EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://terranea.es	Checks	9 pruebas
Dominio	terranea.es	Hallazgos	47 totales
Fecha	23 de abril de 2026 a las 07:54	Problemas	10 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 72/100, lo que equivale a una calificación de grado C. El análisis se basó en la ejecución de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue identificado como fallo crítico. Aunque el cifrado de transporte es robusto, la ausencia total de cabeceras de seguridad y la configuración inadecuada de las cookies representan riesgos significativos para la integridad de los datos. En su estado actual, el sitio se considera vulnerable a ataques de interceptación y explotación del lado del cliente.

Resumen de Riesgos

0	5	4	1	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 320 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	67	AVISO	ASP.NET_SessionId: falta Secure
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 320 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  320 dias restantes (expira: 2027-03-09T11:25:20.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-05T11:25:20.000Z
- 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: Microsoft-IIS/8.0 — 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://www.terranea.es/
- 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

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 — 67/100

Estado: AVISO

ASP.NET_SessionId: falta Secure

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: ASP.NET_SessionId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: ASP.NET_SessionId — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: ASP.NET_SessionId — SameSite**
  SameSite=lax

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (2663 bytes)
- INFO **Reglas robots.txt**
  64 Disallow, 14 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://www.terranea.es/sitemap.xml
- 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] Content-Security-Policy: Falta esta cabecera, lo que permite la ejecución de scripts no autorizados y ataques de inyección XSS.
[HIGH] X-Frame-Options: No configurada, dejando el sitio expuesto a ataques de clickjacking que pueden engañar al usuario.
[HIGH] Strict-Transport-Security: Falta de HSTS, lo que impide que el navegador fuerce siempre una conexión cifrada y segura.
[HIGH] Cookie ASP.NET_SessionId: Falta el flag Secure, permitiendo que la cookie de sesión se transmita a través de conexiones no cifradas.
[MEDIUM] X-Content-Type-Options: Ausente, permitiendo que el navegador intente adivinar el tipo de contenido, facilitando ataques de sniffing.
[MEDIUM] Referrer-Policy: No detectada, lo que puede provocar la filtración accidental de información sensible en la URL a sitios externos.
[MEDIUM] Permissions-Policy: Falta esta cabecera para restringir el acceso del navegador a APIs sensibles como la cámara o el micrófono.
[MEDIUM] Bloqueo en Robots.txt: El archivo bloquea la indexación de todo el contenido del sitio, lo cual puede ser un error de configuración.
[LOW] Server header expuesto: Se revela la tecnología Microsoft-IIS/8.0, lo que ayuda a un atacante a buscar vulnerabilidades específicas del software.