# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://www.digecam.mil.gt/portal/ | Checks | 9 pruebas |
| Dominio | www.digecam.mil.gt | Hallazgos | 54 totales |
| Fecha | 10 de abril de 2026 a las 17:17 | Problemas | 18 detectados |

**D**

55/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de seguridad realizado al portal web arroja una puntuación exacta de 55/100, lo que equivale a una calificación de nota D. Se ejecutaron 9 checks pasivos de los cuales 6 resultaron satisfactorios, mientras que 3 presentaron fallos críticos en la configuración del servidor y la gestión de sesiones. A pesar de contar con un certificado de cifrado vigente, la ausencia de cabeceras de protección y la falta de redirección segura comprometen la integridad de la plataforma. Los resultados concluyen que el sitio es vulnerable ante ataques de interceptación de datos, clickjacking e inyección de contenido malicioso.

## Resumen de Riesgos

| 0 | 6 | 9 | 3 | 36 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 342 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 | 0 | FALLO | PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu... |
| Contenido Mixto | 100 | OK | No se detecto contenido mixto |
| Robots.txt y Sitemap | 100 | OK | robots.txt y sitemap.xml presentes |
| Puertos Abiertos | 100 | OK | No se detectaron puertos abiertos |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 342 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  342 dias restantes (expira: 2027-03-18T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-18T00:00:00.000Z
- 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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.16 — 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
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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**
  PHP/8.3.16

## Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

## Seguridad de Cookies — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (484 bytes)
- INFO **Reglas robots.txt**
  13 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://digecam.mil.gt/sitemap.xml
- 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] Falta de redirección HTTPS: El servidor no fuerza la conexión segura, permitiendo el acceso mediante HTTP y facilitando la interceptación de tráfico.
[HIGH] Ausencia de Content-Security-Policy (CSP): No existe una política para restringir la carga de recursos, aumentando el riesgo de ataques XSS.
[HIGH] Ausencia de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking al permitir ser cargado dentro de marcos o iframes externos.
[HIGH] Ausencia de Strict-Transport-Security (HSTS): No se obliga al navegador a usar exclusivamente HTTPS, dejando la comunicación expuesta a degradación de seguridad.
[HIGH] Cookies de sesión inseguras (PHPSESSID): La cookie de sesión carece de los flags HttpOnly y Secure, lo que permite su robo mediante scripts o redes no cifradas.
[MEDIUM] Ausencia de X-Content-Type-Options: El navegador puede intentar adivinar el tipo de contenido, lo que facilita la ejecución de archivos maliciosos (MIME-sniffing).
[MEDIUM] Ausencia de Referrer-Policy: No se controla la información de procedencia enviada en las peticiones salientes, pudiendo filtrar rutas internas.
[MEDIUM] Ausencia de Permissions-Policy: No se restringen las APIs del navegador como cámara o micrófono, dejando el control al lado del cliente.
[MEDIUM] Archivos de documentación expuestos: Los archivos /readme.html y /README.txt son accesibles, lo que podría revelar información técnica sobre la infraestructura.
[MEDIUM] Paneles de gestión visibles: Las rutas /wp-login.php, /administrator/ y /user/login están activas, facilitando intentos de acceso no autorizado.
[MEDIUM] Cookie PHPSESSID sin atributo SameSite: La falta de esta configuración hace al usuario vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[LOW] Cabecera Server expuesta: El servidor Apache revela su identidad, facilitando a un atacante la búsqueda de vulnerabilidades específicas para dicha tecnología.
[LOW] Cabecera X-Powered-By expuesta: Se detecta la versión PHP/8.3.16 en las respuestas del servidor, exponiendo detalles innecesarios del framework utilizado.
[LOW] Divulgación de rutas en robots.txt: Se hace referencia a directorios administrativos, orientando a posibles atacantes hacia áreas restringidas del sitio.