Sri Lanka Institute of Information Technology

BSc Honors in Information Technology

Specializing in Cyber Security

IE2062 - Web Security

Bug Bounty Assignment – (Individual)

IT23236028 - W.V.A.MENDIS

Table of Contents

INTRODUCTION

This journal describes a number of Bug Bounty reports that are aimed at finding and fixing serious bugs in a web application for a particular company. To assess the security of the application, the project included vulnerability scanning, exploitation, and reconnaissance methods. Finding issues that need immediate care was the primary objective in order to improve the organization's digital infrastructure's defenses against attacks via the web. The practical experience gave important insights into how vulnerabilities affect an organization's security posture in the real world.

By promoting international cooperation, bug bounty programs are transforming cybersecurity. They aim to simplify the process of vulnerability disclosure and discovery by allowing individuals from a variety of backgrounds to participate in the security of digital ecosystems. Bug bounty methods can better handle new cyberthreats by using global pooled intelligence of the world community. Motivated by a strong interest in cybersecurity, I entered into bug bounty hunting to find weaknesses and resolve challenging issues that affect the security of businesses.

I developed my skills to identify, analyze, and disclose vulnerabilities on the journey. I learnt how to find vulnerabilities like SQL injection, cross-site scripting (XSS), and improperly implemented security rules using industry-standard tools. Additionally, I improved my capacity to assess the scope of vulnerabilities and suggest suitable corrective actions. My ability to produce actionable security reports that businesses can use to reduce risks and strengthen their security posture has improved as a result of this real-world experience.

In conclusion, this journal reflects my journey in bug bounty hunting and the skills gained along the way and it also included challenges that I faced while doing bug bounty. It serves as a guide for aspiring bug bounty hunters, offering insights into the tools and techniques used in vulnerability discovery and the importance of producing detailed, actionable reports.

PURPOSE

The objective of this assignment is to have a deeper understanding of web application vulnerabilities and effective mitigation techniques. We identified 10 vulnerabilities in 10 sub-domains by choosing a domain from bug bounty platforms such as **Bugcrowd**, **HackerOne**, or **Intigriti**. The objective was to identify these vulnerabilities, produce bug bounty reports, and suggest viable fixes.

Our skills in vulnerability scanning, reporting, and web application security are improved through this exercise. It also provides us with hands-on experience with actual cybersecurity problems, making us ready to participate in bug bounty programs and contribute towards making digital networks more secure.

Chapter 1: OWASP Top 10 Vulnerabilities

The Open Web Application Security Project **(OWASP)** publishes the ***OWASP Top 10 Vulnerabilities***, a commonly accepted top ten list of the most serious security risks to web applications. It is a company guidebook, security consultant, and developer guidebook to the knowledge, identification, and avoiding the most prevalent and perilous threats to web application security. Based on statistics presented by security experts and future trends in vulnerabilities, the list is updated from time to time.

Cross-site scripting (XSS), injection attacks (such as SQL injection), broken access control, and security misconfiguration errors are some of the common threats. These can reduce the probability of attack and improve the security of your application overall.

1. **Broken Access Control**

Access control means putting some restrictions or limits on website users depending on their needs. So if we fail to give correct access rights, unauthorized parties may modify, or destroy the website's data.

2. **Cryptographic Failures**

The use of old or weak cryptographic algorithms, default encryption keys, and compromised keys are some of the common issues under this vulnerability. The major impact of this vulnerability is compromising all data such as personal data, credentials, credit card information, etc.

3. **Injection**

Injection happens when the developer doesn’t validate or sanitize the user inputs, hostile data is concatenated, etc. SQL injection and NoSQL injections are the most common attack vectors in injection vulnerability.

4. **Insecure Design**

Usage of unsafe APIs, and missing user input bounds are some major issues of this vulnerability. When we think about software and services, if the foundation of the software or services isn’t built well, it may affect the security of that system.

5. **Security Misconfiguration**

Unpatched flaws, Default configurations, Unused pages, Unprotected files and directories, and Unnecessary services are some common attack vectors of security misconfiguration. This vulnerability is occurring because of unstable default settings.

6. **Vulnerable and Outdated Components**

Using Insecure software configurations, using old and unpatched dependencies, and using vulnerable components are some common issues of this vulnerability. There are many tools to find these types of vulnerabilities.

7. **Identification and Authentication Failures**

This vulnerability happens when an application doesn't try to prevent brute forcing password attacks when the app has flaws in password recovery, etc. Because of these authenticated related attacks, user identities may be disclosed to unauthorized parties.

8. **Software and Data Integrity Failures**

This vulnerability happens because of unchecked and unverified apps. Nowadays app developers add auto update functionality so that without checking the update the app updates itself. So an attacker may add his update to attack the app.

9. Security Logging and Monitoring Failures

Logins are not backed up, the Monitoring system fails to identify malicious activities, and missing alerting systems are some issues of this vulnerability. Because of these attacks, information leakages can happen.

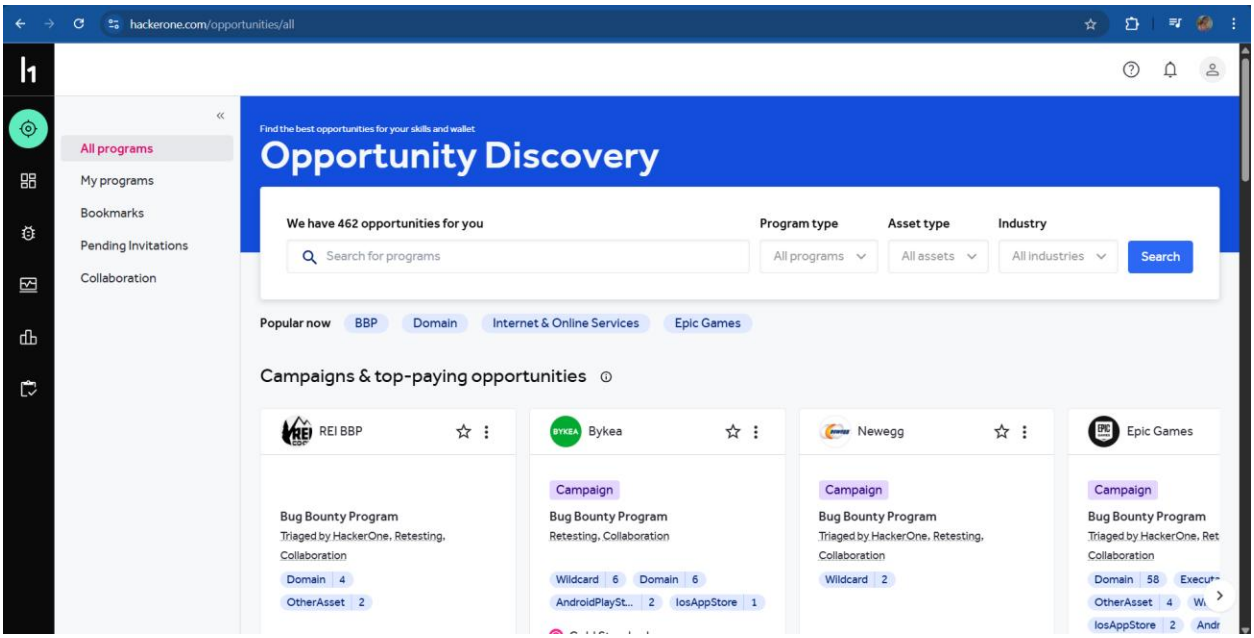
10.Server-side Request Forgery

If an application shows a preview of the URLs, that application is vulnerable to this attack. Fetching a URL has become a common scenario of modern web applications, so as a result SSRF has increased.

Chapter 2: Select a Program and Creating an Account

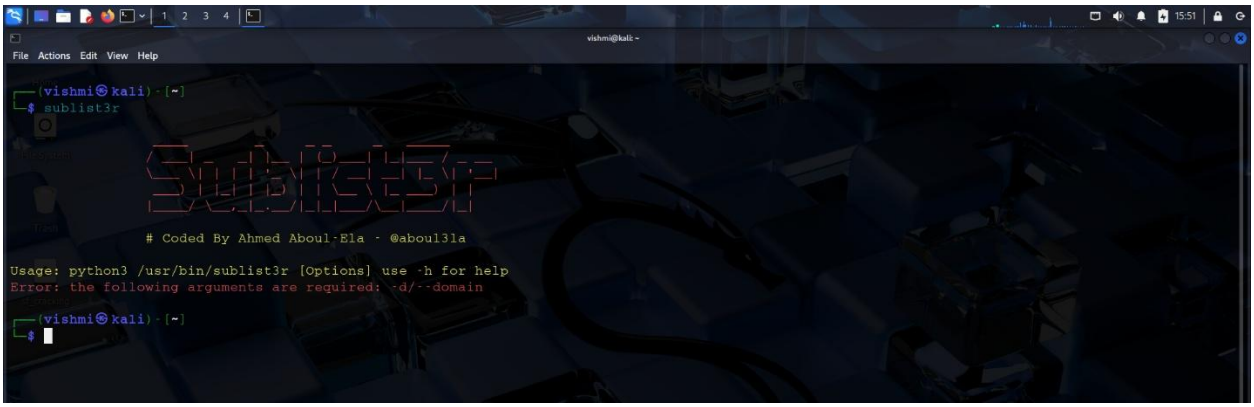
Before beginning my bug bounty journey, I thoroughly researched the various platforms and programs. Among them are **Intigriti, Bugcrowd,** and **HackerOne**. Knowing that the caller and variety of programs offered would affect the efficacy of my bug-hunting efforts, I spent some time researching different platforms and evaluating what they had to offer. These platforms are well-known in the cybersecurity field for their powerful program structures, wide audience, and active community of security researchers.

