EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://centros.edu.xunta.gal/cifprodolfouchapineiro/aulavirtual/my/	Checks	9 pruebas
Dominio	centros.edu.xunta.gal	Hallazgos	53 totales
Fecha	24 de septiembre de 2026 a las 14:01	Problemas	16 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el portal ha dado como resultado una puntuación de 70/100, lo que equivale a una nota de C. Durante este análisis se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 presentó advertencias y 3 fallaron debido a configuraciones de seguridad ausentes. Aunque el cifrado de datos es robusto, existen deficiencias críticas en la protección de las sesiones de usuario y en la implementación de cabeceras de respuesta del servidor. Se han detectado riesgos de interceptación y manipulación de datos debido a la falta de políticas de transporte estricto y seguridad de contenido. En conclusión, el sitio es actualmente vulnerable ante ataques de secuestro de sesión e inyección, requiriendo intervenciones técnicas inmediatas para alcanzar un nivel de seguridad profesional.

Resumen de Riesgos

0	9	3	4	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 156 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 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	22	FALLO	MoodleSessioncifprodolfouchapineiro: falta HttpO...
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 156 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  156 dias restantes (expira: 2027-02-27T10:16:16.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-26T10:16:17.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.33 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: sameorigin
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://centros.edu.xunta.gal/
- 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**
  PHP/8.3.33

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 — 22/100

Estado: FALLO

MoodleSessioncifprodolfouchapineiro: falta HttpOnly; MoodleSessioncifprodolfouchapineiro: falta Secure; MoodleSessioncifprodolfouchapineiro: falta HttpOnly; MoodleSessioncifprodolfouchapineiro: falta Secure; ROUTEID: falta HttpOnly; ROUTEID: falta Secure; ROUTEID: falta SameSite

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: MoodleSessioncifprodolfouchapineiro — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: MoodleSessioncifprodolfouchapineiro — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: MoodleSessioncifprodolfouchapineiro — SameSite**
  SameSite=lax
- ALTO **Cookie: MoodleSessioncifprodolfouchapineiro — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: MoodleSessioncifprodolfouchapineiro — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: MoodleSessioncifprodolfouchapineiro — SameSite**
  SameSite=lax
- ALTO **Cookie: ROUTEID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ROUTEID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ROUTEID — SameSite**
  Falta SameSite — Vulnerable a CSRF

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

[HIGH] Falta de Content-Security-Policy: No se detectó esta cabecera, lo que deja al sitio expuesto a ataques de inyección de scripts y Cross-Site Scripting (XSS).
[HIGH] Falta de Strict-Transport-Security: La ausencia de HSTS permite que atacantes puedan forzar la degradación de la conexión a HTTP no cifrado mediante ataques Man-in-the-Middle.
[HIGH] Cookie MoodleSessioncifprodolfouchapineiro sin flag HttpOnly: La cookie de sesión es accesible mediante JavaScript, facilitando el robo de la identidad del usuario en caso de vulnerabilidad XSS.
[HIGH] Cookie MoodleSessioncifprodolfouchapineiro sin flag Secure: El identificador de sesión puede ser transmitido a través de conexiones no cifradas, permitiendo su captura por terceros.
[HIGH] Cookie ROUTEID sin flag HttpOnly: Al igual que la de sesión, esta cookie de infraestructura carece de protección contra acceso programático malicioso.
[HIGH] Cookie ROUTEID sin flag Secure: Esta cookie se envía en texto plano si existe una degradación de la conexión, exponiendo la arquitectura interna.
[MEDIUM] Cookie ROUTEID sin flag SameSite: La ausencia de esta directiva hace que el navegador sea vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Falta de Referrer-Policy: El servidor no controla qué información de procedencia se envía a enlaces externos, pudiendo filtrar rutas internas de la plataforma.
[MEDIUM] Falta de Permissions-Policy: No se han restringido las APIs del navegador, permitiendo potencialmente que scripts de terceros soliciten acceso a hardware como la cámara o el micrófono.
[LOW] Cabecera Server expuesta: El servidor revela que utiliza Apache, información que ayuda a un atacante a buscar vulnerabilidades específicas para dicho software.
[LOW] Cabecera X-Powered-By expuesta: Se detectó el uso de PHP/8.3.33, revelando la tecnología exacta del backend y facilitando la creación de exploits a medida.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor responde con errores 404 para estos archivos, lo que indica una falta de gestión en el rastreo y organización pública del sitio.