

# Reporte Técnico de Seguridad

Evaluación de Vulnerabilidades

**Workspace:** kopernicus.tech

**Fecha:** 11 de December, 2025

**Hora:** 19:06

# Resumen Ejecutivo

Puntuación de Riesgo Global

2.6/10

LOW

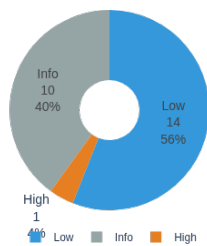
Se realizó una evaluación de seguridad integral de **kopernicus.tech**. El análisis identificó **25 hallazgos** de severidad variable.

# Estadísticas del Escaneo

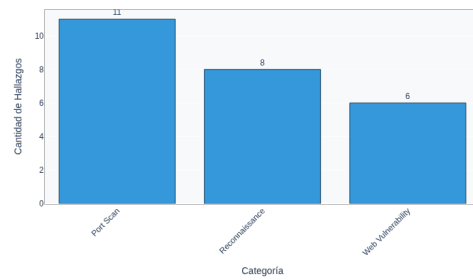
## Visualizaciones



Distribución de Hallazgos por Severidad



Hallazgos por Categoría



CRÍTICAS	ALTAS	MEDIAS	BAJAS/INFO
0	1	0	24

Métrica	Valor
Total de Hallazgos	25
Archivos Procesados	0
Targets Únicos	10
Herramientas Utilizadas	N/A
Tiempo de Generación	0.00 segundos

## Hallazgos Críticos y Altos

**Nikto: /cli/: PHP include error may indicate local or remote file inclusion is possible.**

HIGH

**Target:** kopernicus.tech:80

/cli/: PHP include error may indicate local or remote file inclusion is possible.

# Hallazgos Detallados por Categoría

## Reconnaissance

Total de hallazgos en esta categoría: 8

### Subdomain: **assurant.kopernicus.tech**

INFO

**Target:** assurant.kopernicus.tech

Discovered subdomain through reconnaissance

### Subdomain: **fravega.kopernicus.tech**

INFO

**Target:** fravega.kopernicus.tech

Discovered subdomain through reconnaissance

### Subdomain: **kopernicus.tech**

INFO

**Target:** kopernicus.tech

Discovered subdomain through reconnaissance

### Subdomain: **macro.kopernicus.tech**

INFO

**Target:** macro.kopernicus.tech

Discovered subdomain through reconnaissance

### Subdomain: **www.assurant.kopernicus.tech**

INFO

**Target:** `www.assurant.kopernicus.tech`

Discovered subdomain through reconnaissance

### Subdomain: **www.fravega.kopernicus.tech**

INFO

**Target:** `www.fravega.kopernicus.tech`

Discovered subdomain through reconnaissance

### Subdomain: **www.kopernicus.tech**

INFO

**Target:** `www.kopernicus.tech`

Discovered subdomain through reconnaissance

### Subdomain: **www.macro.kopernicus.tech**

INFO

**Target:** `www.macro.kopernicus.tech`

Discovered subdomain through reconnaissance

## Port Scan

Total de hallazgos en esta categoría: **11**

### Open Port: 110/tcp

LOW

**Target:** 66.97.42.227 (kopernicus.tech)

Service: pop3 Courier pop3d

### Open Port: 143/tcp

LOW

**Target:** 66.97.42.227 (kopernicus.tech)

Service: imap Courier Imapd

### Open Port: 2084/tcp

LOW

**Target:** 66.97.42.227 (kopernicus.tech)

Service: sunclustergeo

### Open Port: 2087/tcp

LOW

**Target:** 66.97.42.227 (kopernicus.tech)

Service: eli

### Open Port: 21/tcp

LOW

**Target:** 66.97.42.227 (kopernicus.tech)

Service: ftp ProFTPD



### Open Port: 465/tcp

LOW

**Target:** 66.97.42.227 (kopernicus.tech)

Service: smtp

### Open Port: 587/tcp

LOW

**Target:** 66.97.42.227 (kopernicus.tech)

Service: smtp

### Open Port: 993/tcp

LOW

**Target:** 66.97.42.227 (kopernicus.tech)

Service: imap Courier Imapd

### Open Port: 995/tcp

LOW

**Target:** 66.97.42.227 (kopernicus.tech)

Service: pop3 Courier pop3d

### Open Port: 443/tcp

INFO

**Target:** 66.97.42.227 (kopernicus.tech)

Service: http Apache httpd

## Open Port: 80/tcp

INFO

**Target:** 66.97.42.227 (kopernicus.tech)

Service: http Apache httpd

## Web Vulnerability

Total de hallazgos en esta categoría: 6

### Nikto: /cli/: PHP include error may indicate local or remote file inclusion is possible.

HIGH

**Target:** kopernicus.tech:80

/cli/: PHP include error may indicate local or remote file inclusion is possible.

### Nikto: /7ZlxUqIZ.php#: The X-Content-Type-Options header is not set. This could allow t

LOW

**Target:** kopernicus.tech:80

/7ZlxUqIZ.php#: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.

### Nikto: /: Retrieved x-powered-by header: PHP/7.4.12.

LOW

**Target:** kopernicus.tech:80

/: Retrieved x-powered-by header: PHP/7.4.12.

### Nikto: /: Web Server returns a valid response with junk HTTP methods which may cause fa

LOW

**Target:** kopernicus.tech:80

/: Web Server returns a valid response with junk HTTP methods which may cause false positives.

### Nikto: /cl/: This might be interesting: potential country code (Chile).

LOW

**Target:** kopernicus.tech:80

/cl/: This might be interesting: potential country code (Chile).

### Nikto: /js: This might be interesting.

LOW

**Target:** kopernicus.tech:80

/js: This might be interesting.

# Conclusión

Este reporte técnico documenta los hallazgos de seguridad identificados durante la evaluación de **kopernicus.tech**.

Se recomienda priorizar la remediación de las vulnerabilidades críticas y altas documentadas en este reporte.

Para más información o asistencia en la remediación, por favor contacte al equipo de seguridad.

Reporte generado automáticamente el 11 de December, 2025 a las 19:06  
Workspace: kopernicus.tech | Total de hallazgos: 25