

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://formularios.bec.eu/	Checks	9 pruebas
Dominio	formularios.bec.eu	Hallazgos	38 totales
Fecha	9 de abril de 2026 a las 07:37	Problemas	8 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 corresponde a una calificación de grado C. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 0 presentaron advertencias y 2 fueron marcados como fallidos. A pesar de contar con un cifrado SSL robusto, el servidor presenta una ausencia total de cabeceras de seguridad esenciales para la protección del usuario final. En su estado actual, el sitio se considera vulnerable a ataques de intermediación y de inyección de contenido debido a la falta de endurecimiento (hardening) en su configuración.

Resumen de Riesgos

0 CRITICO	3 ALTO	3 MEDIO	2 BAJO	30 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 206 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y 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 — 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

- 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.)

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 — 100/100

Estado: OK

No se encontraron cookies

- INFO

Cookies detectadas
El sitio no establece cookies en la respuesta inicial

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO

robots.txt
No encontrado (HTTP 403)
- BAJO

sitemap.xml
No encontrado (HTTP 403)
- BAJO

security.txt
No encontrado — Recomendado para política 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 — Envío 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

[HIGH] Content-Security-Policy: Falta — La ausencia de esta cabecera permite la ejecución de scripts no autorizados, aumentando el riesgo de ataques XSS y de inyección de datos.

[HIGH] X-Frame-Options: Falta — El sitio es susceptible a ataques de clickjacking, permitiendo que un atacante lo cargue en un marco invisible para engañar al usuario.

[HIGH] Strict-Transport-Security: Falta — No se fuerza el uso de conexiones seguras mediante HSTS, lo que permite posibles ataques de degradación de protocolo.

[MEDIUM] X-Content-Type-Options: Falta — El navegador podría intentar interpretar el contenido de forma distinta al tipo MIME declarado, facilitando la ejecución de malware.

[MEDIUM] Referrer-Policy: Falta — No hay control sobre la información de referencia enviada a otros sitios, lo que puede comprometer la privacidad de las rutas de navegación.

[MEDIUM] Permissions-Policy: Falta — No se restringen las capacidades del navegador como el acceso a la cámara o micrófono, dejando el control por defecto al cliente.

[LOW] robots.txt: No encontrado — El servidor devuelve un error HTTP 403, impidiendo que los motores de búsqueda sigan las directrices de rastreo deseadas.

[LOW] sitemap.xml: No encontrado — La ausencia de un mapa del sitio dificulta la indexación correcta y el descubrimiento de contenido legítimo.