EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://fcapacidades.ue003cofopri.gob.pe	Checks	9 pruebas
Dominio	fcapacidades.ue003cofopri.gob.pe	Hallazgos	46 totales
Fecha	13 de junio de 2026 a las 03:23	Problemas	11 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 64/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 fallaron críticamente. El principal riesgo identificado es la proximidad de la expiración del certificado SSL y la ausencia casi total de cabeceras de seguridad fundamentales. Debido a estas omisiones técnicas y configuraciones incompletas, el sitio se considera actualmente vulnerable ante ataques de intermediarios e inyección de código.

Resumen de Riesgos

0	4	4	3	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	50	AVISO	Certificado expira en 5 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	67	AVISO	MoodleSession: falta SameSite
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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 50/100

Estado: AVISO

Certificado expira en 5 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- ALTO **Dias hasta expiracion**
  5 dias restantes (expira: 2026-06-17T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-06-17T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: nginx/1.18.0 (Ubuntu) — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: sameorigin
- 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://fcapacidades.ue003cofopri.gob.pe:9443/
- 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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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, Astro

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 — 67/100

Estado: AVISO

MoodleSession: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: MoodleSession — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: MoodleSession — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: MoodleSession — 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 — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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)**
  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
- 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] Certificado SSL/TLS por expirar: El certificado caduca en 5 días, lo que provocará alertas de seguridad a los usuarios y pérdida de confianza.

[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) y la ejecución de scripts maliciosos.
[HIGH] Falta de Strict-Transport-Security (HSTS): El sitio no obliga al navegador a usar conexiones HTTPS, permitiendo posibles degradaciones de seguridad.
[MEDIUM] Falta de X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría permitir que archivos cargados se interpreten como código ejecutable.
[MEDIUM] Falta de Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios, lo que puede filtrar URLs privadas.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la cámara o el micrófono a través del navegador.
[MEDIUM] Configuración de Cookie (MoodleSession): La cookie de sesión carece del atributo SameSite, aumentando el riesgo de ataques de falsificación de solicitud en sitios cruzados (CSRF).
[LOW] Exposición de cabecera de servidor: Se revela el uso de nginx/1.18.0 (Ubuntu), proporcionando información valiosa a posibles atacantes sobre la infraestructura.
[LOW] Ausencia de archivos de indexación: No se encontraron robots.txt ni sitemap.xml, lo que dificulta la gestión del rastreo por motores de búsqueda.