EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://email.tallerssh.cu	Checks	9 pruebas
Dominio	email.tallerssh.cu	Hallazgos	48 totales
Fecha	3 de mayo de 2026 a las 14:07	Problemas	11 detectados

C

63/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web arroja una puntuacion de 63/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 checks pasivos, resultando en 5 verificaciones correctas, 2 advertencias y 2 fallos criticos de configuracion. Aunque el sitio cuenta con un cifrado de transporte valido, presenta carencias importantes en la implementacion de cabeceras de seguridad y politicas de redireccion. En su estado actual, el sitio se considera vulnerable a ataques de intermediario y de inyeccion de codigo debido a configuraciones incompletas en el servidor.

Resumen de Riesgos

0	4	5	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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	67	AVISO	roundcube_sessid: falta SameSite
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 84 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  84 dias restantes (expira: 2026-07-26T04:07:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-27T04:07:41.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, 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
- INFO **X-Frame-Options**
  Presente: sameorigin
- 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 302 — 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
- INFO **Tecnologias detectadas**
  Next.js

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

roundcube_sessid: falta SameSite

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

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (25 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- 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] Redireccion HTTP a HTTPS: El servidor no redirige automaticamente el trafico inseguro al protocolo cifrado, permitiendo conexiones vulnerables a la interceptacion.
[HIGH] Content-Security-Policy: Falta esta cabecera, lo que deja al sitio expuesto a ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce el uso exclusivo de HTTPS, facilitando ataques de degradacion de seguridad.
[MEDIUM] Cookie roundcube_sessid: El identificador de sesion carece del atributo SameSite, lo que lo hace susceptible a ataques de falsificacion de peticion en sitios cruzados (CSRF).
[MEDIUM] X-Content-Type-Options: No esta configurada, permitiendo que el navegador realice "MIME-type sniffing" y ejecute archivos con tipos de contenido incorrectos.
[MEDIUM] Referrer-Policy: Falta esta cabecera para controlar cuanta informacion de procedencia se comparte con otros dominios al navegar.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el acceso a APIs del navegador, como la camara, el microfono o la geolocalizacion.
[MEDIUM] robots.txt: Se detecto un bloqueo total del sitio mediante la directiva Disallow, lo que impide cualquier tipo de indexacion legitima.
[LOW] Server header expuesto: La cabecera revela el uso de nginx, proporcionando informacion tecnica que un atacante puede usar para buscar exploits especificos.
[LOW] sitemap.xml: El archivo no fue encontrado, lo que representa una deficiencia en la estructura y visibilidad del sitio.