EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://campus.fcytcdelu.uader.edu.ar/my/	Checks	9 pruebas
Dominio	campus.fcytcdelu.uader.edu.ar	Hallazgos	49 totales
Fecha	2 de junio de 2026 a las 01:48	Problemas	13 detectados

C

69/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 69/100, lo que resulta en una calificación de grado C. Se completaron 9 verificaciones de tipo pasivo, obteniendo 5 resultados satisfactorios, 1 advertencia por contenido mixto y 3 fallos críticos en la configuración. El análisis revela que, aunque el cifrado de transporte es robusto, existen deficiencias importantes en la protección de las sesiones de usuario y en la implementación de cabeceras de seguridad. Debido a la exposición de información técnica y al manejo inseguro de cookies, el sitio se considera vulnerable ante ataques de interceptación y secuestro de sesión.

Resumen de Riesgos

0	3	6	4	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 62 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	MoodleSession: falta HttpOnly; MoodleSession: fa...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 62 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  62 dias restantes (expira: 2026-08-03T09:29:04.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-05T09:29:05.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, 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/7.2.34 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: sameorigin
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://campus.fcytcdelu.uader.edu.ar/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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/7.2.34

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

Seguridad de Cookies — 0/100

Estado: FALLO

MoodleSession: falta HttpOnly; MoodleSession: falta Secure; MoodleSession: falta SameSite

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

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.example.com/support.php

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

[ALTA] Falta de Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso en el navegador del usuario.
[ALTA] Cookies de sesión inseguras: La cookie MoodleSession carece de los atributos HttpOnly y Secure, lo que permite que sea robada mediante scripts o interceptada en conexiones no cifradas.
[MEDIA] Falta de cabecera X-Content-Type-Options: Al no estar presente, el navegador podría intentar interpretar archivos como un tipo MIME diferente, facilitando la ejecución de código no autorizado.
[MEDIA] Vulnerabilidad a CSRF en cookies: La cookie de sesión no implementa el atributo SameSite, dejando a los usuarios expuestos a ataques de falsificación de peticiones en sitios cruzados.
[MEDIA] Archivo README.txt expuesto: Este archivo es accesible de forma pública y puede contener detalles sobre la tecnología instalada y versiones de software que facilitan ataques dirigidos.
[MEDIA] Contenido Mixto: Se detectó la carga de un recurso mediante el protocolo inseguro HTTP dentro de una página protegida por HTTPS, lo que debilita la integridad de la sesión.
[MEDIA] Ausencia de Referrer-Policy y Permissions-Policy: No se controla qué información de procedencia se envía a otros sitios ni se restringen funciones sensibles del navegador como la cámara o el micrófono.
[BAJA] Exposición de cabeceras de servidor: El sistema revela el uso de nginx y la versión específica de PHP (7.2.34), proporcionando datos valiosos para que un atacante busque vulnerabilidades conocidas.
[BAJA] Ausencia de archivos de control de rastreo: No se encontraron los archivos robots.txt ni sitemap.xml, lo que afecta la visibilidad controlada y la auditoría de rutas del sitio.