EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.esic.edu/idiomas/	Checks	9 pruebas
Dominio	www.esic.edu	Hallazgos	51 totales
Fecha	24 de septiembre de 2026 a las 09:54	Problemas	17 detectados

D

55/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría de ciberseguridad, el sitio web ha obtenido una puntuación de 55/100, lo que resulta en una calificación de grado D. Se ejecutaron un total de 9 controles pasivos, de los cuales 6 fueron satisfactorios y 3 resultaron en fallo crítico por deficiencias de configuración. No se realizó un pentest activo, por lo que los resultados se limitan a la superficie de exposición externa y cabeceras. Debido a la ausencia de políticas de seguridad esenciales y a la falta de redirección HTTPS obligatoria, el sitio se clasifica actualmente como vulnerable ante ataques de interceptación de datos y suplantación.

Resumen de Riesgos

0	7	6	4	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 44 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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 44 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  44 dias restantes (expira: 2026-11-06T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-06T00:00:00.000Z
- 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

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.0.0 — 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: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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**
  PHP/8.0.0

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1932 bytes)
- INFO **Reglas robots.txt**
  27 Disallow, 18 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, ? URLs
- 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] Redirección HTTPS ausente: El servidor responde con un código 200 en HTTP en lugar de redirigir a HTTPS, permitiendo comunicaciones no cifradas.
[HIGH] HSTS no configurado: La falta de la cabecera Strict-Transport-Security impide que el navegador fuerce conexiones seguras permanentemente.
[HIGH] Falta de Content-Security-Policy: El sitio es vulnerable a ataques de inyección de contenido y Cross-Site Scripting (XSS) al no definir fuentes de confianza.
[HIGH] Falta de X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.
[HIGH] Cookie PHPSESSID sin flag HttpOnly: La cookie de sesión es accesible mediante scripts, lo que permite el robo de identidad en caso de un ataque XSS.
[HIGH] Cookie PHPSESSID sin flag Secure: El identificador de sesión se transmite a través de conexiones no cifradas, exponiéndolo a interceptación en redes públicas.
[MEDIUM] Cookie PHPSESSID sin flag SameSite: La ausencia de este atributo incrementa el riesgo de ataques de falsificación de solicitudes entre sitios (CSRF).
[MEDIUM] Falta de X-Content-Type-Options: El sitio no previene el MIME-type sniffing, lo que podría permitir la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Archivo README.txt accesible: La exposición pública de este archivo puede revelar información sobre el software utilizado y facilitar ataques dirigidos.
[MEDIUM] Panel de login expuesto: La ruta /user/login es accesible públicamente, lo que permite ataques de fuerza bruta contra cuentas administrativas.
[MEDIUM] Falta de Referrer-Policy y Permissions-Policy: No se controla la información de origen enviada ni se restringen las APIs del navegador como la cámara o micro.
[LOW] Server header expuesto: El encabezado revela el uso de nginx, proporcionando pistas sobre la infraestructura a potenciales atacantes.
[LOW] X-Powered-By expuesto: Se revela explícitamente el uso de PHP/8.0.0, permitiendo buscar vulnerabilidades específicas para esa versión.
[LOW] Rutas sensibles en robots.txt: Se mencionan directorios como "admin" y "config", exponiendo la estructura interna del sitio a escaneos malintencionados.