

# Escanear Vulnerabilidades

Informe de Seguridad Web

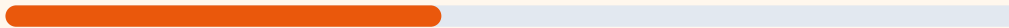
URL https://sambies.com/campus  
Dominio sambies.com  
Fecha 11 de julio de 2026 a las 00:35

Checks 9 pruebas  
Hallazgos 30 totales  
Problemas 9 detectados

# D

## 43/100

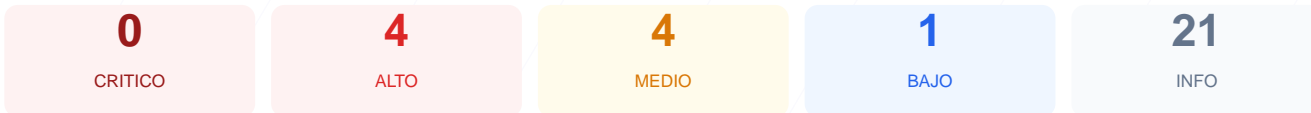
puntos de seguridad



### RESUMEN EJECUTIVO

El análisis de seguridad realizado en sambies.com/campus arroja una puntuación de 43/100, lo que equivale a una nota D. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo como resultado 1 validación correcta, 2 advertencias y 1 fallo crítico de configuración. Se han identificado múltiples carencias en las políticas de seguridad del servidor y una exposición innecesaria de puertos. Debido a la ausencia de protecciones esenciales contra ataques de inyección y suplantación, se concluye que el sitio es vulnerable y requiere intervención inmediata.

### Resumen de Riesgos



### Resumen de Checks

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
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

### 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 tecnología 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://sambies.com/

- **ALTO** **HSTS (Strict-Transport-Security)**  
HSTS no configurado — El navegador no fuerza HTTPS
- **INFO** **Respuesta HTTPS**  
HTTPS responde con status 503

## 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

## 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: La ausencia de esta cabecera permite la ejecución de ataques XSS y la inyección de contenido malicioso en el navegador del usuario.

[HIGH] X-Frame-Options: La falta de esta protección hace al sitio susceptible a ataques de clickjacking, permitiendo que la interfaz sea embebida en marcos externos.

[HIGH] Strict-Transport-Security: No se ha configurado el protocolo HSTS, lo que impide forzar conexiones cifradas y facilita ataques de degradación de SSL.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo aumenta la superficie de ataque y sugiere la presencia de servicios de administración o proxies desprotegidos.

[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría interpretar archivos de forma incorrecta mediante MIME-type sniffing.

[MEDIUM] Referrer-Policy: No existe una política definida para controlar cuánta información de navegación se comparte con sitios de terceros.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.

[LOW] Server header expuesto: El encabezado de respuesta revela el uso de Cloudflare, proporcionando información técnica sobre la infraestructura a posibles atacantes.

[INFO] Respuesta HTTPS inestable: El servidor responde con un código de estado 503 durante las conexiones cifradas, indicando problemas de disponibilidad.