Johana Catherine Ezhil

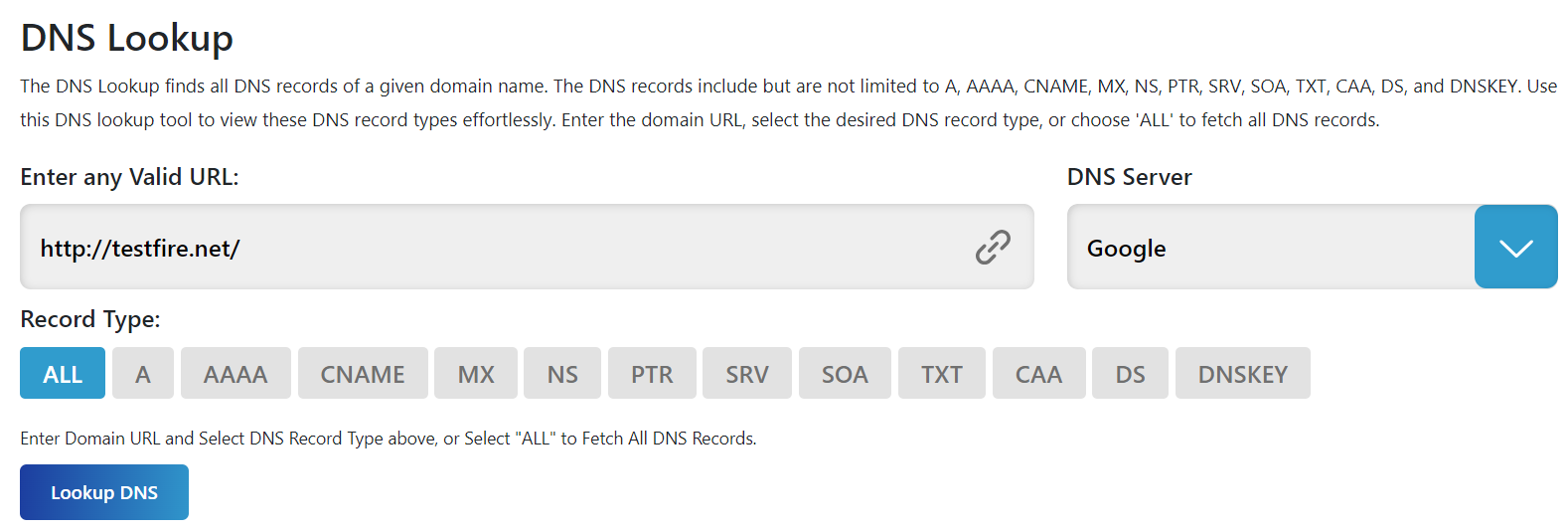
Oasys cybernetics  chennai

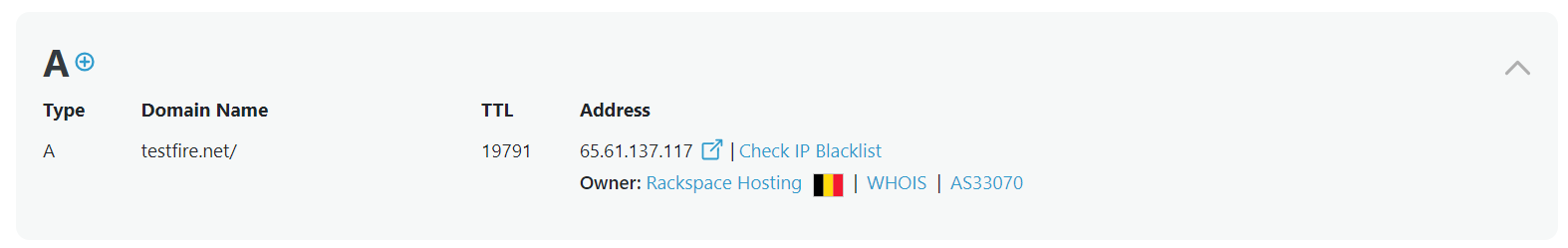
Information Gathering-passive approach

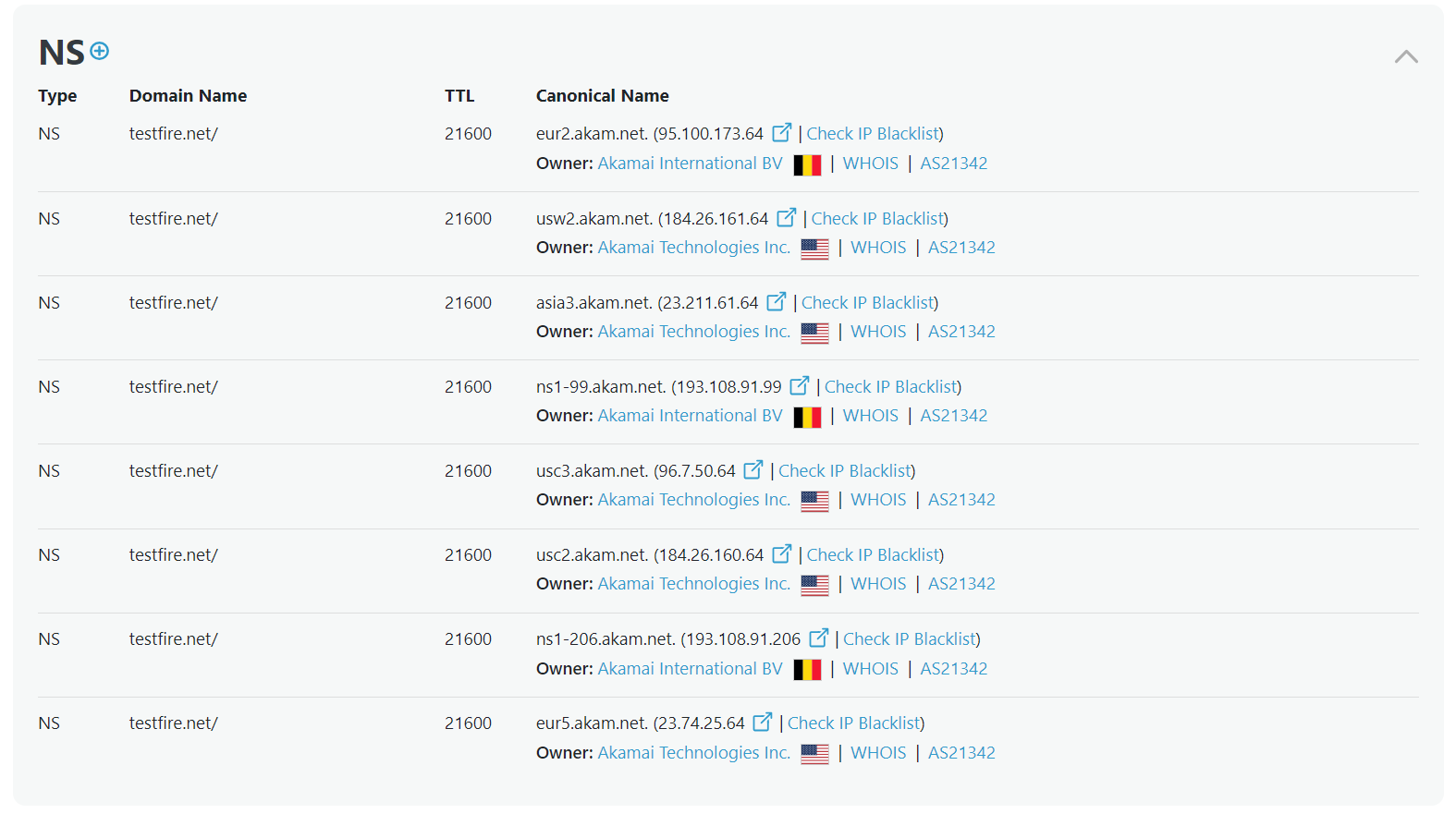
Target –> testfire.net

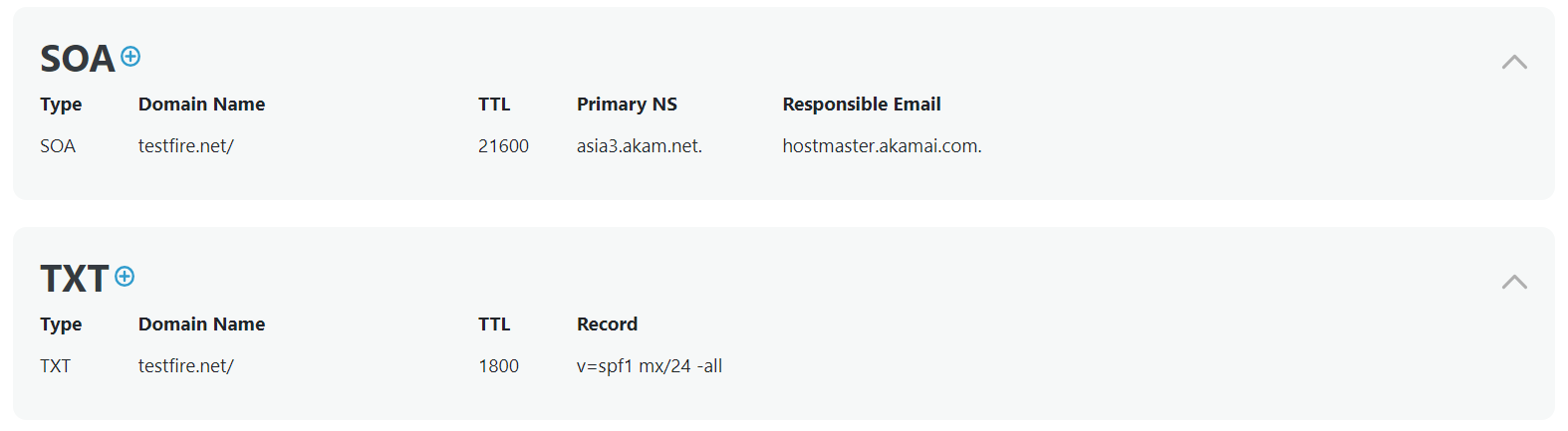
