EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.fbernardino.edu.bo/	Checks	9 pruebas
Dominio	www.fbernardino.edu.bo	Hallazgos	43 totales
Fecha	30 de junio de 2026 a las 02:11	Problemas	6 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio fbernardino.edu.bo arroja una puntuación de 85/100 con una calificación de grado B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 se marcó como fallo técnico. La infraestructura presenta una base sólida en cuanto al cifrado de datos, aunque carece de configuraciones de endurecimiento en las cabeceras de red. Se concluye que el sitio es generalmente seguro para la navegación, pero permanece vulnerable a ataques de degradación de protocolo y divulgación de información técnica.

Resumen de Riesgos

0	2	1	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 65 dias
Cabeceras de Seguridad	65	AVISO	4/6 presentes. Faltan: Strict-Transport-Security...
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	100	OK	No se encontraron cookies
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 — 100/100

Estado: OK

Certificado valido, expira en 65 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  65 dias restantes (expira: 2026-09-02T17:54:06.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-04T17:05:36.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 65/100

Estado: AVISO

4/6 presentes. Faltan: Strict-Transport-Security, Permissions-Policy

- BAJO **Server header expuesto**
  Server: ESF — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: base-uri 'self';object-src 'none';report-uri /_/view/cspreport;script-src 'repor...
- INFO **X-Frame-Options**
  Presente: DENY
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: origin
- 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://www.fbernardino.edu.bo/
- 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
- INFO **Tecnologias detectadas**
  Next.js

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 — 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 — 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] Strict-Transport-Security: La ausencia de esta cabecera impide que el servidor fuerce conexiones HTTPS de manera estricta, aumentando el riesgo de ataques Man-in-the-Middle.
[HIGH] HSTS no configurado: El mecanismo de seguridad no está activado, lo que significa que el navegador no obliga a usar exclusivamente el protocolo cifrado tras el primer contacto.
[MEDIUM] Permissions-Policy: No se han definido restricciones para las APIs del navegador, lo que teóricamente permite que elementos del sitio accedan a hardware como cámara o micrófono.
[LOW] Server header expuesto: El encabezado Server revela el uso de la tecnología ESF, proporcionando a posibles atacantes datos sobre la infraestructura subyacente para buscar exploits específicos.
[LOW] robots.txt no encontrado: La falta de este archivo dificulta el control sobre qué partes del sitio deben o no ser indexadas por motores de búsqueda.

[LOW] sitemap.xml no encontrado: La ausencia de un mapa del sitio afecta la organización del contenido y puede exponer rutas que no deberían ser prioritarias para el rastreo público.