HERMES SECURITY

Security Audit Report



● MEDIO

Dominio analizado:	test-domain-12345.com
Fecha del informe:	17 de noviembre de 2026
Tipo de análisis:	Auditoría de seguridad externa OSINT
Clasificación:	CONFIDENCIAL - Solo para el destinatario

Hermes Security | cyberdefense.valencia@proton.me | cybersofia.tech

Confidencialidad: Este informe contiene información sensible.

Índice de Contenidos

Resumen Ejecutivo

Panorama Visual

Resultados por Módulo

Cadena de Ataque Potencial

Matriz de Priorización

Evidencia Visual

Recomendaciones

Verificación Independiente

Alcance del Servicio

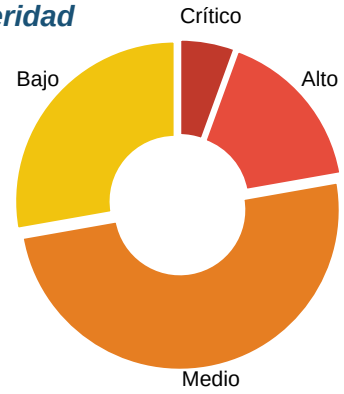
Resumen Ejecutivo

Score Global: **62/100** | Riesgo: **MEDIO**
Este informe presenta los resultados del análisis de seguridad externo realizado sobre el dominio **test-domain-12345.com**. Se han ejecutado **19 módulos**: Attack Surface, Subdomain Discovery, Subdomain Takeover, CMS Detection, Tech Fingerprint, Robots.txt Exposure, Email Security, SSL/TLS, Security Headers, WAF Detection, Threat Intelligence, Recon Pipeline, Certificados TLS, CDN / WAF y más. El score global de 62/100 indica una postura de seguridad mejorable.

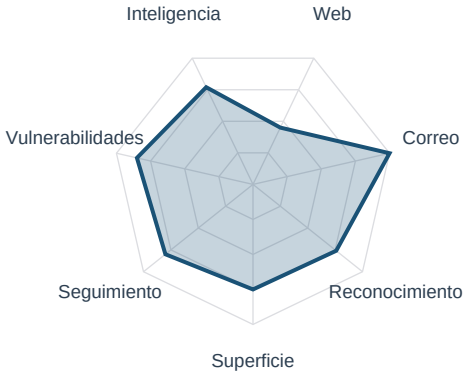
Alcance: 19 módulos del arsenal no se ejecutaron en esta pasada (Reconocimiento JS (katana), Parámetros ocultos (arjun), Breach Exposure, Breach Exposure (Free), WHOIS, Typosquatting, Directory Bruteforce, Nuclei Scanner…). Lo que no aparece aquí no fue evaluado, y por tanto no debe interpretarse como correcto.

Panorama Visual

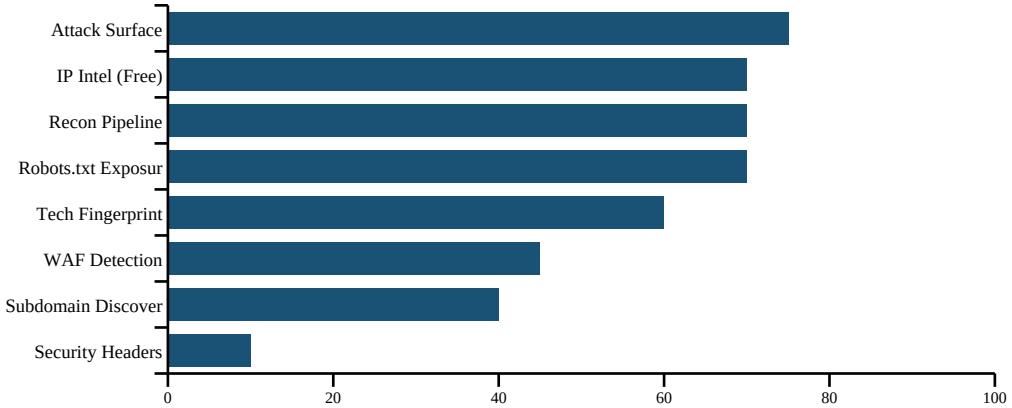
Distribución de Hallazgos por Severidad



Salud por Sector



Módulos con Score más Bajo (Prioritarios)



