EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://empleo.va360labs.com/auth/sign-in	Checks	9 pruebas
Dominio	empleo.va360labs.com	Hallazgos	43 totales
Fecha	17 de junio de 2026 a las 00:20	Problemas	12 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el sitio web arroja una puntuación de 68/100, lo que resulta en una calificación de grado C. El análisis se basó exclusivamente en 9 checks pasivos, de los cuales 5 fueron exitosos, 2 generaron advertencias y 2 resultaron en fallos críticos de configuración. A pesar de contar con un cifrado SSL adecuado, la ausencia total de cabeceras de seguridad y la exposición de servicios de infraestructura representan un riesgo elevado. Por lo tanto, se concluye que el sitio es actualmente vulnerable y requiere acciones correctivas inmediatas para proteger la integridad de los datos.

Resumen de Riesgos

1	4	4	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 22 (SSH)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 89 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  89 dias restantes (expira: 2026-09-14T07:41:16.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-16T07:41:17.000Z
- 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 **X-Powered-By expuesto**
  X-Powered-By: Next.js — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://empleo.va360labs.com/
- 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**
  Next.js, 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 — 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 — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 22 (SSH), 5432 (PostgreSQL)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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

[CRITICAL] Puerto 5432 (PostgreSQL) ABIERTO: Expone directamente el servicio de base de datos a internet, permitiendo intentos de acceso no autorizado y ataques dirigidos.
[HIGH] Content-Security-Policy (CSP) Faltante: La ausencia de esta política permite la ejecución de scripts maliciosos y ataques de inyección de contenido como XSS.
[HIGH] X-Frame-Options Faltante: El sitio no previene ataques de clickjacking, lo que permite que la interfaz sea embebida en sitios maliciosos para engañar al usuario.
[HIGH] Strict-Transport-Security (HSTS) Faltante: No se obliga al navegador a establecer conexiones seguras permanentemente, facilitando ataques de degradación de protocolo.
[MEDIUM] Puerto 22 (SSH) ABIERTO: El servicio de administración remota es visible para cualquier atacante, aumentando la superficie de ataque del servidor.

[MEDIUM] X-Content-Type-Options Faltante: Permite que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy Faltante: No se controla la cantidad de información enviada en las cabeceras de referencia hacia otros dominios.
[MEDIUM] Permissions-Policy Faltante: No se restringen funcionalidades del navegador como el acceso a la cámara o geolocalización a través de APIs.
[LOW] X-Powered-By expuesto (Next.js): Revela el framework utilizado, facilitando que atacantes busquen vulnerabilidades específicas para esa tecnología.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor devuelve un error 404 para archivos esenciales de gestión de rastreo e indexación.