

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://websecgen.unmsm.edu.pe/carne/carne.aspx
Dominio websecgen.unmsm.edu.pe
Fecha 18 de mayo de 2026 a las 03:50

Checks 9 pruebas
Hallazgos 13 totales
Problemas 1 detectados

A

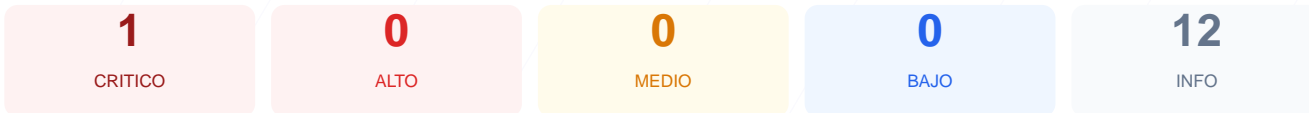
100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 100/100 con una calificación de nota A. Se ejecutaron un total de 9 checks pasivos, resultando 1 de ellos satisfactorio y registrando 0 advertencias y 0 fallos de seguridad. La ausencia de puertos abiertos expuestos contribuye significativamente a este resultado positivo. En base a los datos obtenidos y la calificación recibida, el sitio se concluye como seguro bajo los parámetros de la auditoría pasiva. No se detectaron vectores de ataque inmediatos que comprometan la integridad de la plataforma en este nivel de inspección.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
No se pudo establecer conexion SSL/TLS

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 autentificación 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

No se detectaron vulnerabilidades durante el escaneo pasivo. Debido a que el pentest activo no fue ejecutado, no se han identificado hallazgos adicionales como CWEs, endpoints de API descubiertos o subdominios expuestos. El sistema mantiene un registro de cero fallos en los puntos de control evaluados.