EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.crazygames.com/es/	Checks	9 pruebas
Dominio	www.crazygames.com	Hallazgos	49 totales
Fecha	27 de mayo de 2026 a las 17:57	Problemas	8 detectados

B

79/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado sobre el sitio web ha arrojado una puntuacion de 79/100, lo que equivale a una calificacion de nota B. Se ejecutaron un total de 9 checks pasivos, resultando en 6 verificaciones satisfactorias, 1 advertencia y 2 fallos especificos en la configuracion de seguridad. Los hallazgos principales indican una proteccion robusta en el cifrado de datos, pero debilidades significativas en las politicas de defensa del navegador y la gestion de cookies. Aunque la plataforma presenta una base solida, la ausencia de cabeceras de seguridad criticas permite clasificar ciertos aspectos tecnicos como vulnerables. Es necesario corregir las omisiones en las politicas de contenido para garantizar la integridad total de los usuarios.

Resumen de Riesgos

0	2	5	1	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	33	FALLO	czy_locale: falta HttpOnly; czy_locale: falta Sa...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-08-08T11:46:46.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-10T10:46:54.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, 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
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=604800
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.crazygames.com:443/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=604800
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- MEDIO **HSTS max-age**
  max-age=604800 (7 dias) — Recomendado minimo 180 dias
- 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)

- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 33/100

Estado: FALLO

czy_locale: falta HttpOnly; czy_locale: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: czy_locale — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: czy_locale — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: czy_locale — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (255 bytes)
- INFO **Reglas robots.txt**
  8 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.crazygames.com/sitemap-index.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 permite ataques de inyeccion de codigo y Cross-Site Scripting (XSS) al no restringir las fuentes de contenido.
[HIGH] Cookie czy_locale sin HttpOnly: La falta de este atributo permite que la cookie sea accesible mediante scripts maliciosos, aumentando el riesgo de robo de sesion.
[MEDIUM] Cookie czy_locale sin SameSite: Al no tener definido este parametro, el sitio es susceptible a ataques de falsificacion de peticiones en sitios cruzados (CSRF).
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposicion de este puerto de servicios alternativos puede ser utilizada para identificar proxies o interfaces de gestion desprotegidas.
[MEDIUM] Referrer-Policy: La falta de esta configuracion impide controlar cuanta informacion de navegacion se comparte con otros dominios externos.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones sensibles del navegador como la camara o el microfono, dejando la puerta abierta a usos no autorizados.
[MEDIUM] HSTS max-age insuficiente: El tiempo de persistencia de la conexion segura es de solo 7 dias, cuando el estandar de la industria recomienda al menos 180 dias.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando a posibles atacantes informacion sobre la infraestructura tecnologica utilizada.