**DNSchecker:**

DNSchecker is an online tool that allows you to check the propagation status of DNS records across multiple servers worldwide.

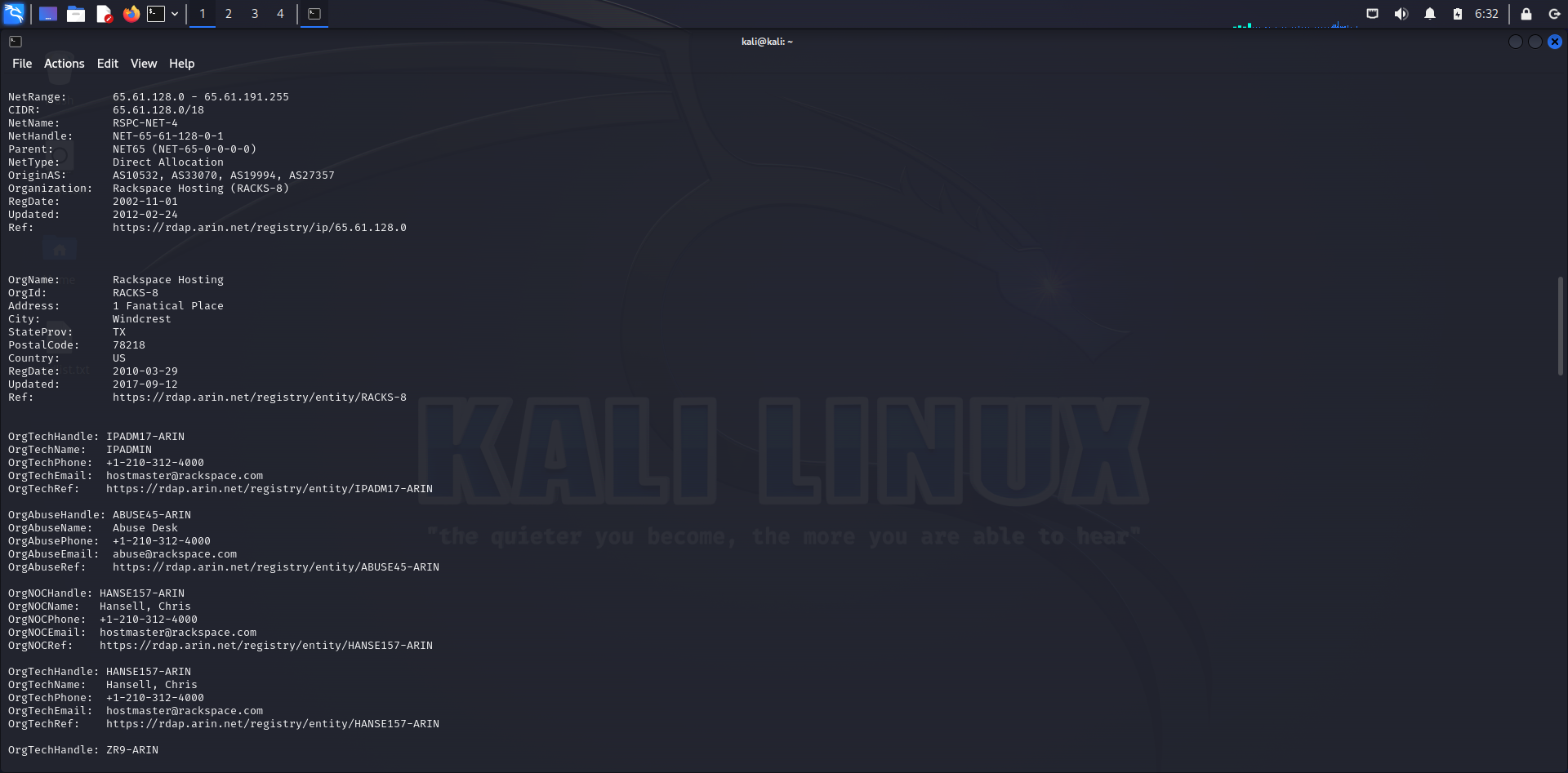








**WhoIS:**

Whois is used to query databases that store registered users or assignees of domain names, IP addresses, and autonomous systems



