EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Lottengo.com	Checks	9 pruebas
Dominio	lottengo.com	Hallazgos	45 totales
Fecha	30 de abril de 2026 a las 17:14	Problemas	16 detectados

D

51/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 51/100, lo que corresponde a una calificación de grado D. Se ejecutaron un total de 9 checks pasivos, obteniendo 5 resultados satisfactorios y 4 fallos críticos en configuraciones base. El sistema carece de protecciones esenciales en las cabeceras de seguridad y presenta una gestión deficiente de las sesiones de usuario. No se detectó un CMS conocido, pero la exposición de rutas administrativas y la falta de cifrado obligatorio comprometen la integridad de la plataforma. En su estado actual, el sitio se considera vulnerable y requiere medidas correctivas inmediatas para proteger la información de los usuarios.

Resumen de Riesgos

0	7	8	1	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 37 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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 37 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  37 dias restantes (expira: 2026-06-06T23:01:57.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-08T23:01:58.000Z
- 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: nginx — 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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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 — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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
- 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

[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).

[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking, permitiendo que un atacante cargue la web en un marco invisible para engañar al usuario.
[HIGH] Falta de Strict-Transport-Security: No se obliga al navegador a usar conexiones seguras, permitiendo ataques de degradación de protocolo.
[HIGH] Ausencia de redirección HTTPS: El servidor responde a peticiones HTTP sin redirigir al protocolo seguro, exponiendo los datos transmitidos a interceptaciones.
[HIGH] Cookie PHPSESSID insegura (HttpOnly): La cookie de sesión es accesible mediante JavaScript, lo que facilita el robo de sesiones en caso de un ataque XSS.
[HIGH] Cookie PHPSESSID insegura (Secure): El identificador de sesión se envía a través de conexiones HTTP no cifradas, permitiendo que un atacante capture la sesión en redes públicas.
[MEDIUM] Cookie PHPSESSID sin atributo SameSite: La falta de esta configuración hace que el sitio sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Exposición de archivos informativos: Los archivos /readme.html y /README.txt son accesibles públicamente, lo que puede revelar detalles técnicos internos.
[MEDIUM] Rutas administrativas expuestas: Los paneles de acceso en /administrator/ y /user/login son visibles, facilitando intentos de acceso por fuerza bruta.
[MEDIUM] Falta de X-Content-Type-Options: Permite que el navegador intente adivinar el tipo de contenido, lo que puede llevar a la ejecución de archivos maliciosos camuflados.
[MEDIUM] Falta de Referrer-Policy: No se controla la cantidad de información que el navegador envía al navegar hacia otros sitios externos.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el uso de APIs del navegador como la cámara o el micrófono, aumentando la superficie de ataque.
[MEDIUM] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos dificulta el control sobre qué partes del sitio deben ser rastreadas por motores de búsqueda.
[LOW] Cabecera de servidor expuesta: El servidor revela que utiliza nginx, información que ayuda a los atacantes a buscar vulnerabilidades específicas para esa tecnología.