EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://edubecas.fepade.org.sv:8012/WebEdubecas/SolicitudUniv?_gl=1*1y8cc79*_ga*MzkxMjA3TkxNTY3LjE3NzY3ODc4Mjg.*_ga_JX1BCZ9P3T*czE3NzY3ODc4MjgkbzEkZzEkdDE3NzY3ODkwMDAkajQxJGwwJGgw	Cookies	9 detectadas
Dominio	edubecas.fepade.org.sv	Hallazgos	42 totales
Fecha	21 de abril de 2026 a las 16:28	Problemas	13 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 61/100, lo que equivale a una nota de grado C. Se ejecutaron 9 checks pasivos, resultando en 4 verificaciones satisfactorias, 1 advertencia y 2 fallos principales detectados en la configuración. El sistema presenta deficiencias críticas en la implementación de protocolos de cifrado y cabeceras de protección esenciales. Debido a la ausencia de una conexión SSL verificable y la falta de políticas de seguridad en el servidor, se concluye que el sitio es actualmente vulnerable. Los datos de los usuarios podrían estar expuestos a interceptaciones o ataques de inyección.

Resumen de Riesgos

1	5	3	4	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	67	AVISO	ASP.NET_SessionId: falta Secure
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	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

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: Microsoft-IIS/10.0 — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — 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: ERROR
No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS

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**
  ASP.NET

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
ASP.NET_SessionId: falta Secure

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: ASP.NET_SessionId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: ASP.NET_SessionId — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP

- INFO **Cookie: ASP.NET_SessionId — SameSite**
  SameSite=lax

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

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

[CRITICAL] Conexion SSL: No se pudo establecer una conexion segura SSL/TLS, impidiendo el cifrado del trafico.
[HIGH] HTTP a HTTPS redireccion: El servidor responde con un codigo 200 en HTTP, lo que indica que no fuerza el uso de conexiones seguras.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecucion de ataques XSS y la inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: No esta implementada, dejando el sitio vulnerable a ataques de clickjacking que pueden engañar al usuario.
[HIGH] Strict-Transport-Security: No existe una politica HSTS para garantizar que el navegador solo se comunique mediante HTTPS.
[HIGH] Cookie ASP.NET_SessionId: Falta el flag Secure, permitiendo que la cookie de sesion se transmita por canales no cifrados.
[MEDIUM] X-Content-Type-Options: El servidor no previene el MIME-type sniffing, lo que podria llevar a la ejecucion de archivos malinterpretables.
[MEDIUM] Referrer-Policy: No se controla la informacion de referencia enviada a otros sitios, lo que puede filtrar URLs internas.
[MEDIUM] Permissions-Policy: Falta la restriccion de acceso a funciones sensibles del navegador como la camara o el microfono.
[LOW] Server header expuesto: Se revela la version Microsoft-IIS/10.0, facilitando a los atacantes la busqueda de exploits especificos.

[LOW] X-Powered-By expuesto: Se muestra el uso de ASP.NET, revelando detalles tecnologicos innecesarios sobre el backend.
[LOW] Archivos robots.txt y sitemap.xml: No se encontraron estos archivos, dificultando la indexacion correcta y la gestion del rastreo.