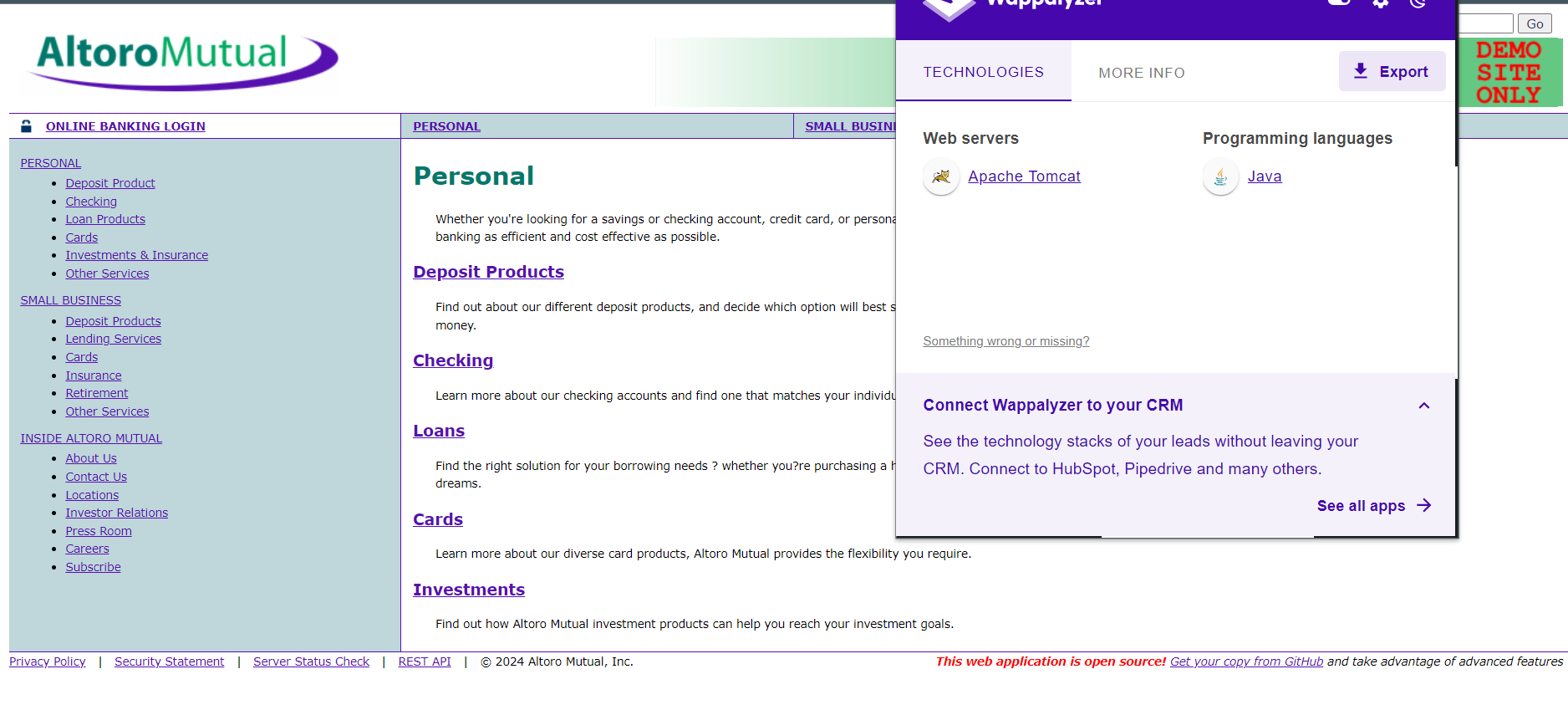
**Dnsenum:**

It automates the process of gathering DNS information, including subdomains, IP addresses, and DNS records like A, NS, TXT, and SOA records.



**Wappalyzer:**

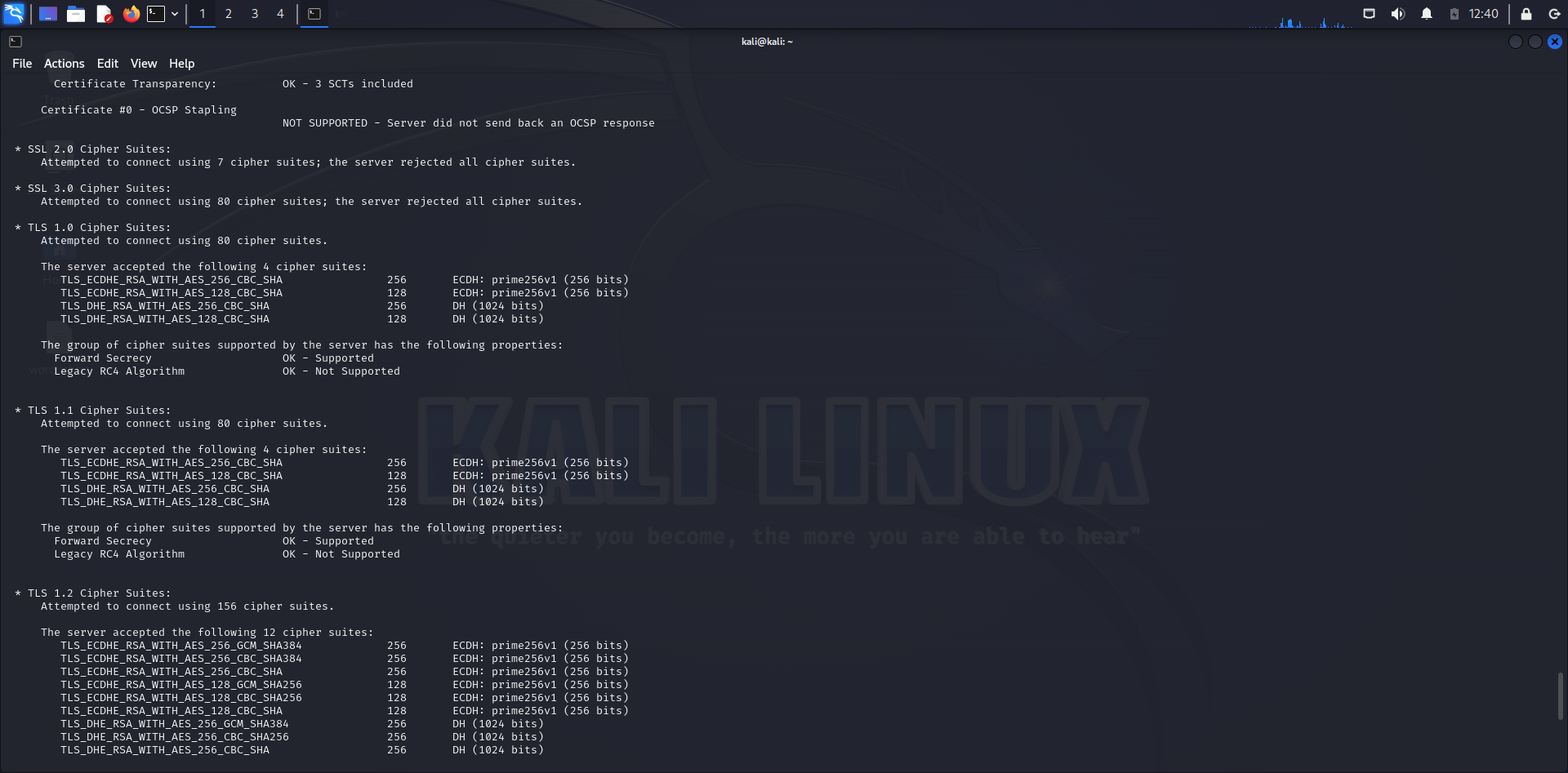
It identifies the technologies used by a website. It detects web technologies such as content management systems, e-commerce platforms, web frameworks, JavaScript libraries, and server software.

****

**Sslyze:**

Sslyze is a command-line tool that performs in-depth analysis of SSL/TLS configurations on a server. It checks for supported SSL/TLS versions, cipher suites, certificate details, etc.

