EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://intranet.unes.edu.ve/comedor/administrador/val_sesion.php	Checks	9 pruebas
Dominio	intranet.unes.edu.ve	Hallazgos	38 totales
Fecha	20 de junio de 2026 a las 10:21	Problemas	12 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio web arroja una puntuación de 59/100, lo que corresponde a una calificación de grado D. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo como resultado 4 verificaciones correctas, 1 advertencia y 2 fallos críticos, además de errores por tiempo de espera en ciertos módulos. La ausencia de protocolos de cifrado y la falta de cabeceras de seguridad exponen la plataforma a riesgos de interceptación de datos e inyección de código. Debido a la exposición de tecnologías obsoletas y la falta de protecciones básicas, se concluye que el sitio es vulnerable.

Resumen de Riesgos

0	5	3	4	26
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

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	100	OK	No se encontraron cookies
Contenido Mixto	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

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/2.2.22 (Debian) — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/5.3.3-7+squeeze19 — 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

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/5.3.3-7+squeeze19

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 — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO **Protocolo**
  El sitio no usa 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

[HIGH] Protocolo HTTPS ausente: El sitio opera bajo HTTP y no redirige a una conexión cifrada, lo que permite la captura de datos en tránsito.
[HIGH] Content-Security-Policy faltante: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[HIGH] X-Frame-Options faltante: El sitio es vulnerable a ataques de Clickjacking, permitiendo que sea embebido en marcos externos maliciosos.
[HIGH] Strict-Transport-Security faltante: No se aplica la política HSTS, dejando a los usuarios expuestos a ataques de degradación de SSL/TLS.
[MEDIUM] X-Content-Type-Options faltante: El navegador podría interpretar archivos de forma incorrecta (MIME sniffing), facilitando la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy faltante: No existe control sobre la información de navegación que se envía a otros dominios mediante el encabezado Referer.
[MEDIUM] Permissions-Policy faltante: No se restringe el acceso del navegador a funcionalidades sensibles como la cámara, el micrófono o la ubicación.
[LOW] Server header expuesto: Se revela el uso de Apache/2.2.22 (Debian), una versión antigua que facilita el reconocimiento de vulnerabilidades conocidas.
[LOW] X-Powered-By expuesto: Se divulga el uso de PHP/5.3.3-7, una versión obsoleta que permite a atacantes dirigir exploits específicos al lenguaje.
[LOW] Archivos robots.txt y sitemap.xml no encontrados: La falta de estos archivos dificulta la gestión del rastreo y puede indicar una configuración de servidor incompleta.