EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://portal.usenash.com/history?nashboard=%22%7B%5C%22state%5C%22%3A%7B%5C%22timezone%5C%22%3A%5C%22America%2FSanto_Domingo%5C%22%2C%5C%22viewId%5C%22%3Anull%2C%5C%22columnsOrder%5C%22%3A%5B%5C%22selection%5C%22%2C%5C%22flag%5C%22%2C%5C%22status%5C%22%2C%5C%22creation_time%5C%22%2C%5C%22delivery_pickup_time%5C%22%2C%5C%22actual_pickup_time%5C%22%2C%5C%22pickup_time%5C%22%2C%5C%22pickup_eta%5C%22%2C%5C%22pickup_location%5C%22%2C%5C%22delivery_dropoff_time%5C% … %5C%22%3Afalse%2C%5C%22actual_dropoff_time%5C%22%3Afalse%2C%5C%22dropoff_eta%5C%22%3Afalse%2C%5C%22dropoff_location%5C%22%3Atrue%2C%5C%22provider%5C%22%3Atrue%2C%5C%22driving_distance%5C%22%3Afalse%2C%5C%22delivery_dropoff_time%5C%22%3Afalse%2C%5C%22delivery_pickup_time%5C%22%3Afalse%2C%5C%22status%5C%22%3Atrue%2C%5C%22package%5C%22%3Afalse%2C%5C%22merchant%5C%22%3Afalse%2C%5C%22job_external_id%5C%22%3Afalse%2C%5C%22package_external_id%5C%22%3Afalse%2C%5C%22package_reference_id%5C%22%3Afalse%2C%5C%22provider_batch_id%5C%22%3Afalse%2C%5C%22tags%5C%22%3Afalse%2C%5C%22created_by%5C%22%3Afalse%2C%5C%22organization%5C%22%3Afalse%2C%5C%22flag%5C%22%3Afalse%2C%5C%22actions%5C%22%3Atrue%2C%5C%22custom_agents%5C%22%3Afalse%7D%2C%5C%22sortByKey%5C%22%3A%5C%22pickupTime%5C%22%2C%5C%22sortOrder%5C%22%3A%5C%22asc%5C%22%2C%5C%22pageSize%5C%22%3A50%2C%5C%22pageNumber%5C%22%3A0%2C%5C%22period%5C%22%3A%5C%22This+month%5C%22%2C%5C%22filters%5C%22%3A%7B%5C%22city%5C%22%3Anull%2C%5C%22state%5C%22%3Anull%2C%5C%22country%5C%22%3Anull%2C%5C%22optionsGroupId%5C%22%3Anull%2C%5C%22organizations%5C%22%3Anull%2C%5C%22flagStatus%5C%22%3A%5B%5D%2C%5C%22isBatch%5C%22%3Anull%2C%5C%22onlyJobsWithQuoteSelected%5C%22 … 2pickupLocationName%5C%22%3Anull%2C%5C%22pickupLocationFullNames%5C%22%3Anull%2C%5C%22pickupLocationAddress%5C%22%3Anull%2C%5C%22pickupLocationCity%5C%22%3Anull%2C%5C%22pickupLocationState%5C%22%3Anull%2C%5C%22pickupLocationCountry%5C%22%3Anull%2C%5C%22pickupStoreLocationIds%5C%22%3Anull%2C%5C%22dropoffLocationName%5C%22%3Anull%2C%5C%22dropoffLocationFullNames%5C%22%3Anull%2C%5C%22dropoffLocationAddress%5C%22%3Anull%2C%5C%22dropoffLocationCity%5C%22%3Anull%2C%5C%22dropoffLocationState%5C%22%3Anull%2C%5C%22dropoffLocationCountry%5C%22%3Anull%2C%5C%22dropoffStoreLocationIds%5C%22%3Anull%2C%5C%22creationSources%5C … null%2C%5C%22tags%5C%22%3Anull%2C%5C%22startDate%5C%22%3A%5C%222026-06-01T04%3A00%3A00.000Z%5C%22%2C%5C%22endDate%5C%22%3A%5C%222026-07-01T03%3A59%3A59.999Z%5C%22%2C%5C%22 … ames%5C%22%3Anull%2C%5C%22healthStatuses%5C%22%3Anull%2C%5C%22customEventNames%5C%22%3Anull%7D%7D%2C%5C%22version%5C%22%3A8%7D%22	Checks	9 pruebas
Dominio	portal.usenash.com	Hallazgos	46 totales
Fecha	1 de junio de 2026 a las 23:54	Problemas	8 detectados

B

89/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio portal.usenash.com ha resultado en una puntuación de 89/100 con una nota final de B. El análisis se basó en la ejecución de 9 checks pasivos, de los cuales 7 resultaron satisfactorios, 1 generó una advertencia y 1 fue calificado como fallo. Aunque la infraestructura de cifrado es excelente, se identificaron deficiencias en la configuración de cabeceras de seguridad y exposición de rutas administrativas. Se concluye que el sitio es generalmente seguro, pero presenta vulnerabilidades de configuración que deben ser mitigadas para evitar ataques dirigidos.

Resumen de Riesgos

0	1	7	0	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 dias
Cabeceras de Seguridad	55	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, X-C...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 89 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  89 dias restantes (expira: 2026-08-29T21:41:55.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-31T20:44:42.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: FALLO

Solo 3/6 presentes. Faltan: X-Frame-Options, X-Content-Type-Options, Permissions-Policy

- INFO **Content-Security-Policy**
  Presente: base-uri 'self'; script-src 'strict-dynamic' 'sha256-P+EbqY+05+V2ngxP6v31Y8bq+A9...

- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31556926
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: strict-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://portal.usenash.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31556926
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31556926 (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

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 — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] X-Frame-Options: La cabecera está ausente, lo que permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking para engañar a los usuarios.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador puede intentar predecir el tipo de contenido (MIME-sniffing), permitiendo la ejecución de scripts maliciosos camuflados.
[MEDIUM] Permissions-Policy: Falta la restricción de APIs del navegador, lo que deja expuesto el uso innecesario de funciones como la cámara, el micrófono o la geolocalización.
[MEDIUM] Paneles de login expuestos: Las rutas /wp-login.php, /administrator/ y /user/login son accesibles públicamente, aumentando el riesgo de ataques de fuerza bruta.
[MEDIUM] Archivos de información expuestos: Los archivos /readme.html y /README.txt están disponibles, lo que podría revelar versiones de software y detalles técnicos a atacantes.
[LOW] Falta de sitemap.xml: El archivo de mapa del sitio no fue detectado, lo que afecta la visibilidad de la estructura y el control de indexación.