EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://gyt.brokeris.cl/	Checks	9 pruebas
Dominio	gyt.brokeris.cl	Hallazgos	47 totales
Fecha	21 de mayo de 2026 a las 21:05	Problemas	8 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada sobre el sitio web arrojo una puntuacion de 81/100, obteniendo una nota final de B. El analisis se baso en la ejecucion de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron clasificados como fallos tecnicos. Si bien la infraestructura de cifrado es robusta, se detectaron carencias importantes en las cabeceras de seguridad y en la configuracion de sesiones. En su estado actual, el sitio se considera moderadamente seguro, pero vulnerable a ataques especificos como clickjacking y secuestro de sesion.

Resumen de Riesgos

0	1	4	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 74 dias
Cabeceras de Seguridad	60	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, Ref...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	67	AVISO	ASPSESSIONIDAGTRTSAC: falta SameSite
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 74 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  74 dias restantes (expira: 2026-08-04T04:28:48.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-06T03:28:53.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: FALLO

Solo 3/6 presentes. Faltan: X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: frame-ancestors 'self' https://*.corredorasecurity.cl
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://gyt.brokeris.cl/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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 — 67/100

Estado: AVISO

ASPSESSIONIDAGTRTSAC: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: ASPSESSIONIDAGTRTSAC — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ASPSESSIONIDAGTRTSAC — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ASPSESSIONIDAGTRTSAC — 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 — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado dentro de marcos (iframes) en dominios externos, facilitando ataques de clickjacking.
[MEDIUM] Cookie ASPSESSIONIDAGTRTSAC: La falta del atributo SameSite en las cookies de sesion expone a los usuarios a riesgos de falsificacion de peticion en sitios cruzados (CSRF).
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detecto un puerto alternativo abierto que podria actuar como un proxy o servicio administrativo, aumentando la superficie de ataque.
[MEDIUM] Referrer-Policy: No existe una politica definida para el control de la informacion de referencia, lo que puede filtrar URLs internas a terceros.
[MEDIUM] Permissions-Policy: La falta de esta directiva impide restringir el acceso del navegador a funciones sensibles como la camara, el microfono o la geolocalizacion.
[LOW] Cabecera Server expuesta: El servidor responde con informacion sobre el uso de Cloudflare, lo que ayuda a los atacantes en la fase de reconocimiento tecnologico.
[LOW] Ausencia de robots.txt: No se encontro el archivo de reglas para buscadores, lo que dificulta el control de rastreo de directorios privados.
[LOW] Ausencia de sitemap.xml: La falta de este archivo afecta la indexacion organizada y puede exponer una estructura de directorios desordenada.