EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://egaz.eus	Checks	9 pruebas
Dominio	egaz.eus	Hallazgos	46 totales
Fecha	22 de abril de 2026 a las 17:58	Problemas	16 detectados

D

56/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el dominio egaz.eus ha arrojado una puntuación de 56/100, lo que resulta en una nota de D. Se ejecutaron un total de 9 checks pasivos, de los cuales 4 resultaron correctos, 2 generaron advertencias y 3 finalizaron en fallo crítico. Los resultados muestran una infraestructura con graves carencias en la configuración de cabeceras de seguridad y una obsolescencia preocupante del sistema de gestión de contenidos. Debido a la exposición de puertos críticos y la falta de protecciones modernas, el sitio web se clasifica actualmente como vulnerable. Se requiere una intervención inmediata para mitigar los riesgos de explotación activa.

Resumen de Riesgos

1	6	7	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 233 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
Version CMS Expuesta	20	FALLO	WordPress 3.4.0 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 233 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  233 dias restantes (expira: 2026-12-11T23:59:59.000Z)
- 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: HTTPd — 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://egaz.eus/
- 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

- 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**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WPML ver:4.9.2 stt:16,2;
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 3.4.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 3.4.0 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://empleo.egaz.eus
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://perfilcontratante.txorierri.eu

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (166 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://egaz.eus/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): La base de datos está abierta y expuesta a internet, lo que permite ataques directos de fuerza bruta o robo de información sensible.
[HIGH] WordPress versión 3.4.0: Se utiliza una versión extremadamente antigua que contiene múltiples vulnerabilidades conocidas (CVEs) para ejecución remota de código.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos no está cifrado, permitiendo que un atacante intercepte credenciales y archivos en la red.
[HIGH] Content-Security-Policy (CSP) ausente: La falta de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de datos.
[HIGH] X-Frame-Options ausente: El sitio es vulnerable a clickjacking, permitiendo que atacantes oculten la web en marcos para engañar a los usuarios.
[HIGH] HSTS (Strict-Transport-Security) no configurado: El servidor no obliga a los navegadores a usar HTTPS, facilitando ataques de degradación de conexión.
[MEDIUM] Puerto 22 (SSH): El servicio de administración remota está expuesto públicamente, aumentando la superficie de ataque para accesos no autorizados.
[MEDIUM] Contenido Mixto: Existen recursos que se cargan mediante HTTP dentro de la página segura HTTPS, lo que debilita el cifrado del sitio.
[MEDIUM] X-Content-Type-Options ausente: El navegador podría intentar interpretar archivos de forma incorrecta, permitiendo la ejecución de scripts maliciosos.
[MEDIUM] Archivo /readme.html accesible: Este archivo revela información técnica de la instalación que ayuda a los atacantes en la fase de reconocimiento.
[LOW] Cabecera de servidor expuesta: El servidor revela el uso de HTTPd, proporcionando detalles sobre la tecnología subyacente que pueden ser aprovechados.
[LOW] Meta generator expuesto: Se muestra la versión exacta de plugins como WPML, permitiendo buscar vulnerabilidades específicas para esos componentes.