# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://stueamcommuunity.com/70497a5428550255055b5c2f5a05085e62585404 | | 9 pruebas |
| Dominio | stueamcommuunity.com | Hallazgos | 44 totales |
| Fecha | 27 de mayo de 2026 a las 02:23 | Problemas | 5 detectados |

**B**

78/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis técnico de ciberseguridad ha otorgado al sitio una puntuación de 78/100 con una nota B. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 6 resultados satisfactorios, 1 advertencia y 2 fallos en configuraciones críticas. A pesar de contar con un cifrado SSL activo, la ausencia de redirecciones obligatorias hacia el protocolo seguro compromete la integridad de la sesión del usuario. Debido a estos hallazgos técnicos, el sitio se clasifica actualmente como vulnerable ante ataques de interceptación de tráfico y reconocimiento de infraestructura.

## Resumen de Riesgos

| 0 | 1 | 1 | 3 | 39 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 88 dias |
| Cabeceras de Seguridad | 85 | AVISO | 5/6 presentes. Faltan: Permissions-Policy |
| 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 | 100 | OK | No se encontraron cookies |
| 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 88 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  88 dias restantes (expira: 2026-08-22T15:38:33.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-24T15:38:34.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: frame-ancestors *
- INFO **X-Frame-Options**
  Presente: ALLOWALL
- INFO **Strict-Transport-Security**
  Presente: max-age=15552000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer
- 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
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15552000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15552000 (180 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 — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

## 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] HTTP a HTTPS redireccion: El servidor permite conexiones mediante HTTP sin redirigir automáticamente a HTTPS, lo que facilita ataques de intermediario (MitM).
[MEDIUM] Permissions-Policy: Falta esta cabecera de seguridad, lo que impide restringir el acceso del navegador a APIs sensibles como la cámara, el micrófono o la geolocalización.

[LOW] Server header expuesto: El servidor revela el uso de la tecnología openresty, proporcionando información valiosa a posibles atacantes para buscar exploits específicos.
[LOW] robots.txt: No se encontró el archivo, lo que impide definir reglas para los rastreadores sobre qué directorios deben ser ignorados.
[LOW] sitemap.xml: La ausencia de este archivo dificulta el mapeo estructurado del contenido y la identificación de rutas legítimas en el servidor.