In the end, I decided to use **HackerOne** to complete my bug bounty program.



Chapter 3: RECONNAISSANCE ON THE TARGET

Sublist3r



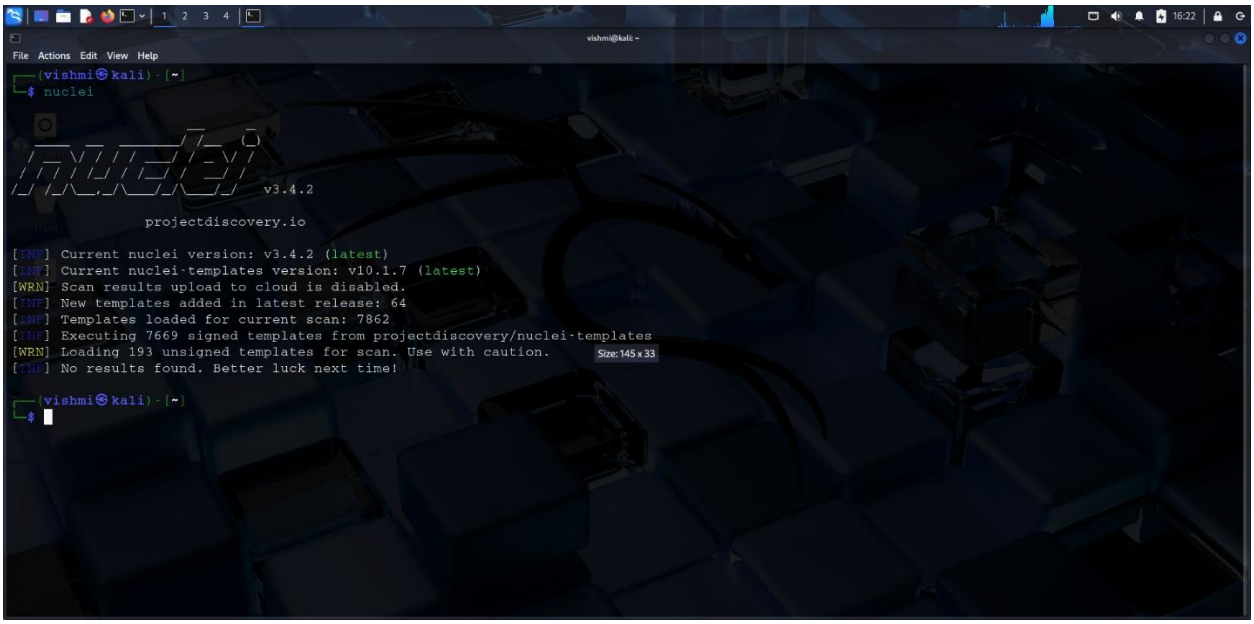
Sublist3r is a quick subdomain scanning application that uses OSINT(Open Source Intelligence) to find website subdomains. Python is used in its writing, and threading is supported for quicker execution. It works especially well to increase the number of possible points of entry for more thorough vulnerability scans.It helps hackers and bug bounty hunters in mapping the attack surface. Several search engines, including Google, Yahoo, Bing, and Netcraft, are integrated. Its capacity to use third-party APIs and brute-forcing for thorough subdomain identification is one of its most notable features.

Httprobe

A lightweight program called HTTprobe is intended to determine which detected domains are hosting active HTTP or HTTPS servers and the active subdomains also.

It is known for its speed and simplicity in allowing data to be piped into it directly from programs like Sublist3r or Amass for immediate results. It is very helpful for rapidly eliminating responsive hosts following subdomain enumeration. Its quickness and ease of use are unique; with little setup, it can test for responsiveness across numerous ports and handle thousands of domains.

Nuclei



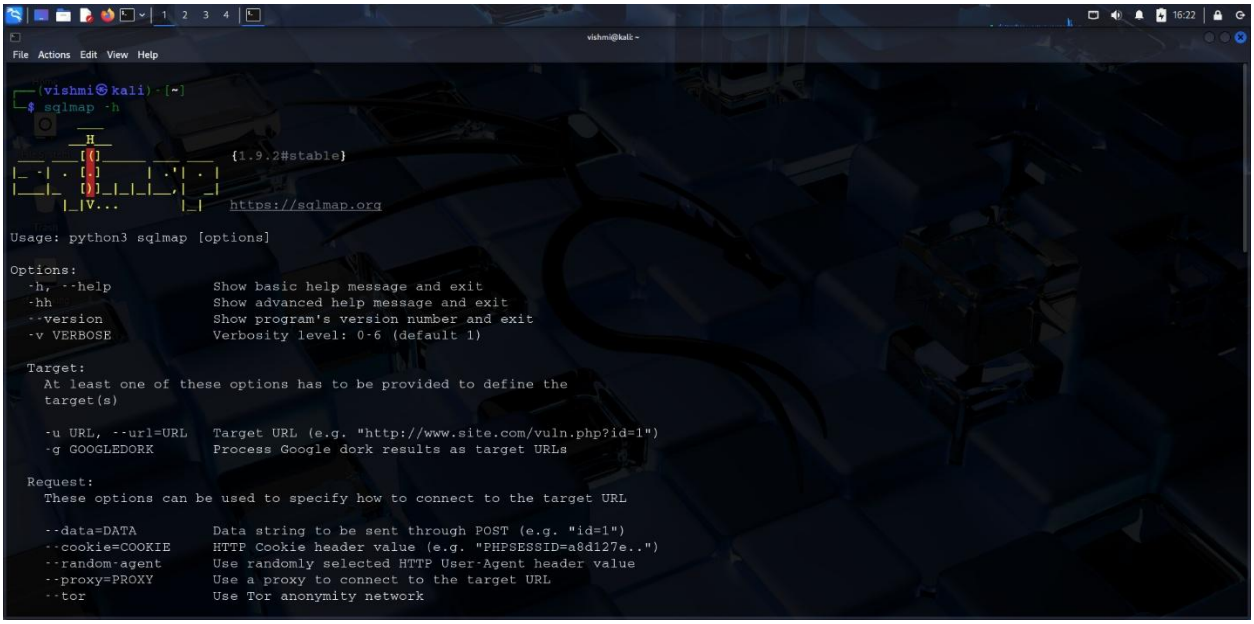
Nuclei is a robust vulnerability scanner that scans for known vulnerabilities through customizable YAML(Yet Another Markup Language) templates. It enables fast and automated scanning for exposures, misconfigurations, and CVEs(Common Vulnerabilities and Exposures). It is perfect for integrating into automated CI/CD security pipelines because it supports output formats including JSON, tagging, and severity levels.

Its customization, which enables customers to develop their own templates, is a key advantage. This enables it to be adapted to any special scanning needs in online, network, and cloud assets.

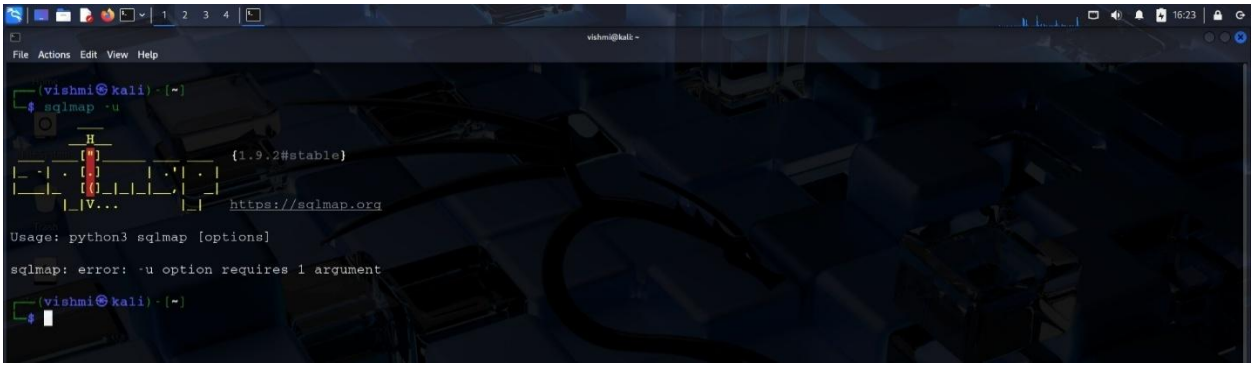
SQLmap

An open-source utility called SQLmap makes it easy to find and exploit SQL injection flaws. It is capable of executing code remotely and retrieving databases and tables. Its automation depth is one of its biggest advantages; it does everything from finding injection points to data gathering, and therefore it is essential for database security testing.

