EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://compilezone.com	Checks	9 pruebas
Dominio	compilezone.com	Hallazgos	46 totales
Fecha	27 de junio de 2026 a las 06:52	Problemas	12 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada en el sitio web arroja una puntuación de 62/100, lo que representa una calificación de grado C. El análisis se basó exclusivamente en 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 presentaron advertencias y 2 fallos críticos de configuración. A pesar de contar con una infraestructura de red estable y un certificado SSL válido, la ausencia total de cabeceras de seguridad y la gestión deficiente de las cookies representan un riesgo significativo. En su estado actual, el sitio se considera vulnerable debido a que carece de protecciones esenciales contra ataques comunes como el secuestro de sesiones y la inyección de contenido.

Resumen de Riesgos

0	6	5	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 32 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 32 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  32 dias restantes (expira: 2026-07-29T05:23:41.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-30T05:23:42.000Z
- 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/2.4.67 (Debian) — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://compilezone.com/
- 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 — 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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://fonts.googleapis.com/css?family=Open+Sans:400,300,600...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (143 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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] Content-Security-Policy: Falta esta cabecera, lo que deja el sitio expuesto a ataques de Cross-Site Scripting (XSS) e inyección de datos maliciosos.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado en iframes, facilitando ataques de clickjacking para engañar a los usuarios.
[HIGH] Strict-Transport-Security: No está configurada la política HSTS, por lo que el navegador no fuerza la conexión HTTPS de forma permanente, permitiendo ataques de degradación.
[HIGH] Cookie PHPSESSID sin flag HttpOnly: El identificador de sesión es accesible mediante JavaScript, lo que permite que un atacante robe la sesión si existe una vulnerabilidad XSS.
[HIGH] Cookie PHPSESSID sin flag Secure: La cookie de sesión puede ser enviada a través de conexiones no cifradas, aumentando el riesgo de interceptación en redes inseguras.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría intentar adivinar el tipo de contenido, lo que permite la ejecución de scripts camuflados como otros archivos.
[MEDIUM] Referrer-Policy: No hay control sobre la información de origen enviada a terceros, lo que podría filtrar rutas internas sensibles de la aplicación.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones del navegador como la cámara, el micrófono o la geolocalización por parte de terceros.
[MEDIUM] Cookie PHPSESSID sin flag SameSite: La falta de este atributo hace que el sitio sea vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se detectó un recurso de Google Fonts cargando vía HTTP, lo que rompe la integridad de la conexión cifrada HTTPS.
[LOW] Server header expuesto: El encabezado revela el uso de Apache/2.4.67 (Debian), proporcionando a los atacantes información valiosa sobre la tecnología del servidor.