EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://bienestaruniversitario.unasam.edu.pe/login	Checks	9 pruebas
Dominio	bienestaruniversitario.unasam.edu.pe	Hallazgos	49 totales
Fecha	12 de julio de 2026 a las 08:39	Problemas	13 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio bienestaruniversitario.unasam.edu.pe arroja una puntuación de 65/100, lo que corresponde a una calificación de nota C. Se ejecutaron 9 checks pasivos, identificando 4 resultados satisfactorios, 4 advertencias y 1 fallo crítico en las configuraciones globales. La ausencia de cabeceras de seguridad y la gestión deficiente de las cookies de sesión representan riesgos significativos para la integridad de los datos. En su estado actual, se concluye que el sitio es vulnerable ante ataques de interceptación y suplantación.

Resumen de Riesgos

0	7	4	2	36
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	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	50	AVISO	XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Se...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

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: 2026-08-31T13:32:37.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-02T12:35:00.000Z
- 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: cloudflare — 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.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://bienestaruniversitario.unasam.edu.pe/
- 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

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 — 50/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Secure; dbu_unasam_session: falta Secure

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: XSRF-TOKEN — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: dbu_unasam_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: dbu_unasam_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: dbu_unasam_session — SameSite**
  SameSite=lax

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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

MEDIO **Puerto 8080 (HTTP-Alt)**

ABIERTO — Servidor web alternativo / proxy

INFO **Puerto 27017 (MongoDB)**

Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: Falta — La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Falta — El sitio es vulnerable a ataques de clickjacking, permitiendo que un atacante cargue el portal en un marco invisible.
[HIGH] Strict-Transport-Security: Falta — No se obliga al navegador a usar conexiones cifradas, facilitando ataques de degradación de protocolo (SSL Stripping).
[HIGH] Cookie XSRF-TOKEN: Falta HttpOnly y Secure — El token puede ser extraído mediante scripts maliciosos y transmitido por canales no cifrados.
[HIGH] Cookie dbu_unasam_session: Falta flag Secure — La sesión del usuario corre el riesgo de ser interceptada al no estar restringida solo a conexiones HTTPS.
[MEDIUM] Puerto 8080 (HTTP-Alt): ABIERTO — La exposición de un puerto alternativo incrementa la superficie de ataque y puede revelar servicios internos vulnerables.
[MEDIUM] X-Content-Type-Options: Falta — Permite que el navegador intente adivinar el tipo de contenido, lo que facilita la ejecución de archivos maliciosos (MIME-sniffing).
[MEDIUM] Referrer-Policy: Falta — No se controla la información de navegación que se envía a sitios externos cuando un usuario hace clic en un enlace.
[MEDIUM] Permissions-Policy: Falta — El sitio no restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la ubicación.
[LOW] Server header expuesto: Server: cloudflare — La infraestructura revela información tecnológica que ayuda a un atacante en la fase de reconocimiento.
[LOW] sitemap.xml: No encontrado — La falta de este archivo dificulta la auditoría de rutas y la correcta indexación de la estructura del sitio.