In addition to scanning, SQLmap facilitates file system access, user enumeration, and database fingerprinting. It can be customized to target particular injection techniques or databases like MySQL, Oracle, or PostgreSQL. It also supports authentication and can operate through proxies.



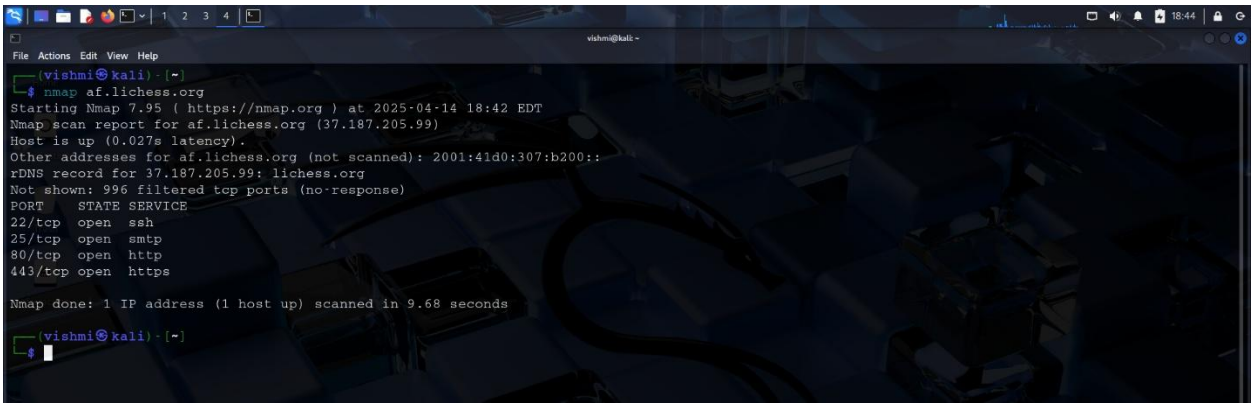
Sqlmap -h = shows the help menu with all SQLmap options and usage instructions.



Sqlmap -u = Target the specified URL for SQL injection testing

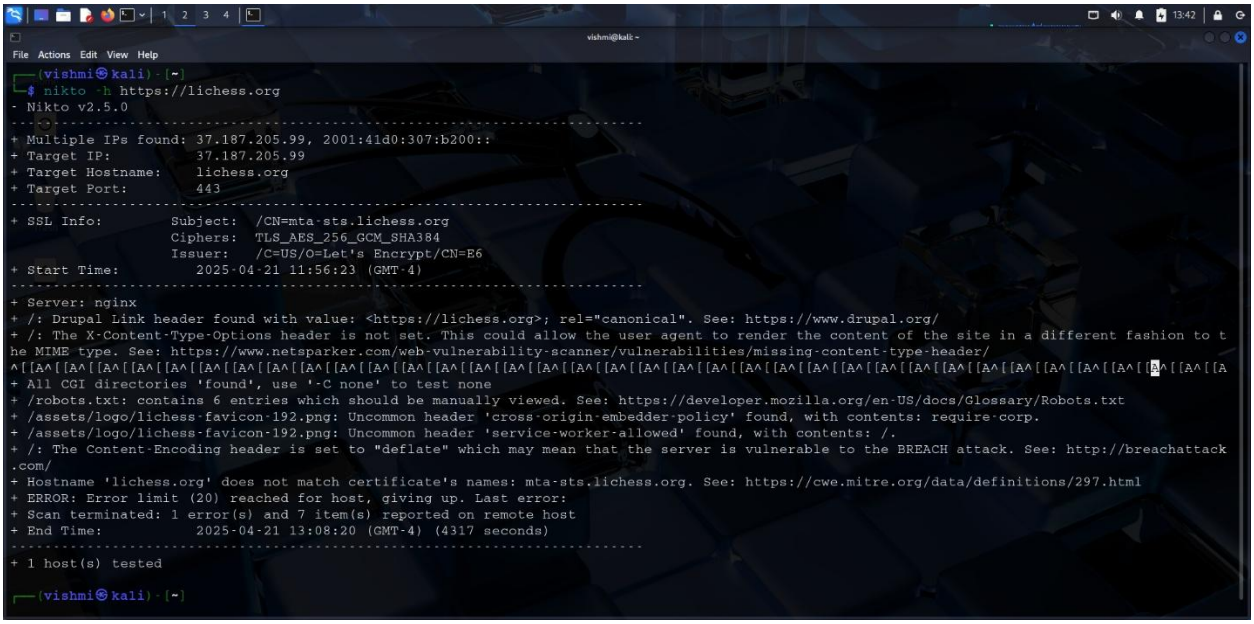
Chapter 4:Searching for vulnerabilities

Nmap



An effective open-source program for network discovery and security auditing is called Nmap (Network Mapper). It assists network administrators with device identification, port and service discovery, and network mapping. Host discovery, OS and service version identification, and scriptable target interaction are important capabilities. Its main goal is to evaluate network security and find weaknesses before attackers do. Routine network inventory, uptime monitoring, and scheduling service upgrades are some common uses for Nmap.

Nikto



Nikto is an open-source web server scanner made to identify security flaws and vulnerabilities. It checks web servers for harmful files or scripts, misconfigured systems, and out-of-date software versions. Configurable report outputs, proxy support, and SSL support are important features. Its primary goal is to promptly detect possible risks in server settings and web applications. Nikto is well-known for being quick and easy to use, which makes it perfect for early-stage penetration testing web vulnerability assessments.

Virustotal

A free web tool called VirusTotal checks files and URLs for trojans, worms, viruses, and other malware. To find dangers, it makes use of more than 70 antivirus scanners and URL/domain blacklisting services. Multi-antivirus engine scanning, file reputation score, and automation through API integration are some of its primary characteristics. The main goal of VirusTotal is to assist people and organizations in rapidly determining if files or websites are secure, offering a crucial first line of protection against the spread of malware and other internet risks.

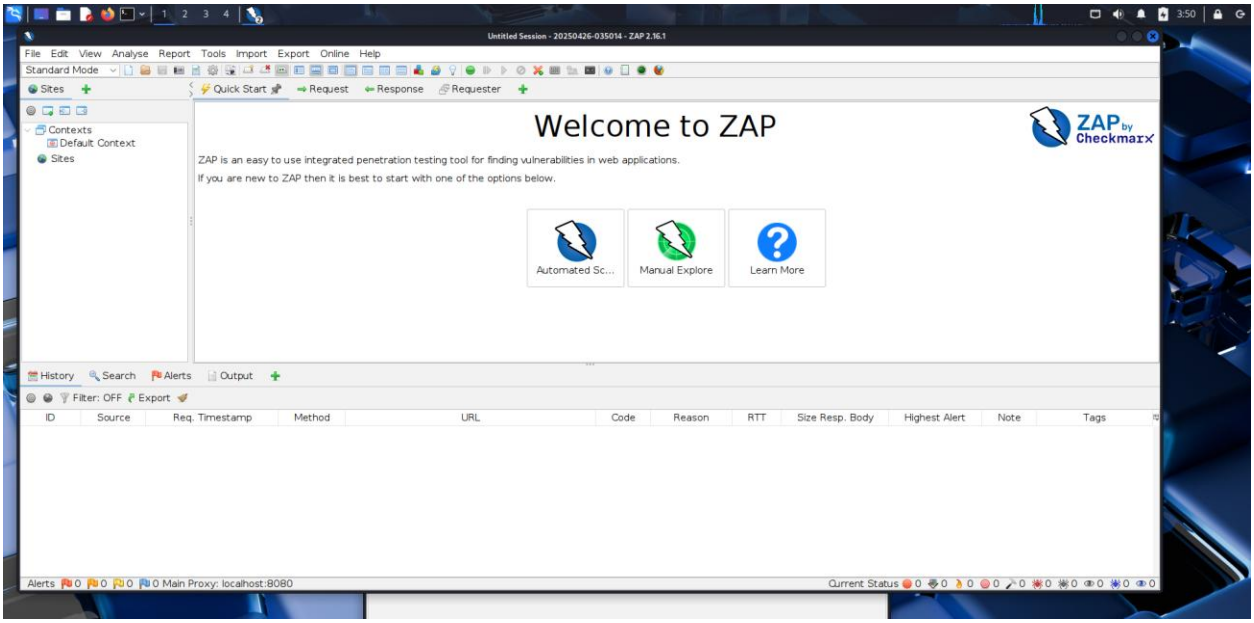
After entering a target URL, we can find out number of security vendors .

