

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://uafe.gob.ec
Dominio uafe.gob.ec
Fecha 31 de agosto de 2026 a las 19:47

Checks 9 pruebas
Hallazgos 44 totales
Problemas 9 detectados

C

65/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del sitio web uafe.gob.ec arroja una puntuación de 65/100, lo que equivale a una calificación de grado C. Durante la evaluación, se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos críticos de configuración. Aunque el cifrado SSL es robusto, la ausencia casi total de cabeceras de seguridad y errores en la redirección HTTPS comprometen la integridad del portal. En su estado actual, el sitio se considera vulnerable ante ataques de intermediarios y de inyección de contenido.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 130 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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 130 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
130 dias restantes (expira: 2027-01-08T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2025-12-08T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO Server header expuesto
Server: nginx — 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
- INFO

Strict-Transport-Security
Presente: max-age=15768000; includeSubDomains; preload;
- 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
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=15768000; includeSubDomains; preload;
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=15768000 (183 dias)
- 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 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 Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) e inyección de datos.
[HIGH] X-Frame-Options: La ausencia de esta protección permite que el sitio sea cargado en frames externos, facilitando ataques de clickjacking.
[HIGH] HTTP a HTTPS redirección: El servidor responde con un error 403 y no redirige automáticamente el tráfico no cifrado hacia la conexión segura.

[MEDIUM] X-Content-Type-Options: Falta la directiva para evitar que el navegador realice MIME-type sniffing, lo que puede derivar en la ejecución de scripts maliciosos.

[MEDIUM] Referrer-Policy: No se ha definido una política de referencia, lo que podría exponer información sensible de la navegación a terceros.

[MEDIUM] Permissions-Policy: La ausencia de esta cabecera impide restringir el acceso del navegador a funciones sensibles como la cámara, el micrófono o la ubicación.

[LOW] Server header expuesto: El servidor revela el uso de nginx, proporcionando información técnica valiosa para que un atacante busque vulnerabilidades específicas.

[LOW] robots.txt no encontrado: El archivo no existe (HTTP 404), lo que impide dar instrucciones claras a los motores de búsqueda sobre la indexación.

[LOW] sitemap.xml no encontrado: La falta de este archivo dificulta la auditoría de la estructura del sitio y su correcta visibilidad en buscadores.