EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://boliplay.com/	Checks	9 pruebas
Dominio	boliplay.com	Hallazgos	43 totales
Fecha	26 de junio de 2026 a las 19:36	Problemas	12 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio boliplay.com arroja una puntuación de 57/100, lo que equivale a una calificación de grado D. Durante la auditoría se ejecutaron 9 comprobaciones pasivas, resultando en 5 verificaciones correctas, 1 advertencia y 3 fallos críticos en la configuración del servidor. Se han identificado deficiencias severas en la implementación de cabeceras de seguridad y en la gestión de protocolos de cifrado obligatorios. Debido a la ausencia total de medidas de protección contra ataques comunes como clickjacking o inyección de código, se concluye que el sitio es actualmente vulnerable y presenta un riesgo significativo para la integridad de la navegación.

Resumen de Riesgos

0	5	6	1	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 43 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	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 43 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  43 dias restantes (expira: 2026-08-09T06:38:38.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-11T05:42:07.000Z
- 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: cloudflare — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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
- INFO **Tecnologias detectadas**
  Next.js

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)
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- 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 **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 facilita ataques de inyección de contenido y scripts maliciosos (XSS).
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking que pueden engañar a los usuarios.
[HIGH] Strict-Transport-Security: La falta de HSTS impide forzar conexiones seguras, permitiendo ataques de degradación de protocolo.
[HIGH] Redireccion HTTP a HTTPS: El servidor no redirige automáticamente el tráfico inseguro al puerto seguro, exponiendo los datos a interceptaciones.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador realice MIME-sniffing, aumentando el riesgo de ejecución de archivos maliciosos.

[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a otros sitios, lo que podría filtrar datos de navegación privada.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs del navegador como la cámara o el micrófono, dejando la privacidad del usuario desprotegida.
[MEDIUM] Ruta /administrator/: El panel de login administrativo es accesible públicamente, facilitando intentos de acceso no autorizado.
[MEDIUM] Ruta /user/login: El punto de entrada de usuarios es visible de forma abierta, aumentando la superficie para ataques de fuerza bruta.
[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto, ofreciendo una superficie de ataque adicional en un servicio no estándar.
[LOW] Server header expuesto: Se revela el uso de Cloudflare como tecnología de servidor, proporcionando información técnica útil para un atacante.