“Security vendors” are businesses or groups that offer equipment, goods, or services to defend networks, systems, and data against online attacks. They develop security information and event management (SIEM) tools, intrusion detection systems, firewalls, and antivirus software. These suppliers support governments, corporations, and individuals in defending against malware, phishing, cyberattacks, and other threats.

OWASP ZAP

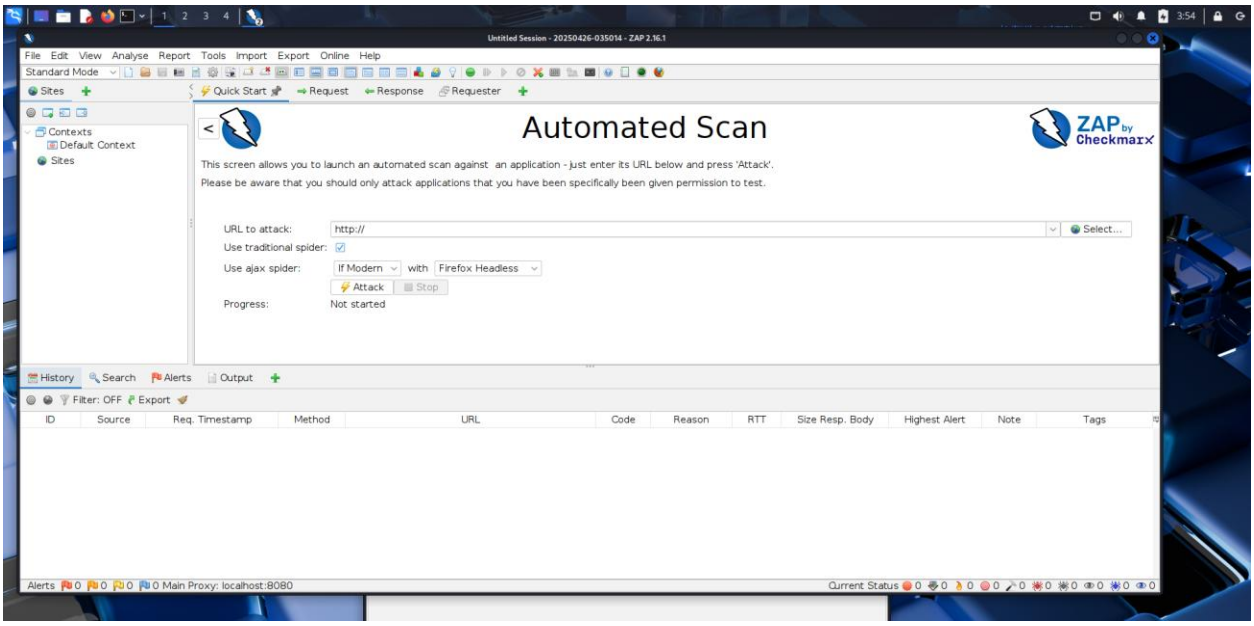
The OWASP community maintains the open-source web application security scanner known as OWASP ZAP (Zed Attack Proxy). It is perfect for both novice and expert testers and automatically assists in identifying vulnerabilities. Automated scanners, passive scanning, fuzzing, and API testing are important characteristics. Its goal is to help developers and security experts safeguard their applications before deployment by detecting problems such as SQL injection, cross-site scripting (XSS), and other web application defects during the development and testing stages.

First, we should install ***"Zaproxy"*** in kali.
This is how zap looks like , Numerous features are available in ZAP for both automatic and manual security testing .



I chose, automated scan.

This is how automated scan looks like.



1.First, we have to give our target URL in ***"URL to attack"*** section.

2.After we have to choose**, "*Use traditional spider, Firefox Headless"*** and click **"*Attack*"** button.

3.Then, we can go to ***"Alerts"*** and examine the vulnerabilities.

