EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ivap.ejgv.euskalsarea.eus	Checks	9 pruebas
Dominio	ivap.ejgv.euskalsarea.eus	Hallazgos	15 totales
Fecha	26 de mayo de 2026 a las 06:00	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ivap.ejgv.euskalsarea.eus arroja una puntuación exacta de 73/100, lo que equivale a una nota de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 1 validación exitosa y 1 fallo confirmado relacionado con la estructura del sitio. Debido a la imposibilidad de verificar parámetros críticos como el cifrado SSL y las cabeceras de respuesta, el sistema muestra debilidades técnicas que impiden garantizar una navegación protegida. En su estado actual, el sitio se considera vulnerable debido a inconsistencias en sus configuraciones de seguridad perimetral.

Resumen de Riesgos

1	0	0	2	12
CRITICO	ALTO	MEDIO	BAJO	INFO

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
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
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

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder
- BAJO **sitemap.xml**
  Error al acceder

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

[CRITICAL] Fallo de conexión SSL/TLS: No se pudo establecer una conexión segura con el servidor, lo que impide cifrar la información intercambiada entre el usuario y el dominio.
[LOW] Ausencia de archivo robots.txt: El error al acceder a este archivo indica que no hay directivas claras para los rastreadores, lo que puede exponer rutas sensibles involuntariamente.
[LOW] Ausencia de sitemap.xml: La falta de este recurso dificulta la auditoría de la estructura del sitio y el control de los endpoints publicados.
[INFO] Error de verificación de cabeceras: No se detectaron políticas de seguridad activa, lo que suele estar vinculado a la exposición frente a ataques de Cross-Site Scripting y Clickjacking.