EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ioc.xtec.cat/educacio/	Checks	9 pruebas
Dominio	ioc.xtec.cat	Hallazgos	42 totales
Fecha	28 de mayo de 2026 a las 15:25	Problemas	13 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el sitio web ha arrojado una puntuación de 60/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 4 resultados satisfactorios, 2 advertencias y 3 fallos críticos en la configuración. Aunque el sitio cuenta con un cifrado SSL robusto, presenta carencias severas en la implementación de cabeceras de seguridad y en la protección de la información del servidor. Se concluye que el sitio es actualmente vulnerable a ataques de clickjacking e inyección de contenido debido a la falta de políticas de seguridad modernas. Se requiere una intervención técnica para mitigar los riesgos asociados a la exposición de versiones del CMS.

Resumen de Riesgos

0	5	6	2	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 231 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	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.8.3 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 231 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  231 dias restantes (expira: 2027-01-14T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-14T00:00:00.000Z
- 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

- BAJO **Server header expuesto**
  Server: Apache/2.4.58 (Ubuntu) — Revela tecnologia del servidor

- 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 301 redirige a https://ioc.xtec.cat:443/
- 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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.8.3
- INFO **Tecnologias detectadas**
  Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.8.3 expuesta

- ALTO **WordPress version**
  Version 6.8.3 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- 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

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

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

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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: Falta esta cabecera esencial, lo que facilita ataques de inyección de scripts y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado en iframes, exponiéndolo a ataques de clickjacking.
[HIGH] Strict-Transport-Security: No existe configuración HSTS, lo que impide forzar conexiones seguras y permite ataques de degradación de protocolo.
[HIGH] WordPress version: La versión 6.8.3 se encuentra expuesta públicamente, lo que facilita a atacantes la búsqueda de vulnerabilidades específicas conocidas.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, pudiendo derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la información enviada en las peticiones de origen, lo que puede comprometer la privacidad de la navegación.

[MEDIUM] Permissions-Policy: Ausencia de restricciones sobre el uso de APIs del navegador, como la cámara o el micrófono, por parte de terceros.
[MEDIUM] Archivos de información expuestos: Los archivos /readme.html y /README.txt son accesibles, revelando detalles técnicos innecesarios del CMS.
[MEDIUM] Puerto 22 (SSH) abierto: El puerto de acceso remoto está disponible, lo que aumenta la superficie de ataque para intentos de intrusión por fuerza bruta.
[LOW] Server header expuesto: El servidor revela el uso de Apache/2.4.58 (Ubuntu), facilitando la fase de reconocimiento de un atacante.
[LOW] Meta generator: La etiqueta meta expone la tecnología WordPress 6.8.3 directamente en el código fuente.