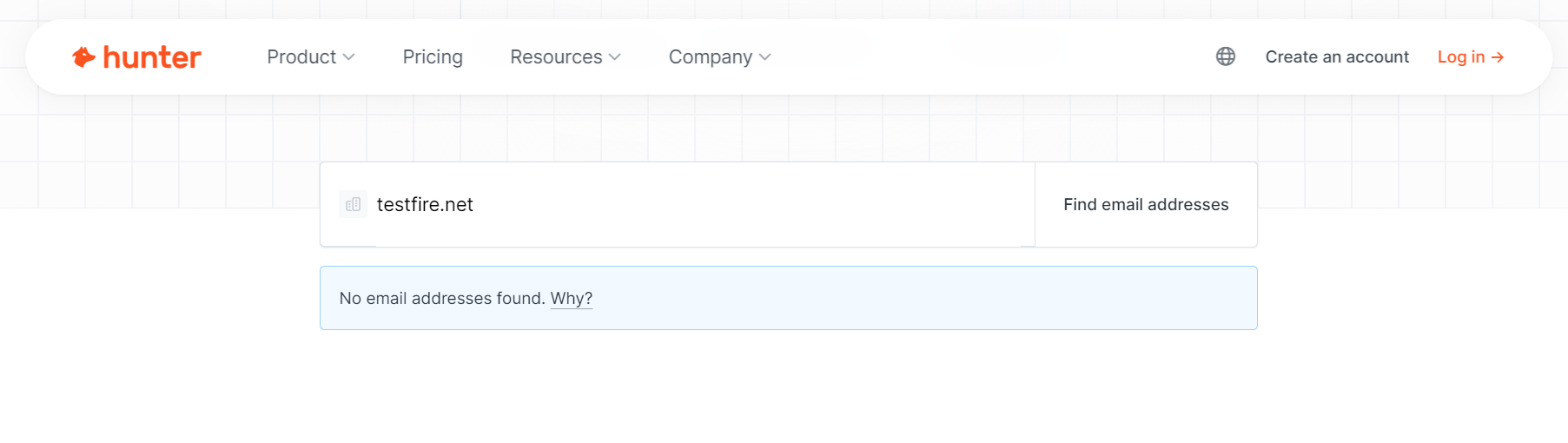






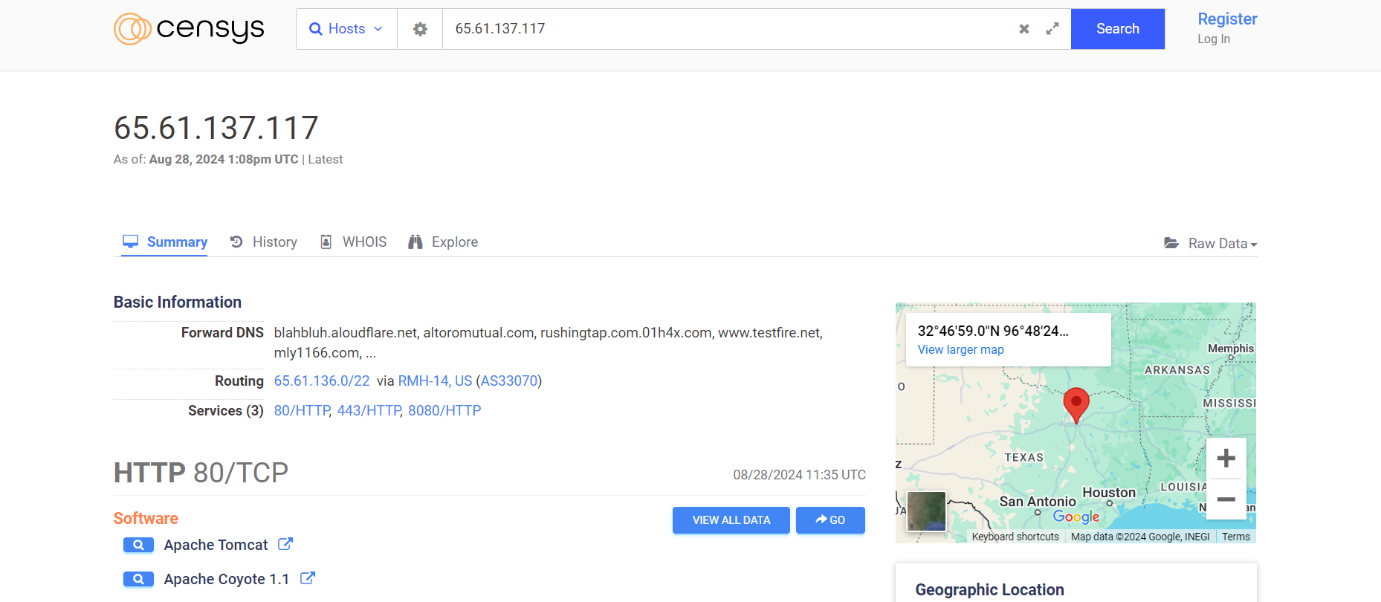
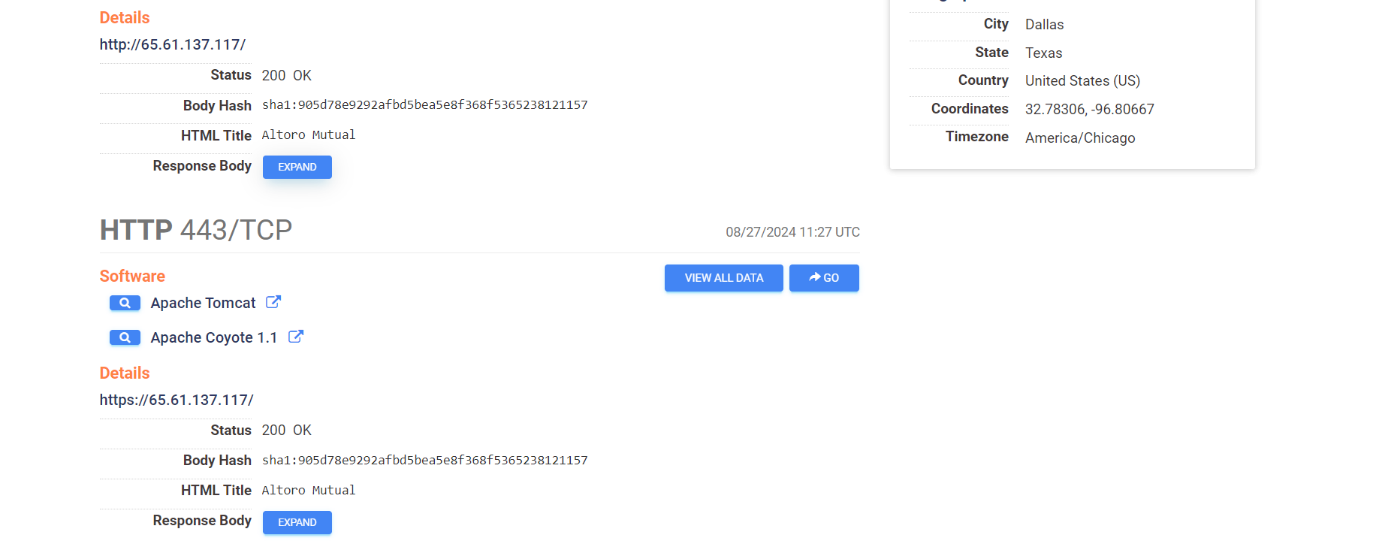
**Hunter.io:**

