EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.igssgt.org	Checks	9 pruebas
Dominio	www.igssgt.org	Hallazgos	47 totales
Fecha	21 de abril de 2026 a las 20:29	Problemas	20 detectados

D

45/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría de seguridad sobre el portal analizado, se ha determinado una puntuación exacta de 45/100, lo que equivale a una nota D. El análisis se basó en 9 checks pasivos ejecutados, de los cuales 4 resultaron satisfactorios y 5 presentaron fallos críticos. No se llevó a cabo un pentest activo, centrando el diagnóstico en la configuración de red y cabeceras web. Los resultados revelan deficiencias graves en la protección de la infraestructura y en la seguridad de las sesiones de usuario. Por lo tanto, se concluye que el sitio es actualmente vulnerable y presenta una superficie de ataque considerable.

Resumen de Riesgos

3	9	6	2	27
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 206 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	17	FALLO	visid_incap_3206936: falta Secure; visid_incap_3...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	5 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 206 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  206 dias restantes (expira: 2026-11-13T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-17T00:00:00.000Z
- 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

- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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 — 17/100

Estado: FALLO

visid_incap_3206936: falta Secure; visid_incap_3206936: falta SameSite; incap_ses_260_3206936: falta HttpOnly; incap_ses_260_3206936: falta Secure; incap_ses_260_3206936: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)

- INFO **Cookie: visid_incap_3206936 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: visid_incap_3206936 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: visid_incap_3206936 — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: incap_ses_260_3206936 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: incap_ses_260_3206936 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: incap_ses_260_3206936 — 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 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

5 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): El servicio de base de datos está expuesto directamente a internet, lo que permite intentos de conexión externa y ataques de fuerza bruta.
[CRITICAL] Puerto 3389 (RDP): El acceso por escritorio remoto de Windows está abierto, facilitando posibles intrusiones si las credenciales son comprometidas.
[CRITICAL] Puerto 6379 (Redis): El servicio de caché está expuesto, lo que podría permitir la manipulación de datos o la exfiltración de información sensible.
[HIGH] Puerto 21 (FTP): Protocolo de transferencia de archivos activo que envía datos y credenciales sin cifrar, siendo vulnerable a interceptación.
[HIGH] Redirección HTTPS: El sitio no redirige automáticamente el tráfico HTTP inseguro hacia HTTPS, exponiendo la comunicación de los usuarios.
[HIGH] Content-Security-Policy: Falta esta cabecera esencial para prevenir ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La ausencia de esta cabecera hace que el sitio sea vulnerable a ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no obliga a realizar conexiones seguras.
[HIGH] Cookie incap_ses_260_3206936: Falta el flag HttpOnly, permitiendo que la cookie sea accesible mediante scripts, y el flag Secure, permitiendo su envío por canales no cifrados.
[HIGH] Cookie visid_incap_3206936: Falta el flag Secure, lo que implica que la información de seguimiento se envía en conexiones HTTP planas.
[MEDIUM] Cookie SameSite: Las cookies carecen del atributo SameSite, lo que deja a los usuarios expuestos a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] X-Content-Type-Options: Falta de protección contra el rastreo de tipos MIME, lo que podría derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy y Permissions-Policy: Ausencia de control sobre la información de referencia enviada y sobre las APIs del navegador que el sitio puede utilizar.
[MEDIUM] Puerto 8080 (HTTP-Alt): Un puerto de servidor web alternativo está abierto, aumentando innecesariamente los puntos de entrada potenciales.
[LOW] Archivos de indexación: No se detectaron los archivos robots.txt ni sitemap.xml, lo que impide una gestión adecuada del rastreo por parte de buscadores.