EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://terranea.es	Checks	9 pruebas
Dominio	terranea.es	Hallazgos	47 totales
Fecha	1 de agosto de 2026 a las 08:01	Problemas	10 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 72/100, lo que equivale a una nota de grado C. Durante la auditoría se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias, 2 presentaron advertencias y una fue clasificada como fallo crítico por la ausencia total de protecciones avanzadas. Aunque el cifrado de datos base es correcto, la carencia de cabeceras de seguridad y la configuración inadecuada de las cookies de sesión exponen el sitio a riesgos evitables. Debido a estas deficiencias técnicas en la configuración del servidor, el sitio se considera vulnerable ante ataques de inyección y suplantación de identidad.

Resumen de Riesgos

0	5	4	1	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 220 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 220 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  220 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: La ausencia de esta cabecera permite ataques de inyección de contenido y XSS al no restringir el origen de los recursos externos.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar al usuario.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras permanentemente, facilitando ataques de degradación de protocolo (SSL Stripping).
[HIGH] Cookie ASP.NET_SessionId (Secure flag): La cookie de sesión carece del atributo Secure, lo que significa que la información de identidad del usuario podría ser enviada a través de conexiones HTTP no cifradas.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría llevar al navegador a interpretar archivos de texto como scripts ejecutables maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación enviada a terceros, lo que compromete la privacidad de los flujos de tráfico del sitio.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso no autorizado a funciones del dispositivo como cámara o micrófono desde el contexto web.
[MEDIUM] Bloqueo total en Robots.txt: El archivo robots.txt bloquea la indexación de todo el sitio mediante la instrucción Disallow: /, lo cual puede ser un error de configuración que afecta la visibilidad.
[LOW] Server header expuesto: El servidor revela el uso de Microsoft-IIS/8.0, información que facilita a un atacante la búsqueda de vulnerabilidades específicas para esa versión de software.