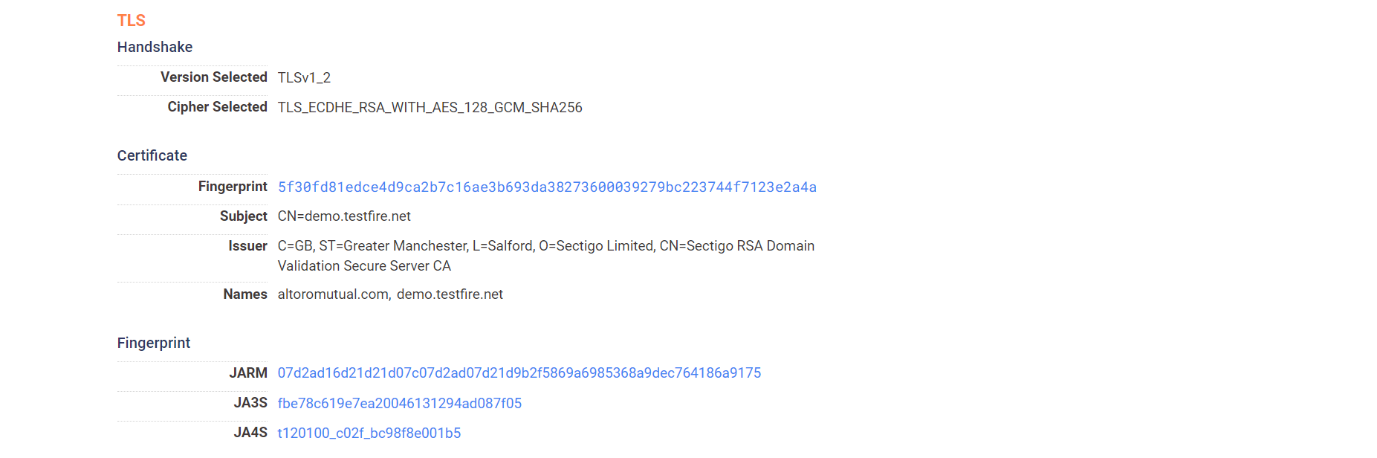
Hunter.io is an online tool that helps you find and verify email addresses associated with a domain. It searches publicly available sources to gather professional email addresses

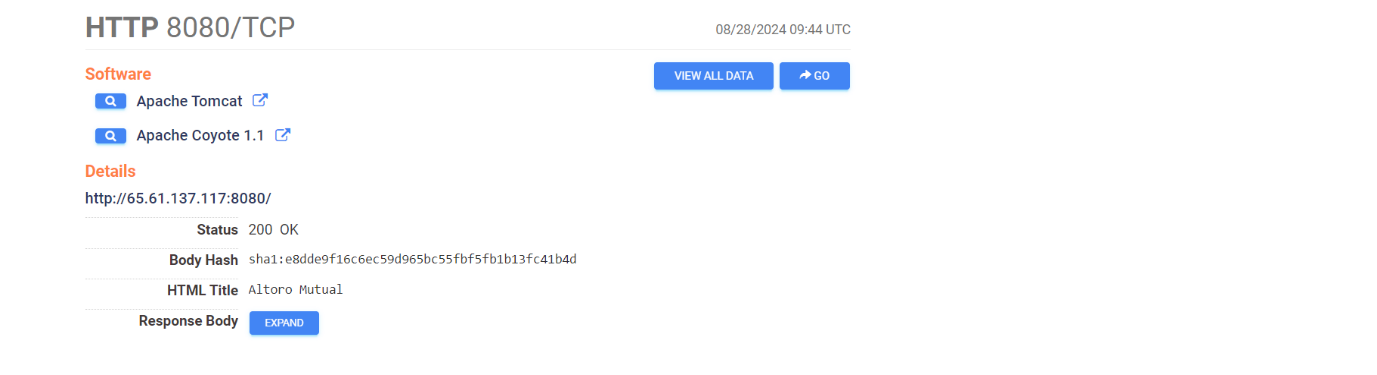
****

**Censys:**

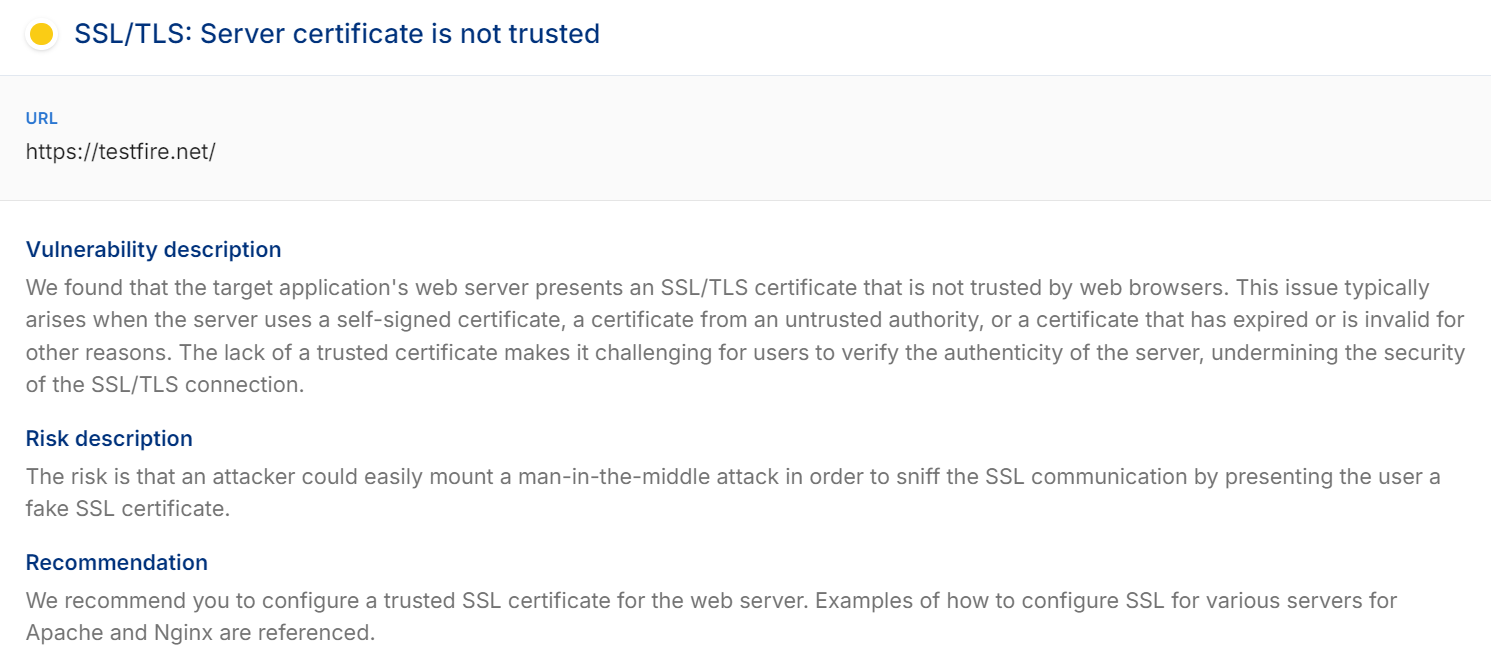
**Censys is a search engine that provides detailed information about devices, networks, and services exposed on the internet.**

