EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://dbzunion.com.br/	Checks	9 pruebas
Dominio	dbzunion.com.br	Hallazgos	48 totales
Fecha	29 de abril de 2026 a las 22:10	Problemas	15 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar el análisis técnico de dbzunion.com.br, se ha determinado una puntuación de 62/100 con una calificación de grado C. La evaluación consistió en 9 checks pasivos, resultando en 5 verificaciones exitosas, 1 advertencia y 3 fallos críticos en la configuración del servidor. Se han detectado debilidades importantes en la protección de sesiones y en la ausencia de cabeceras de seguridad obligatorias. Por lo tanto, se concluye que el sitio es actualmente vulnerable a ataques de secuestro de sesión, clickjacking e inyección de contenido malicioso.

Resumen de Riesgos

0	6	4	5	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 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	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 90 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  90 dias restantes (expira: 2026-07-28T11:30:09.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-29T11:30:10.000Z
- 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/1.24.0 (Ubuntu) — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.30 — Revela framework/lenguaje
- 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://dbzunion.com.br/
- 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
- BAJO **Meta generator**
  Expone: DBZ Union v1.0.0 "Saiyan Awakening"
- INFO **Tecnologias detectadas**
  PHP/8.3.30

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 — 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

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) y la inyección de datos no autorizados.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio puede ser cargado en marcos externos, permitiendo ataques de clickjacking para engañar a los usuarios.
[HIGH] Strict-Transport-Security: No se utiliza HSTS, lo que permite que un atacante intente degradar la conexión de HTTPS a HTTP mediante ataques de intermediario.
[HIGH] Cookie insegura (HttpOnly): La cookie PHPSESSID carece del atributo HttpOnly, lo que permite que sea accesible mediante scripts del navegador y facilita el robo de identidad.
[HIGH] Cookie insegura (Secure): El identificador de sesión PHPSESSID no tiene el flag Secure, por lo que podría ser transmitido accidentalmente a través de conexiones no cifradas.
[MEDIUM] X-Content-Type-Options: Falta esta directiva, dejando el sitio expuesto a ataques de MIME-type sniffing donde el navegador interpreta archivos de forma insegura.
[MEDIUM] Referrer-Policy: No hay control sobre la información de referencia enviada a otros sitios, lo que podría filtrar rutas internas privadas.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de funciones del navegador como la geolocalización o periféricos, aumentando la superficie de ataque.
[MEDIUM] Cookie insegura (SameSite): La falta de este atributo en la cookie de sesión hace que la plataforma sea vulnerable a ataques de Cross-Site Request Forgery (CSRF).
[LOW] Server header expuesto: El encabezado revela el uso de nginx/1.24.0 en Ubuntu, información que ayuda a los atacantes a buscar vulnerabilidades específicas del software.
[LOW] X-Powered-By expuesto: El servidor confirma el uso de PHP/8.3.30, lo que permite acotar los vectores de ataque según la versión del lenguaje.
[LOW] Meta generator: La etiqueta meta expone que el sitio utiliza DBZ Union v1.0.0 "Saiyan Awakening", revelando la tecnología personalizada empleada.
[LOW] Archivos de rastreo faltantes: La ausencia de robots.txt y sitemap.xml dificulta la gestión adecuada de la indexación y el comportamiento de los motores de búsqueda.