EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://terrassa.salesians.cat/	Checks	9 pruebas
Dominio	terrassa.salesians.cat	Hallazgos	53 totales
Fecha	9 de abril de 2026 a las 08:52	Problemas	18 detectados

D

52/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 52/100, lo que otorga una calificación global de grado D. Se realizaron 9 comprobaciones pasivas, resultando en 3 verificaciones correctas, 3 advertencias y 3 fallos críticos en la infraestructura. Los resultados demuestran una carencia absoluta de cabeceras de seguridad y la exposición de servicios obsoletos como FTP. La visibilidad de la versión del CMS y la presencia de contenido mixto comprometen la integridad de la plataforma. Por lo tanto, se concluye que el sitio es vulnerable y requiere medidas correctivas urgentes para proteger a sus usuarios.

Resumen de Riesgos

0	6	9	3	35
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, Wix
Version CMS Expuesta	20	FALLO	WordPress 6.9.4 expuesta
Seguridad de Cookies	67	AVISO	__wpdm_client: falta SameSite
Contenido Mixto	20	FALLO	10 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

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: 2026-11-25T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-10T00:00:00.000Z
- 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: nginx — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.30, PleskLin — Revela framework/lenguaje
- 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://terrassa.salesians.cat/
- 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, Wix

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  Detectado via HTML body
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.2.30, PleskLin

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)

- INFO **Archivo /README.txt**
  No accesible (correcto)

Seguridad de Cookies — 67/100

Estado: AVISO

__wpdm_client: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: __wpdm_client — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __wpdm_client — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __wpdm_client — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

10 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.youtube.com/user/SalesiansTerrassa/videos
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://salesiansterrassa.esemtia.net/moodle
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://edu.esemtia.com
- MEDIO **href (link/stylesheet)**
  ...y 7 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (3076 bytes)
- INFO **Reglas robots.txt**
  82 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **sitemap.xml**
  Presente, ? URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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] Versión de WordPress expuesta: La versión 6.9.4 es visible públicamente, lo que permite a atacantes buscar y aplicar exploits para vulnerabilidades conocidas.
[HIGH] Content-Security-Policy ausente: La falta de esta cabecera facilita ataques de inyección de contenido y scripts maliciosos (XSS).
[HIGH] X-Frame-Options ausente: La ausencia de protección contra marcos hace que el sitio sea vulnerable a ataques de clickjacking.
[HIGH] Strict-Transport-Security ausente: Al no configurar HSTS, el servidor no obliga al navegador a usar siempre conexiones seguras, permitiendo ataques de degradación.
[HIGH] Puerto 21 (FTP) abierto: El servicio de transferencia de archivos está accesible y transmite información sin cifrar, incluyendo posibles credenciales.
[MEDIUM] Contenido mixto detectado: Existen 10 recursos cargados mediante HTTP inseguro dentro de la página HTTPS, rompiendo la cadena de confianza del cifrado.
[MEDIUM] Cookie sin atributo SameSite: La cookie __wpdm_client carece de la directiva SameSite, lo que la hace susceptible a ataques de falsificación de solicitud en sitios cruzados (CSRF).
[MEDIUM] X-Content-Type-Options ausente: El navegador podría intentar adivinar el tipo de contenido, permitiendo la ejecución de archivos maliciosos disfrazados de otros formatos.
[MEDIUM] Referrer-Policy y Permissions-Policy ausentes: No se controla qué información de origen se envía a otros sitios ni se restringen las capacidades del navegador como la cámara o el micrófono.
[LOW] Cabecera Server expuesta: Se revela el uso de nginx, proporcionando información técnica valiosa para la fase de reconocimiento de un atacante.
[LOW] Cabecera X-Powered-By expuesta: Se expone el uso de PHP/8.2.30 y PleskLin, reduciendo el esfuerzo necesario para identificar vectores de ataque específicos.
[LOW] Etiqueta Meta generator expuesta: El código fuente confirma explícitamente el uso de WordPress 6.9.4, facilitando el perfilado del sistema.