EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://else.com.pe	Checks	9 pruebas
Dominio	else.com.pe	Hallazgos	44 totales
Fecha	7 de mayo de 2026 a las 17:18	Problemas	12 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web arroja una puntuación de 61/100, lo que equivale a una calificación de grado C. Se ejecutaron un total de 9 chequeos pasivos, resultando en 6 verificaciones exitosas y 3 fallos críticos en la configuración de seguridad. El análisis revela que, aunque existe un cifrado base, el servidor carece de las protecciones modernas necesarias para mitigar ataques de inyección y suplantación. En conclusión, el sitio web se considera vulnerable debido a una configuración incompleta de sus defensas perimetrales y de transporte de datos.

Resumen de Riesgos

0	5	3	4	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 54 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	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 54 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  54 dias restantes (expira: 2026-06-30T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-05-30T00:00:00.000Z
- 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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- 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
- INFO **Tecnologias detectadas**
  ASP.NET

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 Inteligencia Artificial

---RESUMEN EJECUTIVO---
La auditoría de ciberseguridad realizada al sitio web arroja una puntuación de 61/100, lo que equivale a una calificación de grado C. Se ejecutaron un total de 9 chequeos pasivos, resultando en 6 verificaciones exitosas y 3 fallos críticos en la configuración de seguridad. El análisis revela que, aunque existe un cifrado base, el servidor carece de las protecciones modernas necesarias para mitigar ataques de inyección y suplantación. En conclusión, el sitio web se considera vulnerable debido a una configuración incompleta de sus defensas perimetrales y de transporte de datos.

---VULNERABILITIES---

[HIGH] Redirección HTTPS ausente: El servidor no redirige automáticamente el tráfico HTTP a HTTPS, permitiendo conexiones no cifradas.
[HIGH] HSTS (Strict-Transport-Security) ausente: No se instruye al navegador para que use exclusivamente conexiones seguras, facilitando ataques de degradación de SSL.
[HIGH] Content-Security-Policy (CSP) faltante: La ausencia de esta política permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).
[HIGH] X-Frame-Options faltante: El sitio no protege contra ataques de clickjacking, permitiendo que sea embebido en marcos de sitios externos.
[MEDIUM] X-Content-Type-Options faltante: No se previene el sniffing de tipos MIME, lo que podría permitir la ejecución de archivos con contenido malicioso disfrazado.
[MEDIUM] Referrer-Policy faltante: No se controla la información de referencia enviada a otros dominios, comprometiendo la privacidad de la navegación.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el acceso de las APIs del navegador a funciones sensibles como la cámara o el micrófono.
[LOW] Cabecera Server expuesta: Se revela el uso de Microsoft-IIS/10.0, lo que ayuda a potenciales atacantes a identificar vulnerabilidades específicas del software.
[LOW] Cabecera X-Powered-By expuesta: Se muestra el uso del framework ASP.NET, proporcionando información técnica innecesaria sobre la infraestructura interna.
[LOW] Archivos de rastreo ausentes: No se encontraron los archivos robots.txt ni sitemap.xml, lo que dificulta la gestión del rastreo por motores de búsqueda.