EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://isil.pe	Checks	9 pruebas
Dominio	isil.pe	Hallazgos	42 totales
Fecha	22 de mayo de 2026 a las 05:32	Problemas	11 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha arrojado una puntuación de 61/100, lo que otorga una nota de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 6 verificaciones satisfactorias y 3 fallos en configuraciones críticas. Aunque el cifrado de datos posee una base sólida, la ausencia total de cabeceras de seguridad y la falta de redirección automática hacia protocolos seguros representan una debilidad significativa. En su estado actual, el sitio se considera vulnerable ante ataques de manipulación de tráfico e inyección de contenido debido a configuraciones de servidor incompletas.

Resumen de Riesgos

0	5	3	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 272 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	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 272 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  272 dias restantes (expira: 2027-02-17T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-17T00:00:00.000Z
- 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

- BAJO **Server header expuesto**
  Server: awselb/2.0 — 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 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 — 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 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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] Content-Security-Policy: La ausencia de esta política permite la ejecución de scripts maliciosos y ataques de inyección de datos XSS.
[HIGH] X-Frame-Options: El sitio no protege contra el secuestro de clics (clickjacking), permitiendo que su contenido sea embebido en sitios maliciosos.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador obligue siempre el uso de conexiones cifradas, facilitando ataques de degradación.
[HIGH] Redirección HTTPS: El servidor no redirige el tráfico inseguro HTTP hacia HTTPS, devolviendo en su lugar un error de acceso denegado (403).
[MEDIUM] X-Content-Type-Options: Al no estar configurada, el navegador podría interpretar archivos como tipos MIME diferentes a los declarados, facilitando ataques de ejecución.
[MEDIUM] Referrer-Policy: Existe una falta de control sobre la información de navegación que se envía a sitios de terceros mediante los encabezados de referencia.

[MEDIUM] Permissions-Policy: No se han restringido las capacidades del navegador, lo que deja expuesto el acceso a APIs sensibles como geolocalización o cámara.
[LOW] Server header expuesto: El servidor revela explícitamente el uso de awselb/2.0, proporcionando información técnica que ayuda a potenciales atacantes a perfilar la infraestructura.
[LOW] Robots.txt y Sitemap: La falta de estos archivos impide una gestión adecuada del rastreo por motores de búsqueda y el control de directorios.