****

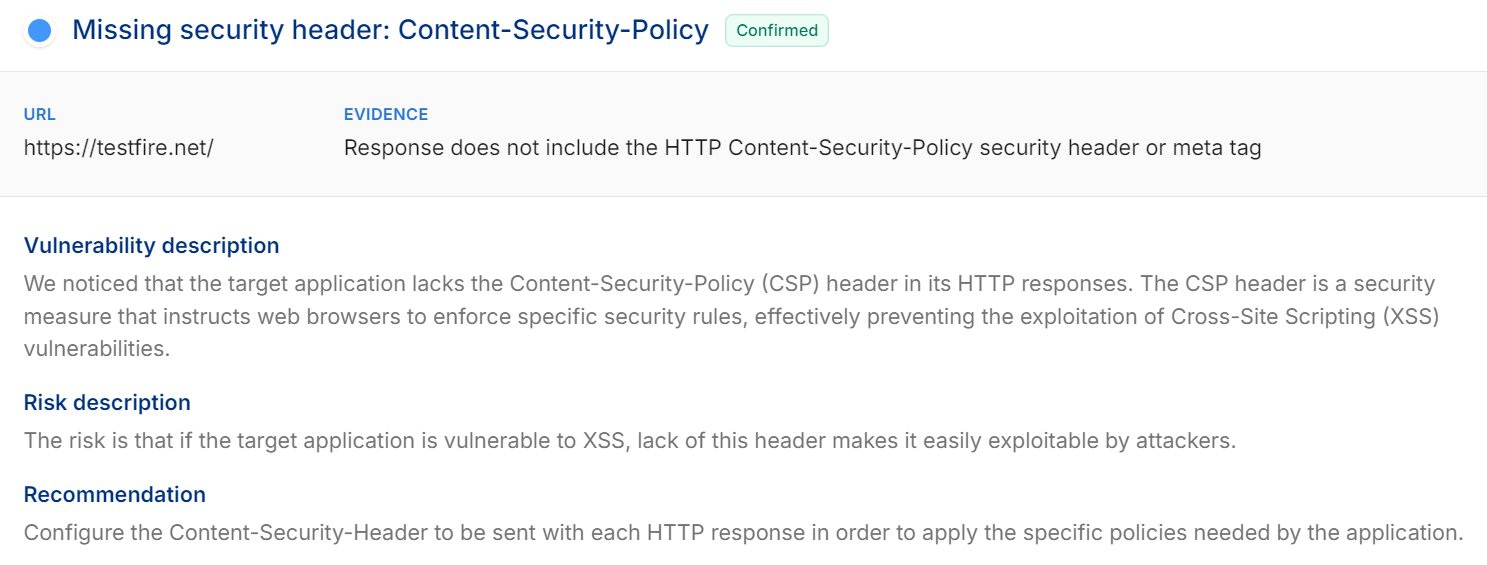
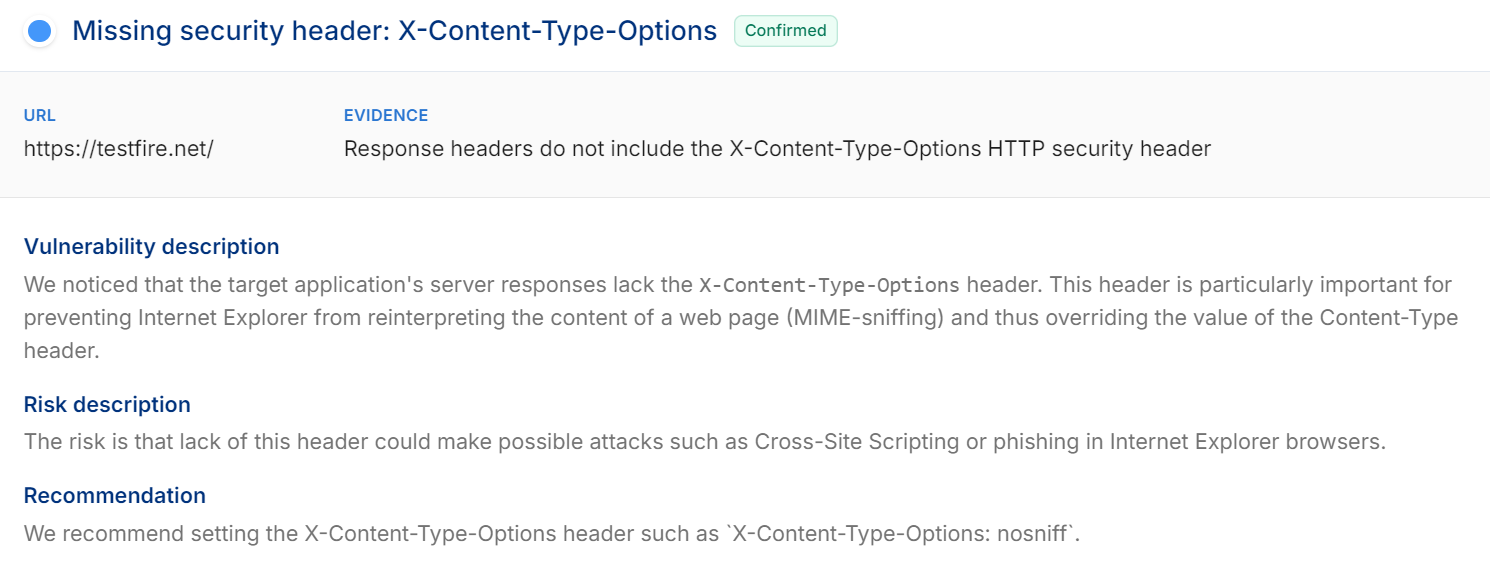
****

