EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://educacionadistancia.juntadeandalucia.es/centros/malaga/m/	Checks	9 pruebas
Dominio	educacionadistancia.juntadeandalucia.es	Hallazgos	54 totales
Fecha	25 de septiembre de 2026 a las 17:00	Problemas	17 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el activo arroja una puntuación de 62/100, lo que se traduce en una nota C. La evaluación se basó en 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 2 generaron advertencias y 3 fallaron de forma crítica. Se han detectado deficiencias estructurales en las políticas de seguridad del servidor y en la configuración de las cookies de sesión. Por lo tanto, se concluye que el sitio es vulnerable ante ataques de interceptación de datos y suplantación de identidad.

Resumen de Riesgos

0	8	7	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 72 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	42	FALLO	BIGipServermoodle-php8: falta SameSite; TS01d584...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
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 72 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  72 dias restantes (expira: 2026-12-06T07:55:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-21T07:55:30.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://educacionadistancia.juntadeandalucia.es/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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 — 42/100

Estado: FALLO

BIGipServermoodle-php8: falta SameSite; TS01d5846c: falta HttpOnly; TS01d5846c: falta Secure; TS01d5846c: falta SameSite; TS01b09f1b: falta HttpOnly; TS01b09f1b: falta Secure; TS01b09f1b: falta SameSite

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- INFO **Cookie: MoodleSessionprocenmal26 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: MoodleSessionprocenmal26 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: MoodleSessionprocenmal26 — SameSite**
  SameSite=lax
- INFO **Cookie: BIGipServermoodle-php8 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: BIGipServermoodle-php8 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: BIGipServermoodle-php8 — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: TS01d5846c — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: TS01d5846c — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: TS01d5846c — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: TS01b09f1b — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: TS01b09f1b — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: TS01b09f1b — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://agrega.juntadeandalucia.es/repositorio/09122020/98/es...

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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options: La falta de esta directiva expone el sitio a ataques de clickjacking, permitiendo que la interfaz sea embebida en marcos maliciosos.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, facilitando ataques de degradación de SSL y Man-in-the-Middle.
[HIGH] Cookies TS01d5846c y TS01b09f1b sin flag HttpOnly: Estas cookies de sesión son accesibles mediante scripts de cliente, aumentando el riesgo de robo de identidad.
[HIGH] Cookies TS01d5846c y TS01b09f1b sin flag Secure: Al no estar marcadas como seguras, estas cookies podrían transmitirse a través de conexiones HTTP no cifradas.
[MEDIUM] Cookie BIGipServermoodle-php8 sin flag SameSite: La falta de este atributo hace que el sitio sea susceptible a ataques de falsificación de solicitudes entre sitios o CSRF.
[MEDIUM] Contenido Mixto: Se ha detectado un recurso de hoja de estilo cargado vía HTTP, lo que compromete la integridad de la conexión cifrada.
[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite el sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy y Permissions-Policy: La falta de estas cabeceras impide controlar la información enviada en el referer y restringir el acceso a APIs sensibles del navegador.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor responde con errores 404 para estos archivos, dificultando la gestión de la indexación por motores de búsqueda.