EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.utecvirtual.edu.sv/	Checks	9 pruebas
Dominio	www.utecvirtual.edu.sv	Hallazgos	44 totales
Fecha	7 de septiembre de 2026 a las 01:00	Problemas	12 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio analizado ha obtenido una puntuación exacta de 60/100, lo que equivale a una nota C. De los 9 checks pasivos ejecutados, se han identificado 5 resultados satisfactorios, 1 advertencia y 2 fallos críticos relacionados con la configuración de seguridad del servidor y el manejo de sesiones. La evaluación revela una carencia total de cabeceras de protección web y deficiencias en la seguridad de las cookies, además de la presencia de contenido mixto. Concluyo que el sitio es actualmente vulnerable ante ataques de interceptación de sesiones e inyección de contenido, requiriendo atención técnica inmediata.

Resumen de Riesgos

0	5	6	1	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 95 dias
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	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	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 95 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  95 dias restantes (expira: 2026-12-10T15:51:13.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-10T15:51:13.000Z
- 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: Apache/2.4.58 (Ubuntu) — Revela tecnologia del servidor

- 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.)

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 — 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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.utec.edu.sv/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.utec.edu.sv/Inicio/Publicaciones

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (67 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 1 Allow
- INFO **sitemap.xml**
  Presente, 13 URLs
- 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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) y otras inyecciones de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a ataques de clickjacking que podrían engañar a los usuarios para realizar acciones no deseadas.
[HIGH] Strict-Transport-Security: No se implementa la directiva HSTS, lo que impide forzar de manera segura el uso de conexiones HTTPS en todo momento.
[HIGH] Cookie PHPSESSID sin flags HttpOnly y Secure: La sesión es accesible mediante scripts del lado del cliente y puede ser transmitida por canales no cifrados, facilitando el robo de identidad.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador realice MIME-type sniffing, aumentando el riesgo de ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la cantidad de información que el navegador envía al navegar desde este sitio hacia otros enlaces externos.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.

[MEDIUM] Contenido Mixto: Se detectaron dos recursos cargados mediante protocolo HTTP inseguro dentro del entorno HTTPS, lo que degrada la seguridad de la conexión.
[MEDIUM] Cookie PHPSESSID sin atributo SameSite: La falta de esta configuración expone a los usuarios a posibles ataques de falsificación de petición en sitios cruzados (CSRF).
[LOW] Server header expuesto: El servidor revela el uso de Apache/2.4.58 sobre Ubuntu, proporcionando información técnica valiosa para un atacante.