EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://unizar.es	Checks	9 pruebas
Dominio	unizar.es	Hallazgos	51 totales
Fecha	13 de mayo de 2026 a las 11:55	Problemas	17 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio unizar.es ha resultado en una puntuación de 57/100, lo que equivale a una calificación de grado D. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales solo 4 resultaron satisfactorios, mientras que se identificaron 2 advertencias y 3 fallos críticos en la configuración del servidor. La ausencia de mecanismos de redirección segura y la falta de cabeceras de protección esenciales comprometen la integridad de la plataforma. Como conclusión, el sitio se clasifica actualmente como vulnerable ante ataques de interceptación de datos y explotación de vulnerabilidades web comunes.

Resumen de Riesgos

0	4	7	6	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 192 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	CMS detectado: Drupal, PrestaShop
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	101 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 192 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  192 dias restantes (expira: 2026-11-21T07:29:47.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-21T07:29:47.000Z
- 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: nginx/1.24.0 (Ubuntu) — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.30 — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 301 — No redirige a HTTPS
- 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: Drupal, PrestaShop

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  Detectado via HTML body
- 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: Drupal 10 (https://www.drupal.org)
- INFO **Tecnologias detectadas**
  PHP/8.2.30

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 — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 20/100

Estado: FALLO

101 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.unizar.es/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.unizar.es/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.unizar.es/
- MEDIO **href (link/stylesheet)**
  ...y 98 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (2027 bytes)
- INFO **Reglas robots.txt**
  34 Disallow, 18 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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] Ausencia de Redirección HTTPS: El servidor no redirige automáticamente las conexiones HTTP a HTTPS, permitiendo el tráfico de datos sin cifrar.
[HIGH] Falta de Strict-Transport-Security (HSTS): No se comunica al navegador la obligatoriedad de usar conexiones seguras, facilitando ataques de degradación de SSL.
[HIGH] Falta de Content-Security-Policy (CSP): El sitio carece de una política que prevenga ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[MEDIUM] Contenido Mixto Detectado: Se identificaron 101 recursos (hojas de estilo y enlaces) cargando por HTTP dentro de la página HTTPS, lo que debilita el cifrado.
[MEDIUM] Falta de Referrer-Policy: No existe control sobre la información de navegación que se comparte con terceros al hacer clic en enlaces externos.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la ubicación.
[MEDIUM] Puerto 22 (SSH) Abierto: La interfaz de administración remota es visible públicamente, lo que aumenta la superficie de ataque para intentos de intrusión.
[LOW] Exposición de Cabecera Server: El servidor revela el uso de nginx/1.24.0 (Ubuntu), proporcionando datos técnicos útiles para un atacante.
[LOW] Exposición de Cabecera X-Powered-By: Se muestra públicamente la versión PHP/8.2.30 utilizada por la aplicación.
[LOW] Meta generator expuesto: El código fuente confirma el uso de Drupal 10, exponiendo la tecnología base del sitio.
[LOW] Rutas sensibles en robots.txt: Se referencian directorios como admin y config, guiando involuntariamente a posibles atacantes hacia zonas restringidas.
[LOW] Ausencia de sitemap.xml: El archivo de mapa del sitio no fue localizado, lo que afecta la organización y auditoría de la estructura web.