EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ucenfotec.ac.cr/ecommerce/tecnologias-de-informacion/?utm_source=google&utm_medium=cpc&utm_campaign=aprendizaje_continuo&utm_content=cloud_computing&gad_source=1&gad_campaignid=23574519306&gbraid=0AAAApGwjlyG175Q2aX1tDJT-1z9lePQM&gclid=CjwKCAjwwdbPBhBgEiwAxBRA4So9TU7HIZMWE5JiO39UfymTccQ-jznRnRUj4rBA8ABF2YcCpBmk1RoCdQEQAvD_BwE	Checks	9 pruebas
Dominio	ucenfotec.ac.cr	Hallazgos	41 totales
Fecha	2 de mayo de 2026 a las 07:24	Problemas	10 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación técnica de 61/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos críticos relacionados con la configuración del servidor. El portal presenta una ausencia total de cabeceras de seguridad y deficiencias en la redirección de tráfico cifrado. Debido a la carencia de protecciones básicas contra ataques comunes como XSS o Clickjacking, se concluye que el sitio es actualmente vulnerable. Es imperativo implementar las medidas correctivas para elevar el estándar de protección de los datos de los usuarios.

Resumen de Riesgos

0	5	3	2	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 50 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 50 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  50 dias restantes (expira: 2026-06-21T06:09:50.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-23T06:09:51.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

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

- 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: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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

- 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 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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 — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Cerrado — 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

[ALTA] Ausencia de Content-Security-Policy: La falta de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[ALTA] Ausencia de X-Frame-Options: El sitio es vulnerable a ataques de Clickjacking, permitiendo que atacantes embeban el portal en marcos invisibles para engañar a los usuarios.
[ALTA] Falta de Strict-Transport-Security (HSTS): No se obliga al navegador a usar conexiones HTTPS, permitiendo posibles degradaciones de seguridad en la comunicación.
[ALTA] Error en Redirección HTTPS: El servidor no redirige automáticamente el tráfico HTTP a HTTPS y responde con un código 403, lo que interrumpe la experiencia segura del usuario.
[MEDIA] Ausencia de X-Content-Type-Options: El sitio queda expuesto a ataques de MIME-type sniffing, donde el navegador podría interpretar archivos de forma incorrecta y peligrosa.
[MEDIA] Ausencia de Referrer-Policy: No se controla qué información de procedencia se envía a otros sitios, lo que podría filtrar datos de navegación internos.
[MEDIA] Ausencia de Permissions-Policy: No se restringe el acceso de las APIs del navegador como la cámara o el micrófono, aumentando la superficie de riesgo.

[BAJA] Falta de archivos de indexación: La ausencia de robots.txt y sitemap.xml dificulta la correcta gestión del rastreo por parte de motores de búsqueda.