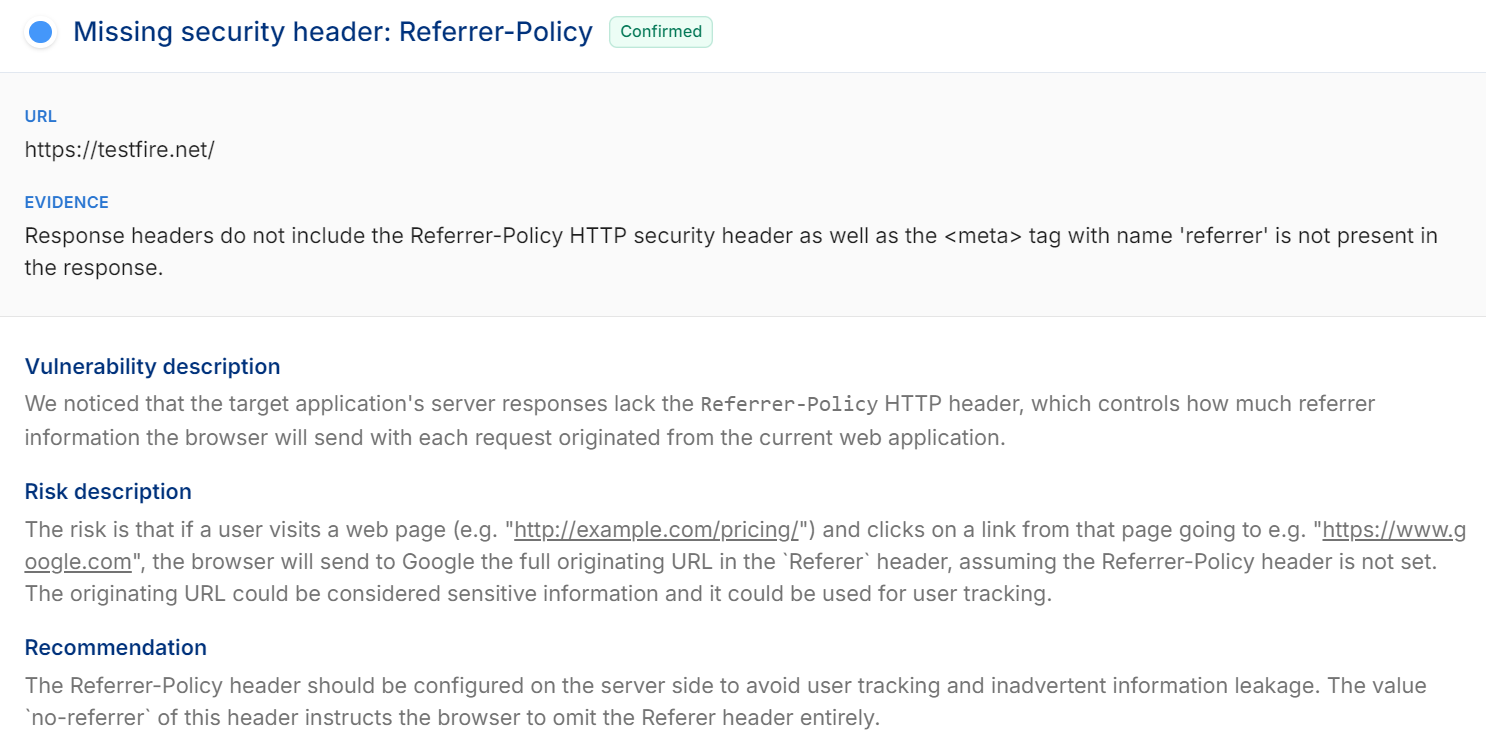
****

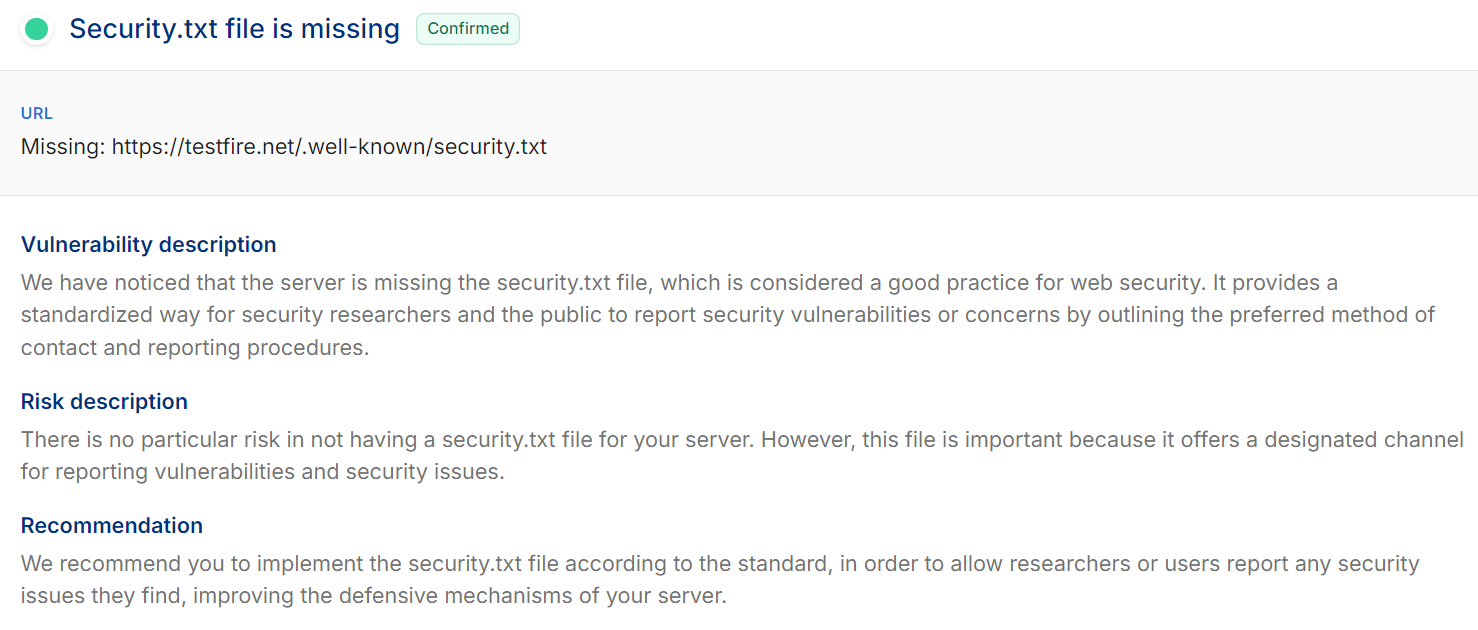
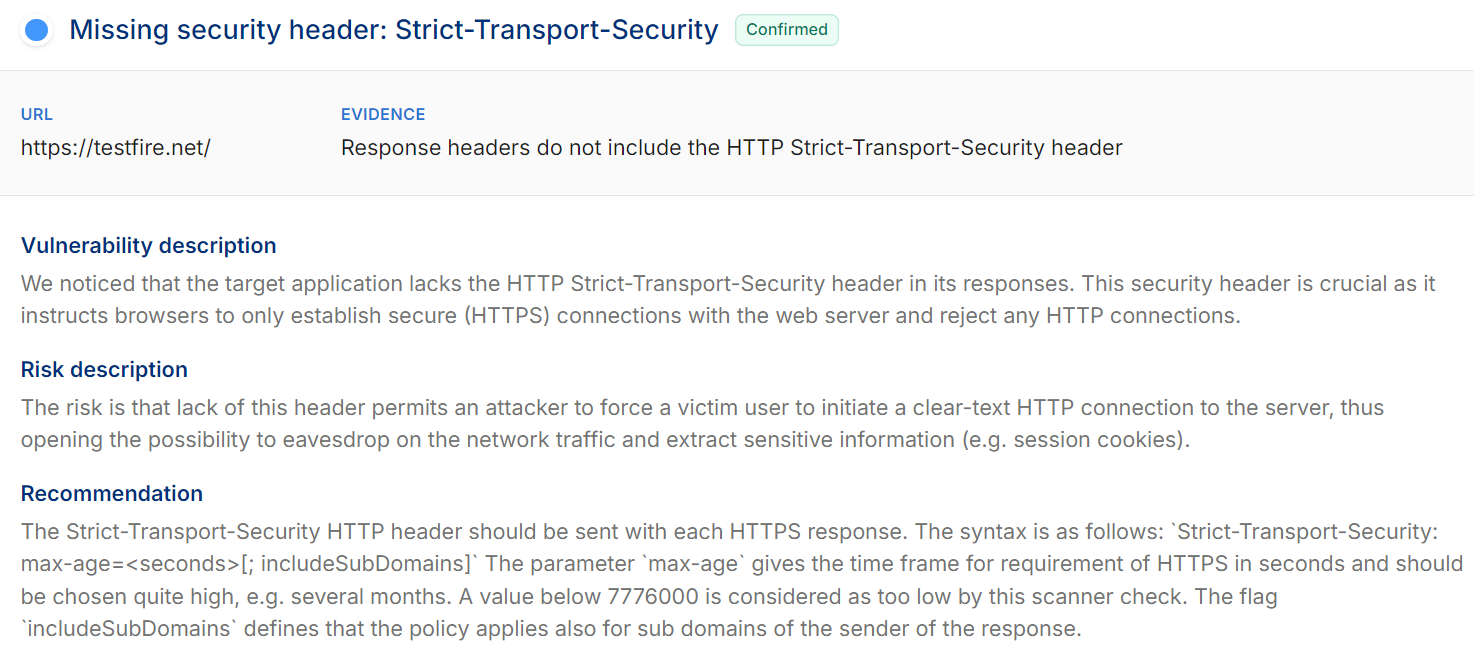
**Pentest-tool**

