

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://boyfriendtv.net
Dominio boyfriendtv.net
Fecha 19 de junio de 2026 a las 02:32

Checks 9 pruebas
Hallazgos 44 totales
Problemas 5 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre boyfriendtv.net arroja una puntuación de 77/100, lo que equivale a una nota de B. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 6 resultados satisfactorios, 1 advertencia y 2 fallos técnicos. El sitio demuestra una implementación sólida de cabeceras de seguridad y cifrado, pero presenta deficiencias críticas en la redirección de tráfico y visibilidad de archivos de configuración. Debido a la falta de redirección forzada a HTTPS y la exposición de puertos alternativos, el sitio se clasifica actualmente como vulnerable ante posibles ataques de interceptación y reconocimiento.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 69 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 69 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
69 dias restantes (expira: 2026-08-26T18:22:07.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-05-28T18:22:08.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO **Server header expuesto**
Server: cloudflare — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
Presente: default-src 'none'; script-src 'nonce-KlepZlmDzbEfiaG8q31obl' 'unsafe-eval' http...
- INFO **X-Frame-Options**
Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
Presente: max-age=15552000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
Presente: nosniiff
- INFO **Referrer-Policy**
Presente: same-origin
- INFO **Permissions-Policy**
Presente: accelerometer=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),g...

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
HTTP 403 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=15552000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
HSTS cubre subdominios
- INFO **HSTS max-age**
max-age=15552000 (180 dias)
- INFO **Respuesta HTTPS**
HTTPS responde con status 403

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 politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- **MEDIO** **Puerto 8080 (HTTP-Alt)**
ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Redirección HTTPS ausente: El servidor responde con un código 403 y no redirige automáticamente las solicitudes HTTP hacia HTTPS, permitiendo conexiones no seguras.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: Se detectó un puerto alternativo accesible que suele utilizarse para servicios de gestión o proxys, aumentando la superficie de ataque.

[LOW] Cabecera de servidor expuesta: El campo Server revela el uso de Cloudflare, proporcionando información sobre la infraestructura que puede ser aprovechada en fases de reconocimiento.

[LOW] Archivos de navegación faltantes: El servidor deniega el acceso a robots.txt y sitemap.xml con errores 403, lo que indica una configuración de permisos deficiente o una estructura de archivos incompleta.