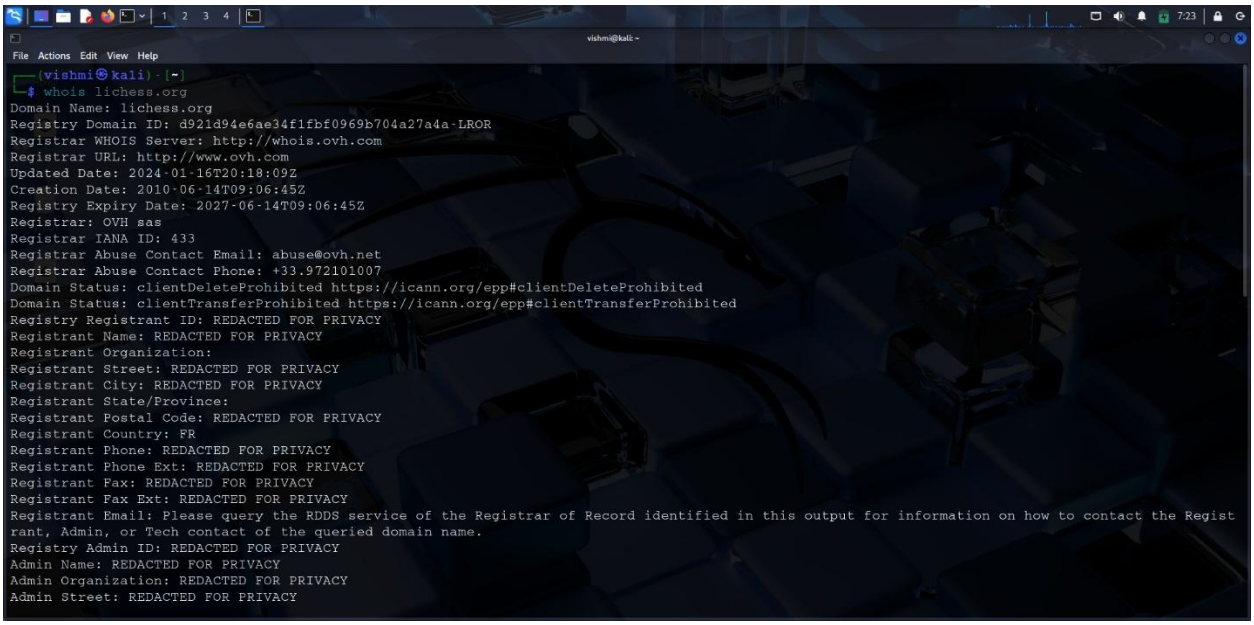
Report-01

Web Audit
lichess.org

Domain = *lichess.org*
Sub-domain = *af.lichess.org*
URL = *https://lichess.org*

Target Reconnaissance

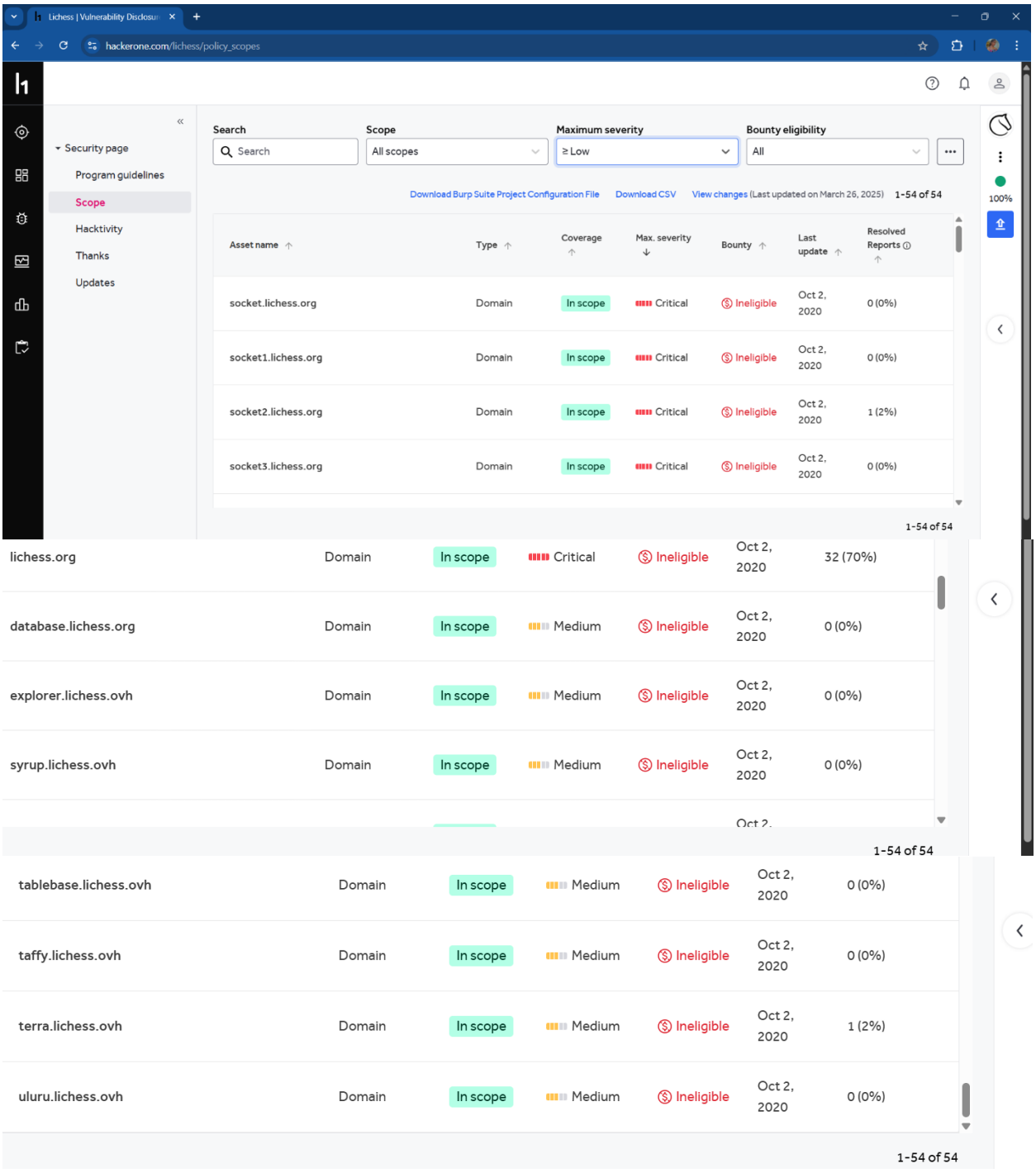
Introduction to Lichess and Audit Scope



“Lichess” is an open-source, advertisement-free, and free online chess website for everyone to play, learn, and enjoy chess. Created in 2010 by French computer programmer Thibault Duplessis, **lichess** offers numerous features like casual and ranked games, tournaments, solving puzzles, game analysis with a powerful engine, and learning features like training and studies. It has all sorts of variants of chess, such as Bullet, Blitz, Classical, Chess960, etc. With its community-driven and inclusive approach, **lichess** is funded solely through donations and remains among the most popular and respected websites to play chess all around the world.

These subdomains (and all included) have been approved as legitimate subdomains for testing in the **Hackerone** Bug Bounty program.

Eligible in-scope subdomains for bug bounty program are mentioned below



Information gathering phase.

The information-gathering phase, often known as reconnaissance or recon, is essential to both assessments of security and cyberattacks. In order to map out the target's structure and determine how it functions, the target of this stage is to gather as much information as possible about it. Because it helps auditors or attackers identify vulnerabilities that could be exploited later on, this fundamental understanding is essential.

There are two main approaches to information gathering

1. **Active Scanning :**

   Involves direct interaction with the target, which can generate noticeable activity and typically uncovers a wealth of details about the system.

2. **Passive Scanning :**

   Seeks to observe the target without direct engagement, resulting in less detectable activity but often providing more limited information

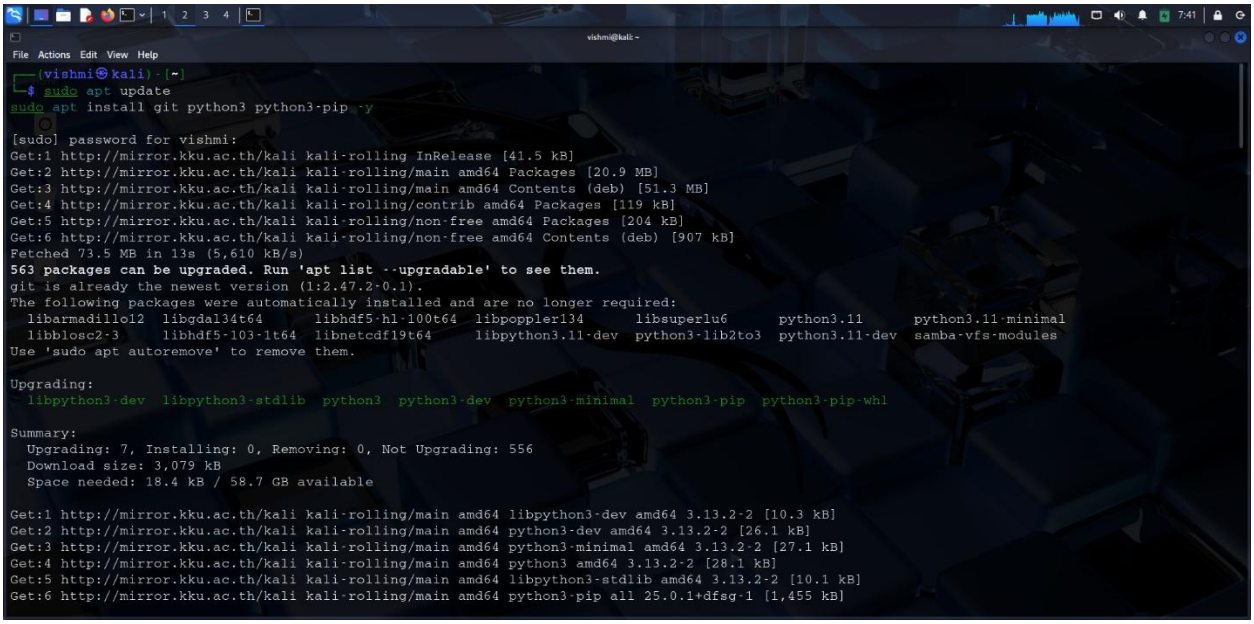
Finding active subdomains and their states

Sublist3r

Sublist3r is an open-source Python application that uses OSINT (Open Source Intelligence) techniques to quickly and effectively scan subdomains. Subdomains linked to a target domain can be found by penetration testers, security researchers, and bug bounty hunters using a variety of search engine queries (including Google, Yahoo, Bing, Baidu, and Ask). Additionally, Sublist3r includes a brute-force module (subbrute) to employ a stronger wordlist to improve the probability of discovering more subdomains.

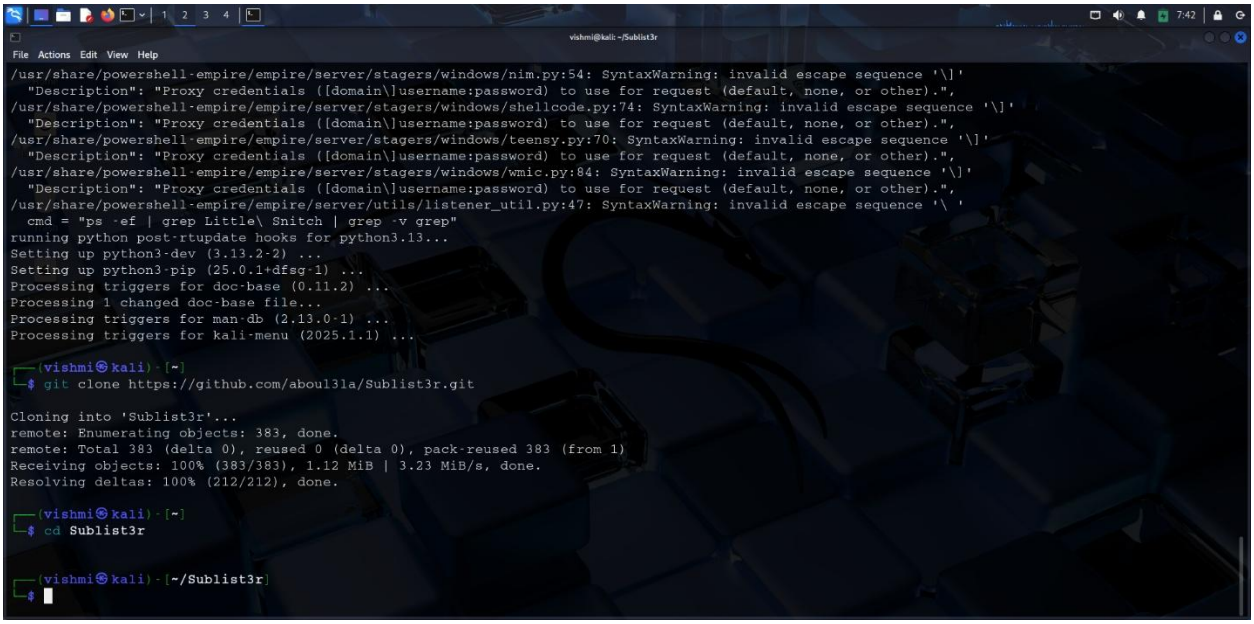
To install Sublist3r in Linux, we can use the below command.

