnly activo — No accesible via JavaScript
- INFO

Cookie: NSC_mc2_fev_kcptt_2_jubdb_7101 — Secure
Flag Secure activo — Solo se envia por HTTPS
- INFO

Cookie: NSC_mc2_fev_kcptt_2_jubdb_7101 — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO

security.txt
Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)
Cerrado — Servidor web
- INFO

Puerto 443 (HTTPS)
Cerrado — 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] Ausencia de X-Frame-Options: La falta de esta cabecera permite que el sitio sea cargado en marcos o iframes, facilitando ataques de clickjacking.
- [MEDIUM] Ausencia de X-Content-Type-Options: No se previene el MIME-type sniffing, lo que podría permitir al navegador ejecutar archivos con interpretaciones incorrectas de su contenido.
- [MEDIUM] Ausencia de Referrer-Policy: El sitio no controla qué información de procedencia se envía a terceros cuando un usuario hace clic en un enlace externo.
- [MEDIUM] Ausencia de Permissions-Policy: No se definen restricciones para el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.
- [MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente y pueden revelar detalles técnicos del sistema subyacente.
- [MEDIUM] Paneles de acceso expuestos: Las rutas /wp-login.php, /administrator/ y /user/login son visibles, lo que facilita intentos de intrusión por fuerza bruta.
- [FAIL] Ausencia de archivos de rastreo: No se detectaron robots.txt ni sitemap.xml, lo que impide una gestión controlada del contenido indexable por buscadores.