

EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://www.unefa.edu.ve/portal/	Checks	9 pruebas
Dominio	www.unefa.edu.ve	Hallazgos	35 totales
Fecha	29 de septiembre de 2026 a las 13:36	Problemas	9 detectados

C

67/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al portal institucional arroja una puntuación de 67/100, obteniendo una nota final de C. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 4 verificaciones exitosas, 1 advertencia y 2 fallos críticos relacionados con la privacidad y el cifrado. La ausencia de un protocolo de comunicación seguro y la falta de cabeceras de protección básicas exponen la infraestructura a diversos vectores de ataque. Por lo tanto, se concluye que el sitio es vulnerable y requiere intervenciones técnicas inmediatas para mitigar riesgos de interceptación de datos.

Resumen de Riesgos

0 CRITICO	4 ALTO	4 MEDIO	1 BAJO	26 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

Cabeceras de Seguridad	30	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
Server: Apache/2.4.10 — 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)
- INFO **X-Content-Type-Options**
Presente: nosniff
- 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: ERROR

No se pudo verificar la redireccion HTTPS

ALTO

HTTP != HTTPS redireccion

HTTP 302 — No redirige a HTTPS

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

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

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 — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

ALTO

Protocolo

El sitio no usa HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

INFO

security.txt

Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

1 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 — Envío de correo
●	INFO	Puerto 80 (HTTP) Abierto (esperado) — 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] Protocolo HTTPS ausente: El sitio opera bajo HTTP, lo que permite que toda la información transmitida sea capturada en texto plano por terceros.

[HIGH] Content-Security-Policy (CSP) ausente: La falta de esta cabecera facilita la ejecución de ataques XSS y la inyección de contenido malicioso.

[HIGH] Strict-Transport-Security (HSTS) ausente: No se obliga al navegador a usar conexiones seguras, permitiendo ataques de degradación de protocolo (Man-in-the-Middle).

[MEDIUM] Referrer-Policy ausente: No hay control sobre la información de navegación que se envía a otros dominios al seguir enlaces.

[MEDIUM] Permissions-Policy ausente: El servidor no restringe el acceso del navegador a componentes sensibles como la cámara, el micrófono o la geolocalización.

[MEDIUM] Archivos de información expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, pudiendo revelar detalles sobre la arquitectura interna.

[LOW] Cabecera de servidor expuesta: El sistema revela el uso de Apache/2.4.10, permitiendo a potenciales atacantes buscar vulnerabilidades específicas para esa versión.

[LOW] Ausencia de Robots.txt y Sitemap: La falta de estos archivos impide una indexación controlada y profesional por parte de los motores de búsqueda.