"sudo apt update
sudo apt install git python3 python3-pip -y"



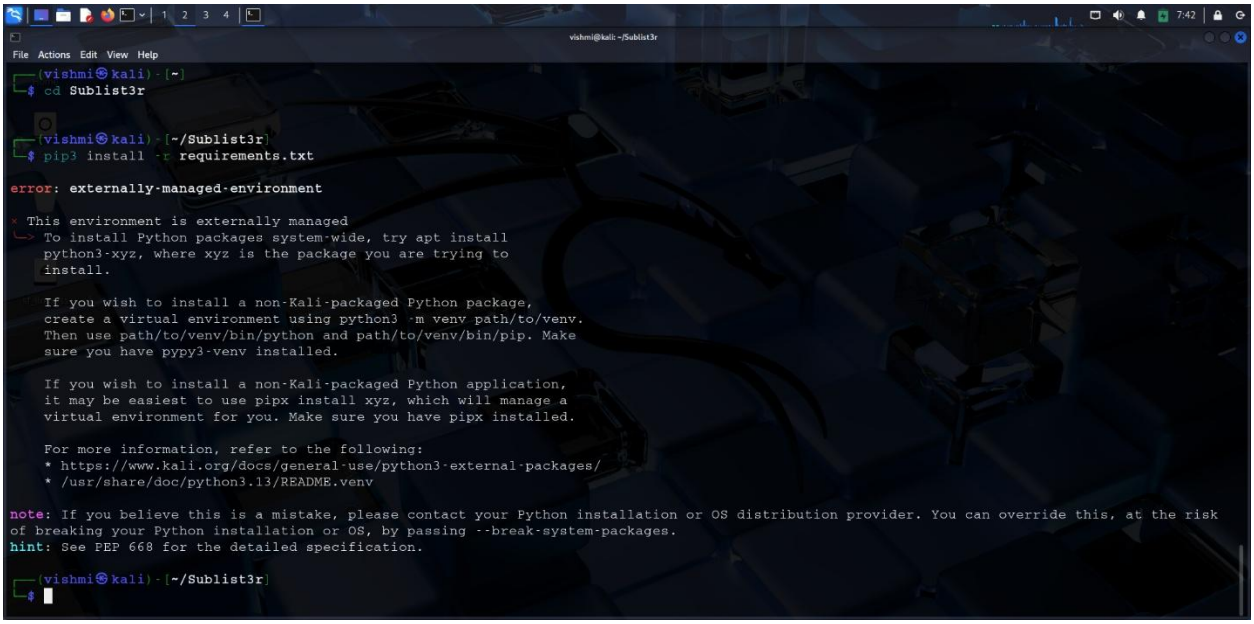
All of the files needed to install the application are contained in this repository. To download it, run the following command in your shell.

"git clone https://github.com/aboul3la/Sublist3r.git"



Once the files have been downloaded, navigate to the "Sublist3r" directory and install the required documents by typing

"pip3 install -r requirements.txt "

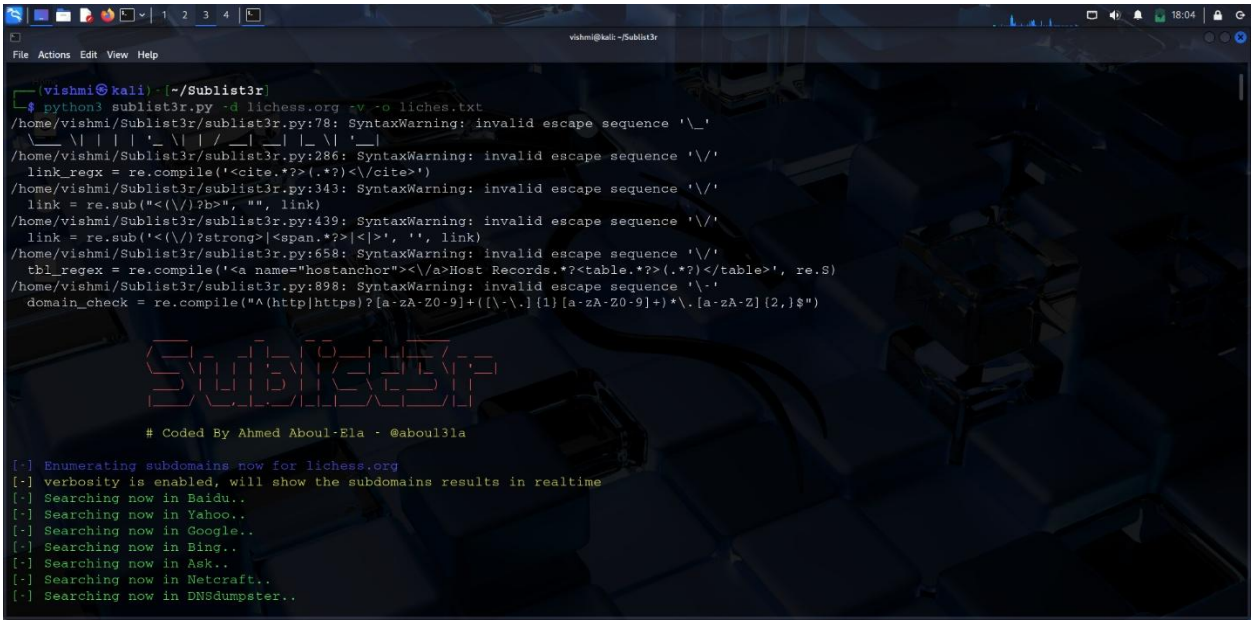


After installing the requirements, enter

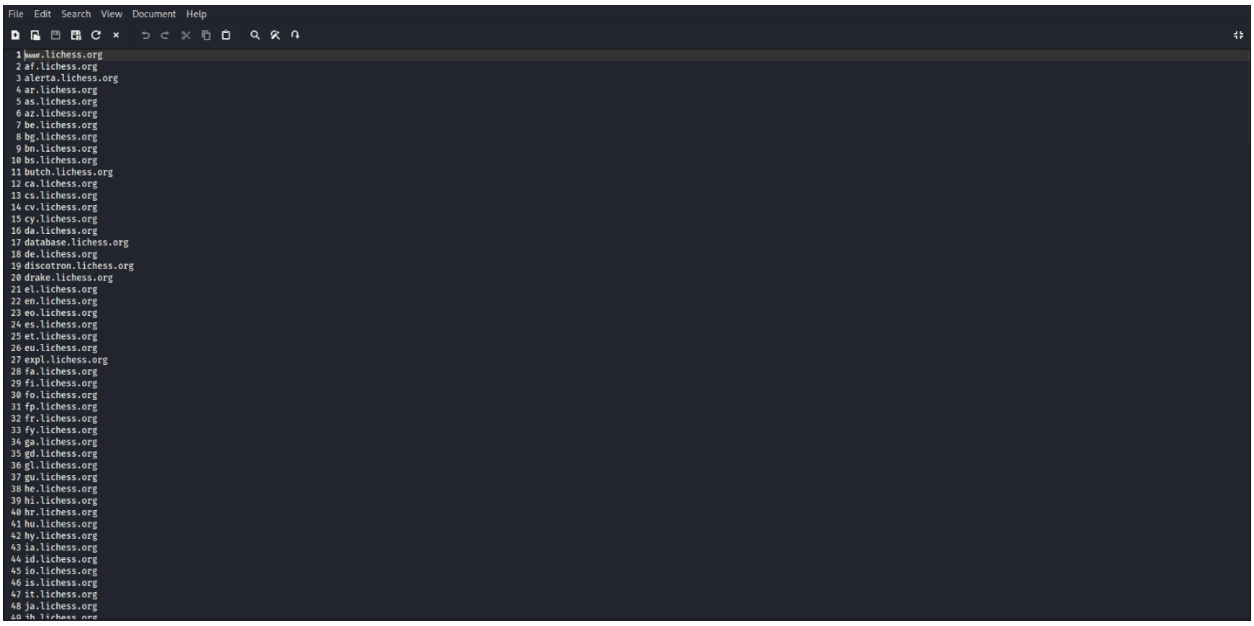
python3 sublist3r.py -d <domain_name>

Before that, I created a .txt file to store the subdomain headers that were initiated via sublist3r.