Resultados por Módulo

Módulo	Score	Estado	Alertas	Hallazgo Principal
Superficie				
Attack Surface	75/100	Regular	2 Med	Puerto 80 (HTTP) abierto - verifique que redirige a HTTPS
Reconocimiento				
Subdomain Discovery	40/100	Critico	2 Med	Descubiertos 23 subdominios
Subdomain Takeover	90/100	Bueno	1 Alta	No se detectaron CNAMEs colgantes en los subdominios analizados
CMS Detection	80/100	Bueno	1 Total	No se detecto un CMS estandar (WordPress/Joomla/Drupal/...). Revisar si es aplicacion a...
Tech Fingerprint	60/100	Regular	1 Med	No se identificaron tecnologias claras
Robots.txt Exposure	70/100	Regular	1 Med	robots.txt presente con 1 regla(s); ninguna sensible
Recon Pipeline	70/100	Regular	29 Total	29 subs · 29 live · 29 URLs
Certificados TLS	100/100	Bueno	--	29 hosts · 2 certs · 0 caducados · 0 autofirmados · 0 caducan pronto
CDN / WAF	90/100	Bueno	--	aws (29)
ASN / Proveedor	85/100	Bueno	1 Total	AS16509 AMAZON-02 - Amazon.com, Inc., US · 2 IPs
DNS History (Free)	80/100	Bueno	2 Total	16 subdominio(s) descubiertos historicamente (crt.sh + HackerTarget + RapidDNS)
Correo				
Email Security	100/100	Bueno	--	SPF/DKIM/DMARC correctos
Web				
SSL/TLS	80/100	Bueno	1 Crit	HSTS no detectado
Security Headers	10/100	Critico	1 Med	Faltan 7 cabeceras de seguridad: Strict-Transport-Security, Content-Security-Policy, X-...
WAF Detection	45/100	Critico	1 Total	No se detecto WAF conocido: el objetivo depende de proteccion propia
Vulnerabilidades				
Shodan InternetDB	85/100	Bueno	1 Med	NOERROR: ip_no_indexada_en_shodan
Inteligencia				
Threat Intelligence	85/100	Bueno	1 Alta	Sin coincidencias con feeds IOC (Feodo C2, mining pools)
IP Intel (Free)	70/100	Regular	1 Total	No se pudo geolocalizar ninguna IP

No ejecutados en este perfil (19): Reconocimiento JS (katana), Parámetros ocultos (arjun), Breach Exposure, Breach Exposure (Free), WHOIS, Typosquatting, Typosquat Avanzado, Photon Crawler y 11 más. Actívalos y vuelve a lanzar el análisis para incluirlos en el informe.

