EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://priorgame.net/site/	Checks	9 pruebas
Dominio	priorgame.net	Hallazgos	42 totales
Fecha	24 de abril de 2026 a las 00:53	Problemas	15 detectados

D

41/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 41/100, lo que equivale a una nota D. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 2 generaron advertencias y 3 fueron fallos críticos. Se han detectado deficiencias graves en el cifrado de datos y una exposición peligrosa de puertos de infraestructura. Debido a la falta de protecciones básicas y la visibilidad de servicios internos, el sitio se considera vulnerable y presenta un riesgo alto para la integridad de la información.

Resumen de Riesgos

2	6	5	2	27
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- INFO **Dias hasta expiracion**
  190 dias restantes (expira: 2026-10-30T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-29T00:00:00.000Z
- 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: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS

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 — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO **Protocolo**
  El sitio no usa 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] Certificado SSL no válido: La ausencia de un certificado válido impide el cifrado de la conexión, permitiendo la interceptación de datos.
[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos está expuesta directamente a internet, lo que permite intentos de acceso no autorizado y ataques de fuerza bruta.
[HIGH] Redirección HTTP a HTTPS fallida: El sitio responde a través de HTTP 200 sin forzar una conexión segura, dejando a los usuarios vulnerables.
[HIGH] Ausencia de Content-Security-Policy (CSP): La falta de esta cabecera facilita ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] Ausencia de X-Frame-Options: El sitio es susceptible a ataques de clickjacking al permitir que el contenido sea embebido en marcos externos.
[HIGH] Ausencia de Strict-Transport-Security (HSTS): No se obliga al navegador a usar siempre conexiones cifradas, permitiendo ataques de degradación de protocolo.
[HIGH] Puerto 21 (FTP) abierto: Este servicio transmite credenciales y archivos sin cifrar, siendo un objetivo primario para el robo de información.
[HIGH] Protocolo no seguro: El uso exclusivo de HTTP en lugar de HTTPS expone toda la actividad del usuario a terceros.
[MEDIUM] Ausencia de X-Content-Type-Options: Permite que los navegadores adivinen el tipo de contenido, lo que puede derivar en la ejecución de scripts maliciosos.

[MEDIUM] Puerto 22 (SSH) abierto: La exposición de este puerto de administración remota aumenta la superficie de ataque sobre el servidor.
[MEDIUM] Configuración de robots.txt: El archivo bloquea el acceso total a los motores de búsqueda, lo que puede indicar una configuración de entorno de desarrollo expuesta.
[MEDIUM] Ausencia de Referrer-Policy y Permissions-Policy: Existe una falta de control sobre la privacidad de la navegación y el uso de APIs del navegador como la cámara o el micro.
[LOW] Cabecera Server expuesta: El servidor revela el uso de Apache, proporcionando información técnica valiosa para que un atacante busque exploits específicos.
[LOW] sitemap.xml no encontrado: La ausencia de este archivo dificulta la auditoría de rutas y la correcta indexación de contenidos.