Path to .txt file = ***home/kali/Documents/audit/lichess/lichess.txt***



After opening lichess.txt file, I got these subdomains in lichess.

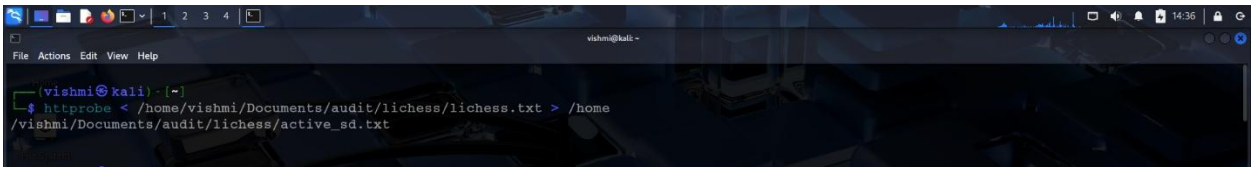


HTTProbe

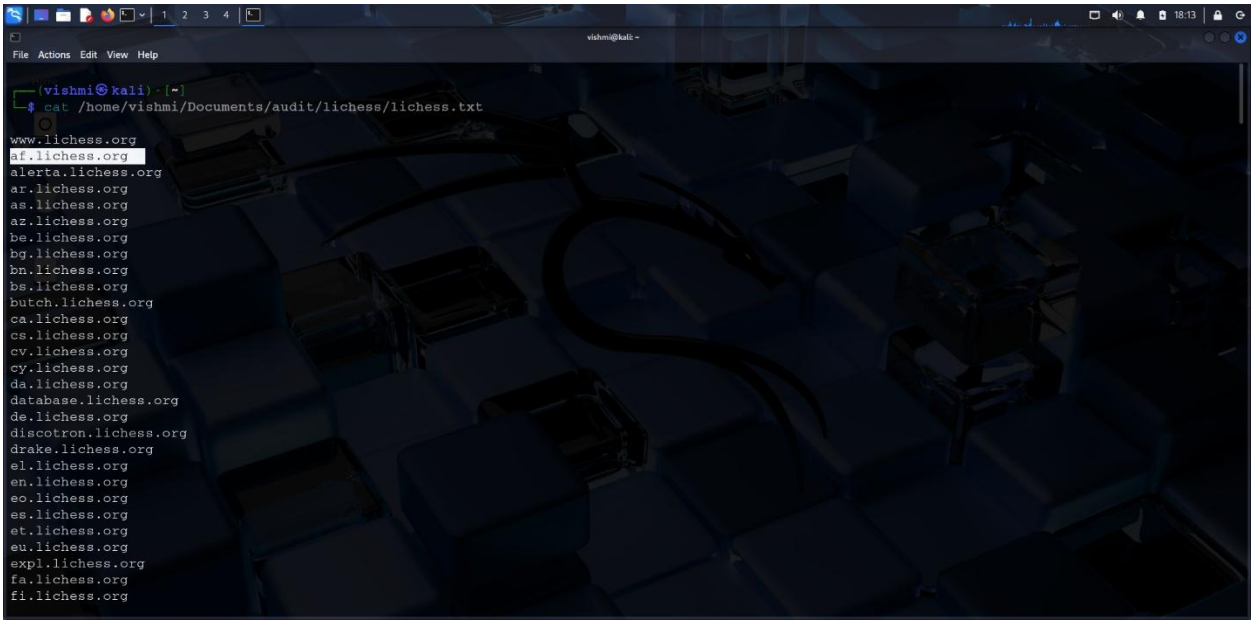
HTTProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing on achievable goals by providing you with the URLs of active domains.

First, I installed httprobe.

After that, I am using the text file generated before by the sublist3r and stored the active subdomains to another new .txt file.



Below, we can see the active subdomains related to the ***lichess.org*** domain.

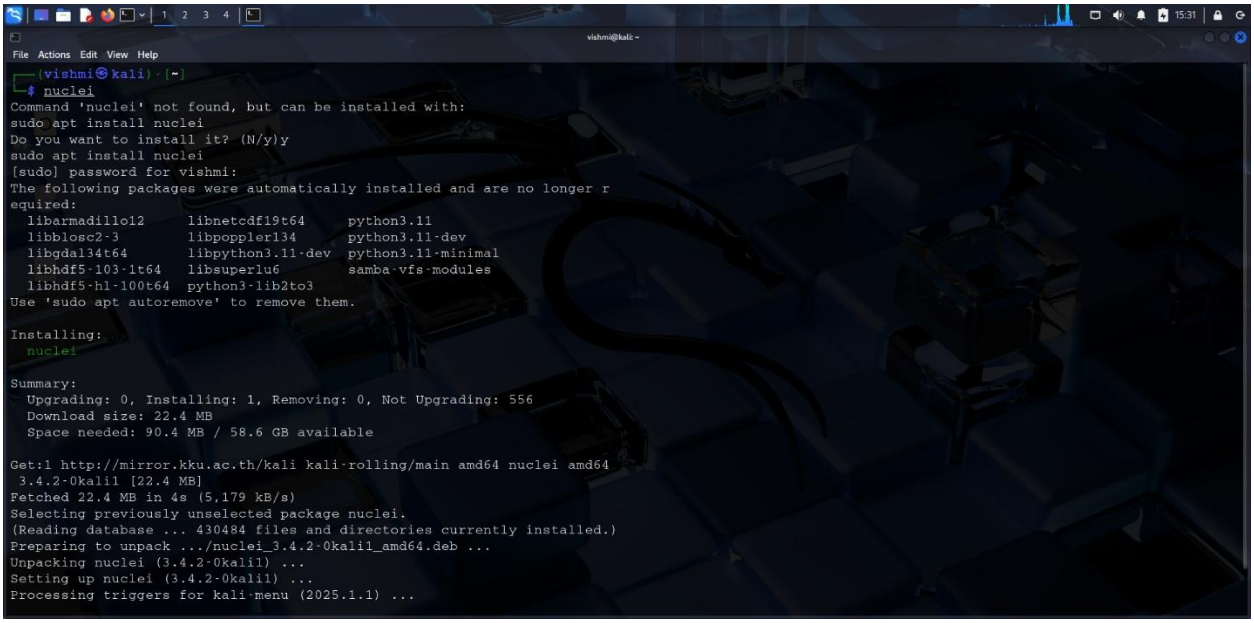


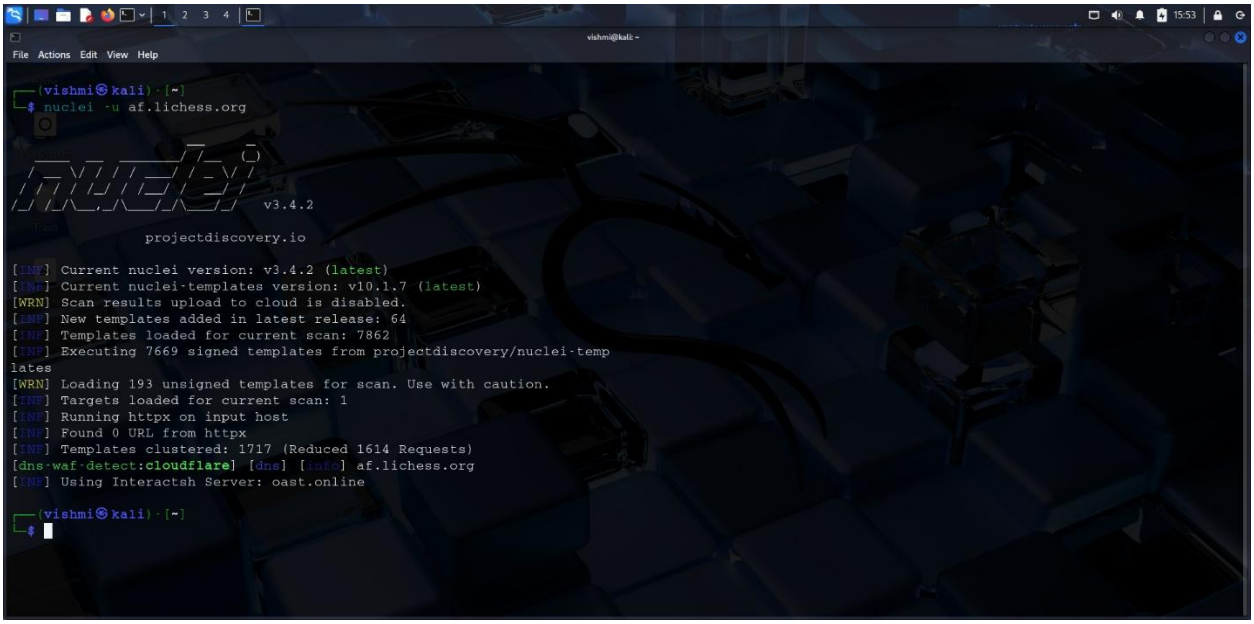
To move forward, I chose the active subdomain as **“af.lichess.org”.**

Nuclei

Nuclei is an open-source vulnerability scanner developed by ProjectDiscovery for security professionals, penetration testers, and bug bounty hunters. It uses customizable YAML("Yet Another Markup Language") -based templates to identify vulnerabilities such as misconfigurations, outdated software, and known CVEs (Common Vulnerabilities and Exposures).