****

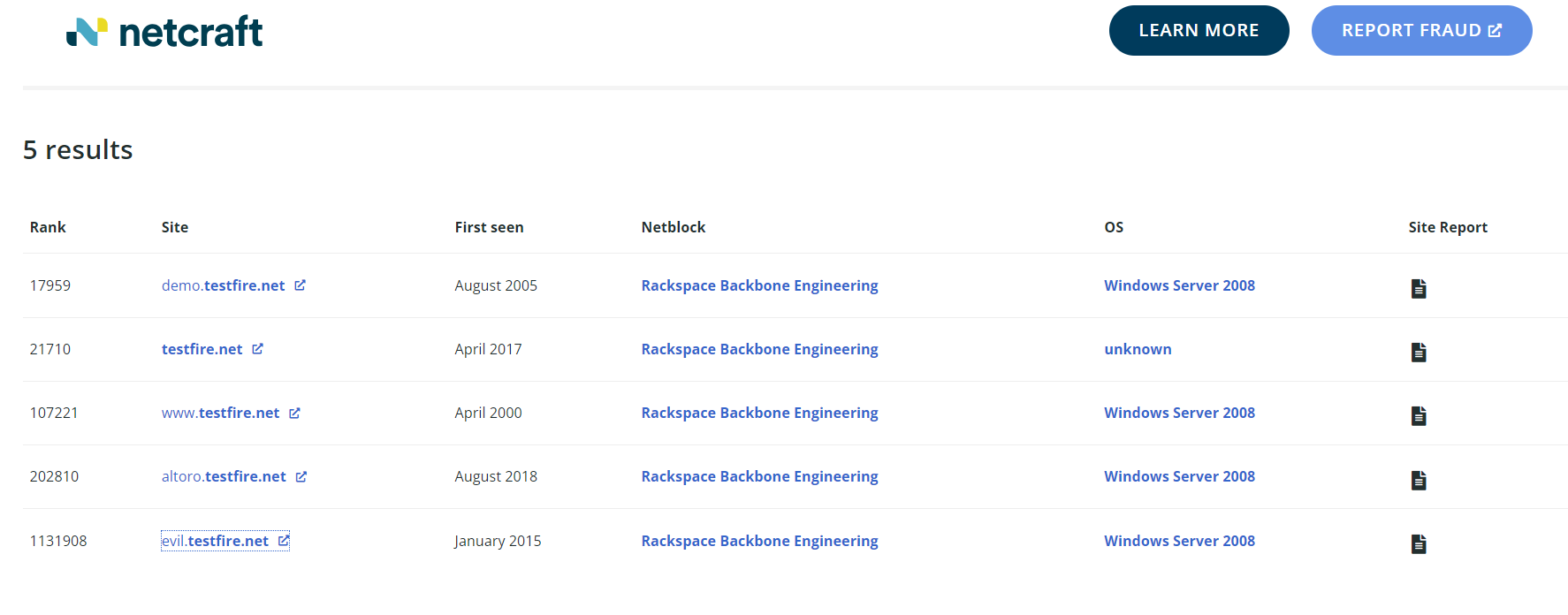
****

****

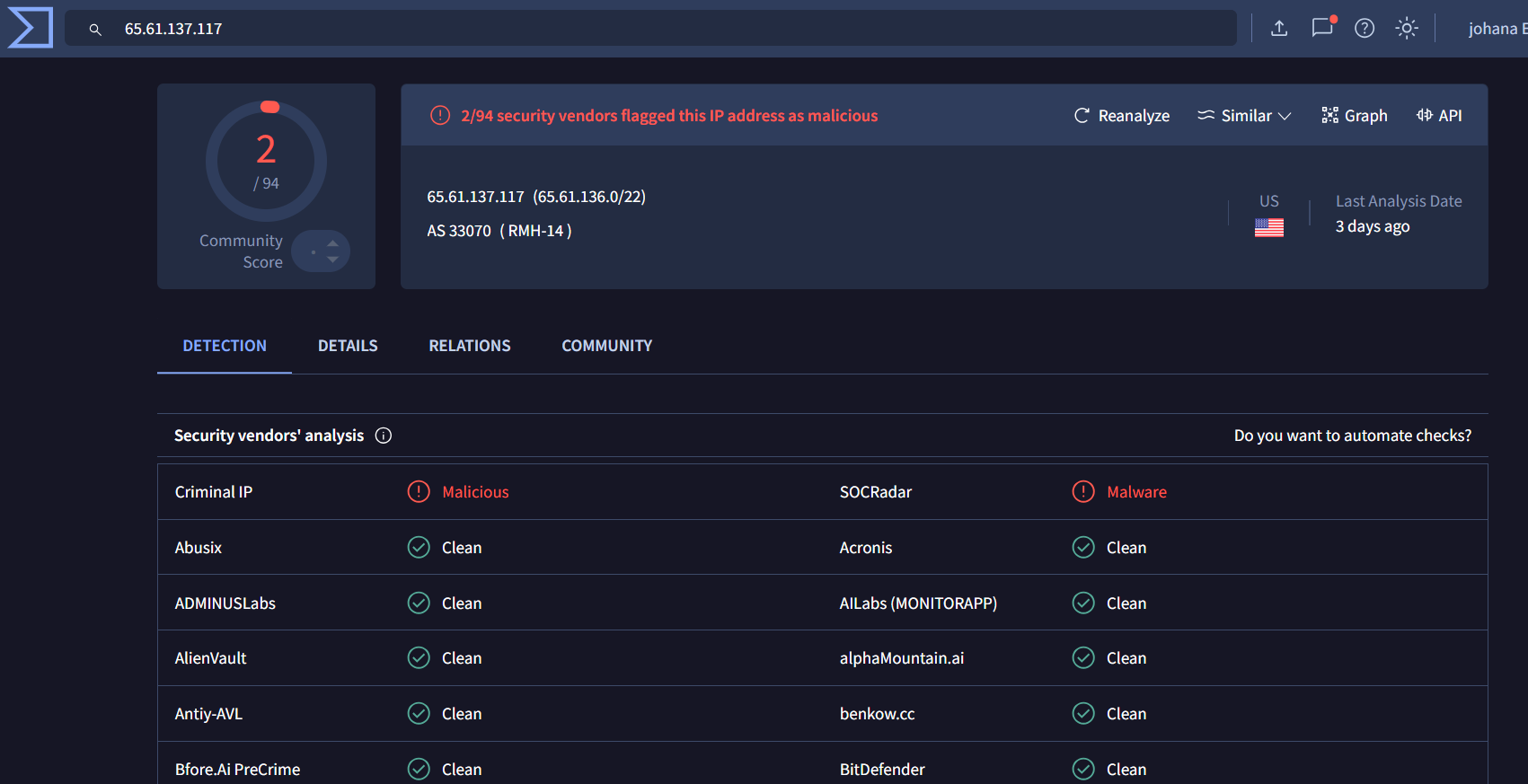
****

****

**Netcraft - subdomains**

****

**VirusTotal:**

****

**Conclusion:**

In this task, I successfully utilized a variety of tools to gather critical information about the target. By leveraging Nessus, VirusTotal, Pentest-Tools, Censys, DNSchecker, and Wappalyzer, I was able to collect valuable insights such as OS details, IP addresses, domain information, SSL certificates, and the web technologies used by the target. These tools provided comprehensive data, aiding in a thorough understanding of the target's infrastructure and potential vulnerabilities, laying a solid foundation for further analysis and security assessments.