EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://es.bongacams.com	Checks	9 pruebas
Dominio	es.bongacams.com	Hallazgos	45 totales
Fecha	27 de mayo de 2026 a las 17:00	Problemas	10 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web ha arrojado una puntuacion de 62/100, lo que corresponde a una nota de grado C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 genero una advertencia y 3 fueron calificados como fallos criticos. El sitio muestra una gestion adecuada del certificado SSL y la seguridad de las cookies, pero presenta deficiencias graves en la configuracion de cabeceras de seguridad y en la gestion del trafico cifrado. Debido a la ausencia de politicas contra inyeccion de codigo y la falta de redireccion automatica a HTTPS, se concluye que el sitio es actualmente vulnerable a diversos vectores de ataque.

Resumen de Riesgos

0	4	3	3	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 305 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
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	1 cookies, todas con flags correctos
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 305 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  305 dias restantes (expira: 2027-03-28T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-26T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Permissions-Policy

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

- 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)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: same-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
  SameSite=none

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] Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso al no restringir las fuentes de scripts y recursos.

[HIGH] Strict-Transport-Security: No se ha configurado la cabecera HSTS, lo que impide que el navegador fuerce conexiones seguras y deja a los usuarios expuestos a ataques de intermediario (MitM).
[HIGH] HTTP a HTTPS redireccion: El servidor no redirige automaticamente las conexiones inseguras a la version cifrada, operando de forma independiente y permitiendo el acceso via HTTP simple.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que podria llevar a que el navegador interprete archivos de texto como scripts ejecutables.
[MEDIUM] Permissions-Policy: No existe una politica que restrinja el acceso de las APIs del navegador a funciones sensibles como la camara, el microfono o la geolocalizacion.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un puerto de servidor web alternativo abierto incrementa la superficie de ataque y podria exponer interfaces administrativas o servicios no protegidos.
[LOW] Server header expuesto: El encabezado revela el uso de Cloudflare, proporcionando informacion tecnica que un atacante podria usar para buscar vulnerabilidades especificas de la infraestructura.
[LOW] Robots.txt no encontrado: La falta de este archivo impide el control sobre que partes del sitio deben ser indexadas por los motores de busqueda.
[LOW] Sitemap.xml no encontrado: La ausencia de un mapa del sitio dificulta la auditoria de endpoints y la correcta indexacion de la estructura web.