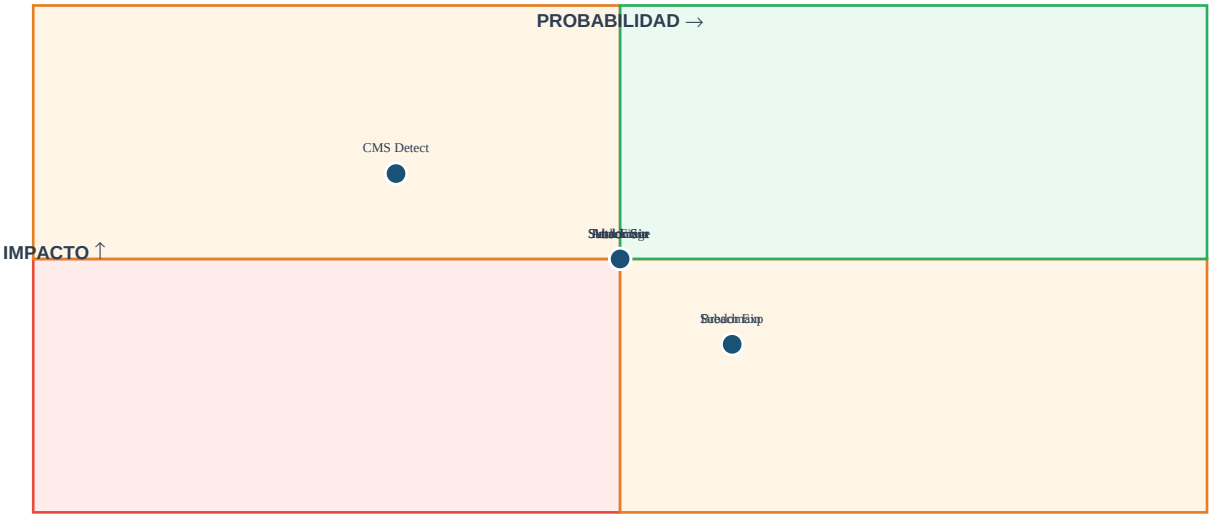
Cadena de Ataque Potencial

Secuencia de explotación más probable a partir de los hallazgos detectados:



Matriz de Priorización

Posición de los hallazgos según su impacto potencial y probabilidad de explotación:



Evidencia Visual

Captura real del estado actual del objetivo. Esta evidencia permite verificar de forma independiente los hallazgos del análisis.

EVIDENCIA — Headers HTTP devueltos por el servidor/CDN

Content-Type:	text/html
Date:	Tue, 17 Nov 2026 13:03:20 GMT
Content-Length:	114

Firewall Web (WAF)

■■ No se detectó WAF conocido — verificar protección del sitio

Recomendaciones

Prioridad	Acción Recomendada	Módulo
■ Media	Puerto 80 (HTTP) abierto - verifique que redirige a HTTPS	Attack Surface
■ Media	Subdominios potencialmente sensibles detectados: dev.test-domain-12345.com, api.test-domain-12345.com	Attack Surface
■ Media	Revisar cada subdominio descubierto; los de dev/staging/api deberian requerir autenticacion y no estar en internet publi	Subdomain Discovery
■ Baja	Si es aplicacion a medida, asegurar hardening especifico del framework	CMS Detection
■ Media	robots.txt presente con 1 regla(s); ninguna sensible	Robots.txt Exposure
■ Crítica	Habilitar HSTS	SSL/TLS
■ Crítica	Actualizar suite de cifrado	SSL/TLS
■ Media	Implementar Strict-Transport-Security: HSTS fuerza HTTPS y evita downgrade	Security Headers
■ Media	Implementar Content-Security-Policy: CSP mitiga XSS e inyeccion	Security Headers
■ Media	Implementar X-Frame-Options: Previene clickjacking	Security Headers
■ Media	Implementar X-Content-Type-Options: Evita MIME sniffing	Security Headers
■ Baja	Considerar un WAF/CDN de borde (Cloudflare, AWS WAF) para mitigar DDoS, scraping y ataques web automatizados	WAF Detection
■ Media	29 hosts vivos - superficie amplia, priorizar auditoria de los servicios expuestos	Recon Pipeline
■ Baja	Ninguna fuente respondio. Revisa conexion y rate limits. IP-API se rompe si excedes 45 req/min.	IP Intel (Free)
■ Baja	Verificar que cada subdominio sigue vivo (pipeline_recon los probea)	DNS History (Free)
■ Baja	Wayback URLs pueden revelar paginas historicas con informacion sensible (debug endpoints, paneles admin antiguos)	DNS History (Free)

Verificación Independiente

SSL Labs | MXToolbox | HaveIBeenPwned

Alcance del Servicio

Este informe constituye un diagnóstico de seguridad externa basado en fuentes públicas y herramientas técnicas automatizadas. Hermes Security se especializa en detección y monitorización continua de vulnerabilidades, ofreciendo dos niveles de ayuda:

1. **Correcciones directas:** problemas de configuración DNS y correo (SPF, DKIM, DMARC) y cabeceras de seguridad web, con acceso al panel de gestión del cliente.

2. **Coordinación con el proveedor de hosting:** problemas de infraestructura del servidor (firewall, certificados), facilitando un diagnóstico detallado para su revisión.

Hermes Security
Contacto: cyberdefense.valencia@proton.me
cybersofia.tech — nuestros servicios y auditorías
Autor: Svetoslav Atanasov Dubarov (NIE Y5597333K)
© 2026 Hermes Security. Todos los derechos reservados.
Confidencialidad: Este informe es confidencial y está dirigido únicamente al destinatario.