EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Lottolivery.com	Checks	9 pruebas
Dominio	lottolivery.com	Hallazgos	45 totales
Fecha	30 de abril de 2026 a las 17:18	Problemas	19 detectados

D

43/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar el análisis de seguridad en Lottolivery.com, se ha determinado una puntuación de 43/100, lo que otorga al sitio una calificación de nota D. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 4 verificaciones exitosas y 5 fallos significativos en áreas críticas de la infraestructura. La ausencia total de cabeceras de seguridad y la exposición de servicios internos de base de datos representan un riesgo de seguridad elevado. Por tanto, se concluye que el sitio es actualmente vulnerable a ataques de interceptación de datos y acceso no autorizado.

Resumen de Riesgos

1	8	9	1	26
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 33 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	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 33 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  33 dias restantes (expira: 2026-06-02T20:02:28.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-04T20:02:29.000Z
- 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 — 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): ABIERTO — La base de datos está expuesta directamente a internet, permitiendo intentos de acceso externo.

[HIGH] Content-Security-Policy: Falta — El sitio no tiene protecciones contra ataques de inyección de scripts (XSS).
[HIGH] X-Frame-Options: Falta — La plataforma es vulnerable a ataques de clickjacking que pueden engañar al usuario.
[HIGH] Strict-Transport-Security: Falta — No se fuerza el uso de conexiones seguras, permitiendo degradaciones de protocolo.
[HIGH] HTTP a HTTPS redireccion: FAIL — El servidor no redirige automáticamente el tráfico inseguro al puerto cifrado.
[HIGH] Puerto 21 (FTP): ABIERTO — Servicio de transferencia de archivos activo sin cifrado, permitiendo la captura de credenciales.
[HIGH] Cookie PHPSESSID: Falta HttpOnly y Secure — La sesión del usuario puede ser robada mediante scripts maliciosos o en redes no seguras.
[MEDIUM] X-Content-Type-Options: Falta — El navegador podría interpretar archivos de forma incorrecta, facilitando la ejecución de malware.
[MEDIUM] Referrer-Policy: Falta — Se podría filtrar información sensible de navegación a dominios de terceros.
[MEDIUM] Permissions-Policy: Falta — No existen restricciones sobre el acceso del sitio a funciones del hardware del usuario.
[MEDIUM] Puerto 22 (SSH): ABIERTO — El puerto de administración remota es visible, aumentando la superficie de ataque por fuerza bruta.
[MEDIUM] Cookie PHPSESSID: Falta SameSite — El sitio es susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Archivos /readme.html y /README.txt: Expuestos — Estos archivos pueden revelar detalles técnicos sobre el desarrollo del sitio.
[MEDIUM] Rutas /administrator/ y /user/login: Accesibles — Los paneles de gestión son visibles para cualquier atacante.
[LOW] Server header expuesto: Revela el uso de nginx, lo que ayuda a un atacante a buscar exploits específicos para esa versión.