# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://arquitectotecnicofj.es | Checks | 9 pruebas |
| Dominio | arquitectotecnicofj.es | Hallazgos | 20 totales |
| Fecha | 12 de mayo de 2026 a las 04:32 | Problemas | 9 detectados |

F

20/100

puntos de seguridad

## RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada sobre el activo digital ha resultado en una puntuación crítica de 20/100, obteniendo una calificación de grado F. El análisis de los checks pasivos revela deficiencias severas en la configuración de seguridad, con un fallo crítico en la implementación de cabeceras y una advertencia por exposición de servicios. Se detectaron múltiples errores por tiempo de espera en el escaneo, lo que indica inestabilidad o problemas de respuesta en la infraestructura del servidor. La ausencia total de mecanismos de protección modernos y el uso de protocolos obsoletos comprometen la integridad de la plataforma. Se concluye que el sitio es vulnerable y presenta un riesgo alto para la continuidad del servicio y la privacidad de los datos.

## Resumen de Riesgos

| 0 | 4 | 3 | 2 | 11 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| Cabeceras de Seguridad | 0 | FALLO | Solo 0/6 presentes. Faltan: Content-Security-Pol... |
| Puertos Abiertos | 60 | AVISO | 1 puerto(s) potencialmente riesgoso(s): 21 (FTP) |

## 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: nginx — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.4.33, PleskLin — 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.)

## Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- 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] Content-Security-Policy: Falta esta cabecera esencial para prevenir ataques de inyección de contenido y XSS.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite ataques de clickjacking que pueden engañar a los usuarios.
[HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones seguras HTTPS, dejando el sitio vulnerable a ataques de degradación de SSL.
[HIGH] Puerto 21 (FTP): El servicio FTP está abierto y permite la transferencia de archivos sin cifrado, exponiendo credenciales en texto plano.
[MEDIUM] X-Content-Type-Options: Falta la protección contra el olfateo de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a terceros, lo que puede filtrar URLs privadas.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso no autorizado a funciones como la cámara o el micrófono.
[LOW] Server header expuesto: El servidor revela el uso de nginx, facilitando a posibles atacantes la búsqueda de vulnerabilidades específicas para esa tecnología.
[LOW] X-Powered-By expuesto: Se detecta el uso de PHP/7.4.33 y Plesk, revelando versiones exactas de software que pueden tener exploits conocidos.