EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://gambitogames.com/site/	Checks	9 pruebas
Dominio	gambitogames.com	Hallazgos	44 totales
Fecha	24 de abril de 2026 a las 00:38	Problemas	14 detectados

D

55/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web presenta una puntuación de 55/100, lo que resulta en una calificación de grado D. Durante el análisis se ejecutaron un total de 9 controles pasivos, obteniendo 5 resultados satisfactorios, 1 advertencia y 3 fallos críticos en la configuración. Se han detectado deficiencias severas en la protección de cabeceras HTTP y una preocupante exposición de puertos de servicios internos. En su estado actual, el sitio web se considera vulnerable y requiere una intervención inmediata para mitigar riesgos de intrusión y fuga de datos.

Resumen de Riesgos

1	6	5	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 53 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 53 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  53 dias restantes (expira: 2026-06-16T04:54:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-18T04:55:00.000Z
- 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

- BAJO **Server header expuesto**
  Server: Apache — 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

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (194 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): El puerto de la base de datos está abierto al exterior, permitiendo intentos de conexión directa y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos está abierto y utiliza protocolos no cifrados, facilitando la interceptación de credenciales.

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La falta de esta cabecera deja el sitio vulnerable a ataques de clickjacking para engañar a los usuarios.
[HIGH] Strict-Transport-Security: No se implementa HSTS, por lo que el navegador no obliga a realizar conexiones cifradas.
[HIGH] Redirección HTTP a HTTPS: El sitio responde a peticiones inseguras sin redirigir automáticamente al protocolo cifrado.
[MEDIUM] Puerto 22 (SSH): El acceso remoto está expuesto, lo que representa un vector de ataque si no se gestiona con políticas de acceso estrictas.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a sitios externos.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador como el acceso a la cámara o micrófono.
[MEDIUM] robots.txt restrictivo: El archivo bloquea la indexación de todo el sitio mediante la directiva Disallow: /, lo cual es inusual.
[LOW] Server header expuesto: El servidor revela el uso de Apache, proporcionando información técnica útil para atacantes.
[LOW] sitemap.xml: No se encuentra el mapa del sitio, lo que dificulta la auditoría de recursos y la indexación legítima.