EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://agrestsrl.com	Checks	9 pruebas
Dominio	agrestsrl.com	Hallazgos	45 totales
Fecha	4 de septiembre de 2026 a las 19:52	Problemas	11 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio agrestsrl.com arroja una puntuación de 61/100, lo que equivale a una nota de grado C. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 fallaron críticamente. El sitio web dispone de un cifrado SSL válido, pero carece de las protecciones esenciales en las cabeceras de respuesta y no obliga al uso de conexiones seguras. La presencia de contenido mixto y la exposición de información del servidor incrementan la superficie de ataque. En su estado actual, el sitio se considera vulnerable ante ataques de intermediarios, inyección de scripts y clickjacking.

Resumen de Riesgos

0	5	4	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 151 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	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 151 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  151 dias restantes (expira: 2027-02-02T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-26T00:00:00.000Z
- 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

- BAJO **Server header expuesto**
  Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- 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 200 — 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
- BAJO **Meta generator**
  Expone: Mobirise v4.12.4, mobirise.com
- 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 — 100/100

Estado: OK

No se encontraron cookies

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

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.agrestsrl.com/

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (35 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **sitemap.xml**
  Presente, 4 URLs
- 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] Ausencia de redirección HTTP a HTTPS: El sitio permite el acceso a través de conexiones no cifradas, lo que expone los datos de los usuarios a intercepciones.

[HIGH] Falta de Strict-Transport-Security (HSTS): No se instruye al navegador para que use exclusivamente HTTPS, permitiendo ataques de degradación de SSL.
[HIGH] Falta de Content-Security-Policy (CSP): El sitio no posee una política que prevenga la ejecución de scripts maliciosos o ataques de inyección de contenido (XSS).
[HIGH] Falta de X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en marcos (iframes), facilitando ataques de clickjacking.
[MEDIUM] Presencia de Contenido Mixto: Se detectó un recurso stylesheet cargado mediante protocolo HTTP inseguro dentro de la página HTTPS, comprometiendo la integridad.
[MEDIUM] Falta de X-Content-Type-Options: El sitio es vulnerable al sniffing de tipos MIME, lo que podría permitir que archivos cargados se interpreten como scripts ejecutables.
[MEDIUM] Falta de Referrer-Policy: No se controla la cantidad de información que el navegador envía al navegar desde agrestsrl.com hacia otros enlaces.
[MEDIUM] Falta de Permissions-Policy: No se restringe el acceso de las APIs del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[LOW] Cabecera de servidor expuesta: El sistema revela explícitamente el uso de Microsoft-IIS/10.0, facilitando a un atacante la búsqueda de vulnerabilidades específicas.
[LOW] Meta Generator expuesto: El código fuente revela el uso de Mobirise v4.12.4, proporcionando detalles sobre la tecnología de construcción del sitio.