EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://guia.agrocalidad.gob.ec/agrodb/index.phphttps://guia.agrocalidad.gob.ec/agrodb/index.php	Objetivo	Página web
Dominio	guia.agrocalidad.gob.ec	Hallazgos	48 totales
Fecha	21 de abril de 2026 a las 21:36	Problemas	20 detectados

D

51/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio guia.agrocalidad.gob.ec arroja una puntuacion de 51/100, lo que equivale a una nota de D. Durante el analisis se ejecutaron 9 checks pasivos, de los cuales 3 resultaron correctos, 2 presentan advertencias y 4 fueron calificados como fallos criticos. Se han detectado multiples servicios de infraestructura expuestos y una carencia total de politicas de endurecimiento en el servidor web. En su estado actual, el sitio se considera vulnerable y presenta un riesgo significativo para la integridad de los datos y la disponibilidad del servicio.

Resumen de Riesgos

3	8	6	3	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 20 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	17	FALLO	visid_incap_2209164: falta Secure; visid_incap_2...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	5 puertos riesgosos abiertos

SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 20 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  20 dias restantes (expira: 2026-05-11T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-04-10T00:00:00.000Z
- 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: Apache — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://guia.agrocalidad.gob.ec/
- 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

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 — 17/100

Estado: FALLO

visid_incap_2209164: falta Secure; visid_incap_2209164: falta SameSite; incap_ses_1854_2209164: falta HttpOnly; incap_ses_1854_2209164: falta Secure; incap_ses_1854_2209164: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: visid_incap_2209164 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: visid_incap_2209164 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: visid_incap_2209164 — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: incap_ses_1854_2209164 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: incap_ses_1854_2209164 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: incap_ses_1854_2209164 — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 20/100

Estado: FALLO

5 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy

INFO **Puerto 27017 (MongoDB)**

Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 3306 (MySQL): La base de datos esta expuesta a internet, permitiendo intentos de conexion externa y ataques de fuerza bruta.
[CRITICAL] Puerto 3389 (RDP): El servicio de escritorio remoto esta abierto, lo que facilita el acceso directo al sistema operativo por parte de atacantes.
[CRITICAL] Puerto 6379 (Redis): Servicio de cache expuesto sin autenticacion, lo que puede derivar en la fuga de informacion sensible almacenada en memoria.
[HIGH] Content-Security-Policy: Ausencia de esta cabecera, lo que deja al sitio vulnerable a ataques de inyeccion de codigo y XSS.
[HIGH] X-Frame-Options: La falta de esta cabecera permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo ataques de degradacion de cifrado.
[HIGH] Puerto 21 (FTP): Uso de protocolo de transferencia de archivos no cifrado que expone credenciales y datos en la red.
[HIGH] Cookie incap_ses_1854_2209164 (HttpOnly): Falta de atributo que impide que scripts maliciosos accedan a la cookie de sesion.
[HIGH] Cookies de sesion (Secure): Las cookies carecen del flag Secure, por lo que pueden ser enviadas a traves de conexiones HTTP no cifradas.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podria ejecutar archivos maliciosos.
[MEDIUM] Cookies de sesion (SameSite): Ausencia de proteccion contra ataques de falsificacion de solicitudes en sitios cruzados (CSRF).
[MEDIUM] Puerto 8080 (HTTP-Alt): Servidor web alternativo expuesto que aumenta la superficie de ataque disponible.
[LOW] SSL/TLS: El certificado de seguridad es valido pero expirara en un plazo muy corto de 20 dias.
[LOW] Server header: El servidor revela que utiliza Apache, proporcionando informacion util para explotar vulnerabilidades especificas de esa version.
[LOW] Archivos de navegacion: No se encontraron los archivos robots.txt ni sitemap.xml, afectando la gestion del rastreo web.