EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://net12.bec.eu	Checks	9 pruebas
Dominio	net12.bec.eu	Hallazgos	44 totales
Fecha	9 de abril de 2026 a las 07:28	Problemas	10 detectados

C

69/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado sobre el sitio web ha dado como resultado una puntuacion de 69/100, lo que corresponde a una calificacion de grado C. Durante la evaluacion se ejecutaron 9 checks pasivos, resultando en 5 verificaciones correctas, 1 advertencia y 2 fallos criticos en la configuracion de seguridad. A pesar de contar con un cifrado SSL valido, la ausencia de cabeceras de proteccion modernas y una gestion deficiente de las cookies de sesion comprometen la integridad del sitio. En conclusion, el sitio web se considera vulnerable ante ataques de secuestro de sesion e inyeccion de contenido malicioso.

Resumen de Riesgos

0	4	4	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 206 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
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	0	FALLO	JSESSIONID: falta HttpOnly; JSESSIONID: falta Se...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 206 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  206 dias restantes (expira: 2026-10-31T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-10T00:00:00.000Z
- 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

- 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.)

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 — 0/100

Estado: FALLO

JSESSIONID: falta HttpOnly; JSESSIONID: falta Secure; JSESSIONID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: JSESSIONID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: JSESSIONID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: JSESSIONID — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (720 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 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)**
  Cerrado — 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

[ALTA] Ausencia de Content-Security-Policy: No se detecto esta cabecera, lo que facilita ataques de Cross-Site Scripting (XSS) y la inyeccion de scripts externos no autorizados.
[ALTA] Ausencia de Strict-Transport-Security: La falta de HSTS impide obligar al navegador a usar siempre conexiones seguras, permitiendo ataques de degradacion de protocolo.
[ALTA] Cookie JSESSIONID sin flag HttpOnly: Al carecer de este atributo, la cookie de sesion es accesible mediante JavaScript, aumentando el riesgo de robo de identidad en ataques XSS.
[ALTA] Cookie JSESSIONID sin flag Secure: La cookie puede ser enviada a traves de conexiones HTTP no cifradas, lo que permite a un atacante interceptar la sesion en la red.
[MEDIA] Ausencia de Referrer-Policy y Permissions-Policy: No se controla que informacion de procedencia se envia ni se restringen las capacidades del navegador como el uso de camara o microfono.

[MEDIA] Cookie JSESSIONID sin flag SameSite: La omision de este parametro hace que el sistema sea susceptible a ataques de Cross-Site Request Forgery (CSRF).
[MEDIA] Error en Redireccion HTTPS: No se ha podido confirmar que el sitio redirija automaticamente el trafico inseguro al puerto seguro.
[BAJA] Exposicion de rutas en robots.txt: El archivo bloquea todo el acceso y revela una ruta denominada config, lo cual podria guiar a un atacante hacia directorios sensibles.
[BAJA] Ausencia de sitemap.xml: El archivo de estructura del sitio no esta accesible, devolviendo un error de permiso denegado 403.