First, I installed nuclei.

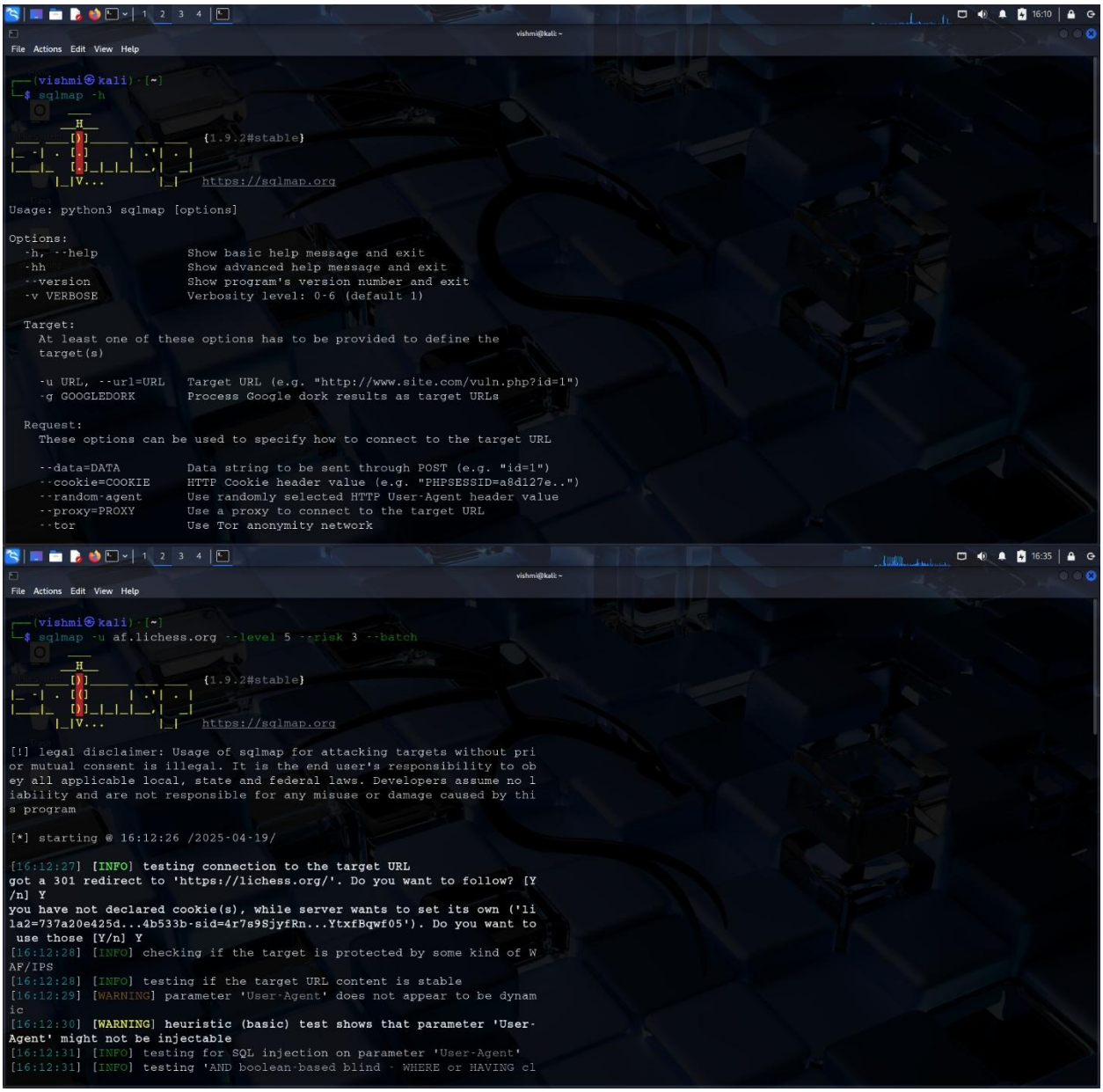




Vulnerability Type	Description	Risk
Dns-waf-detect [cloudflare]	By using Cloudflare Web Application Firewall (WAF), the domain *af.lichess.org is* protected. Through the filtering and blocking of malicious traffic, security is improved.	Low/ Informational

SQLmap

An open-source penetration testing tool called SQLmap makes it easier to find and take advantage of SQL injection flaws in web apps. If the database permits, it can even access the underlying file system or run commands on the server in addition to identifying the type of database and extracting data. Security experts frequently use it to evaluate and protect web apps from SQL injection attacks.



Option	Meaning
-u	For basic testing, the target URL is required.
--level5	Increases the number of payloads and tests that are done (maximum is 5).
--risk3	Increase the danger level of the payloads used (maximum is 3)
--batch	Executes SQLMap in a non-interactive mode, selecting default responses automatically.

Detected Information

* ***[WARNING] heuristic (basic) test shows that parameter 'User-Agent' might be injectable***

[This is a *potential* vulnerability, but not confirmed.]

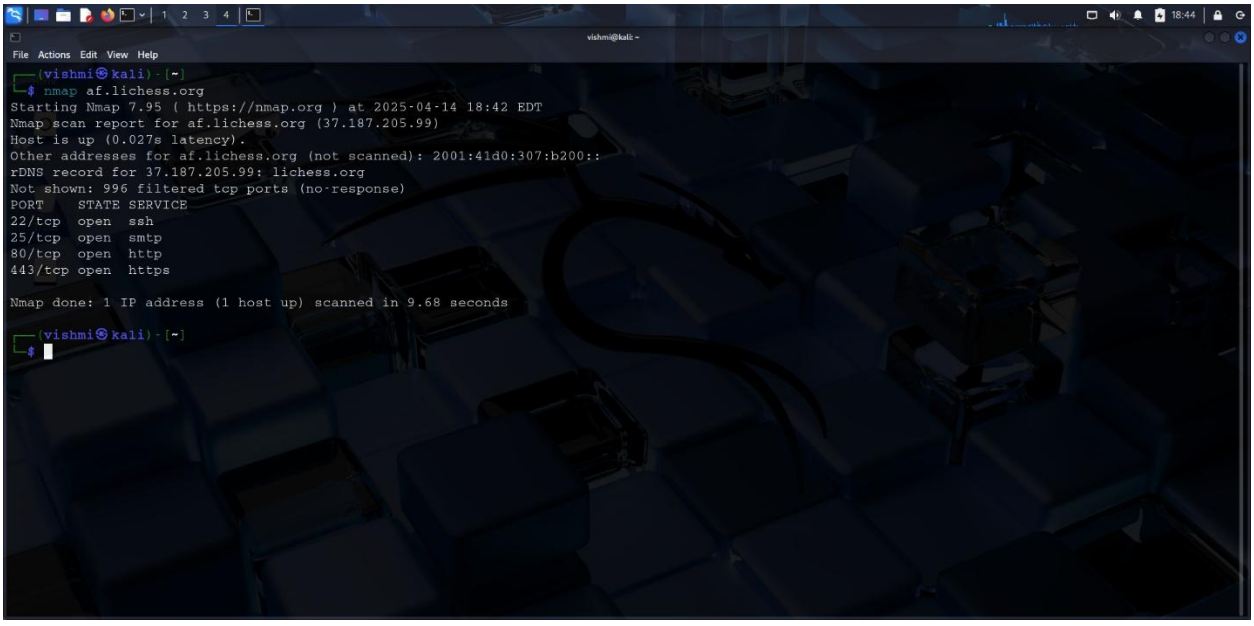
* ***[INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'***

[SQLmap is still in the process of testing for SQL injection using Boolean-based techniques.]

Searching for vulnerabilities

Nmap

Nmap (Network Mapper) is a strong, open-source network scanning program that uses packet transmission and response analysis to find hosts and services on a computer network. To find open ports, running services, operating systems, and active devices on a network, network managers and security experts utilize Nmap. Network inventory, vulnerability assessment, security auditing, and penetration testing are among its many uses.



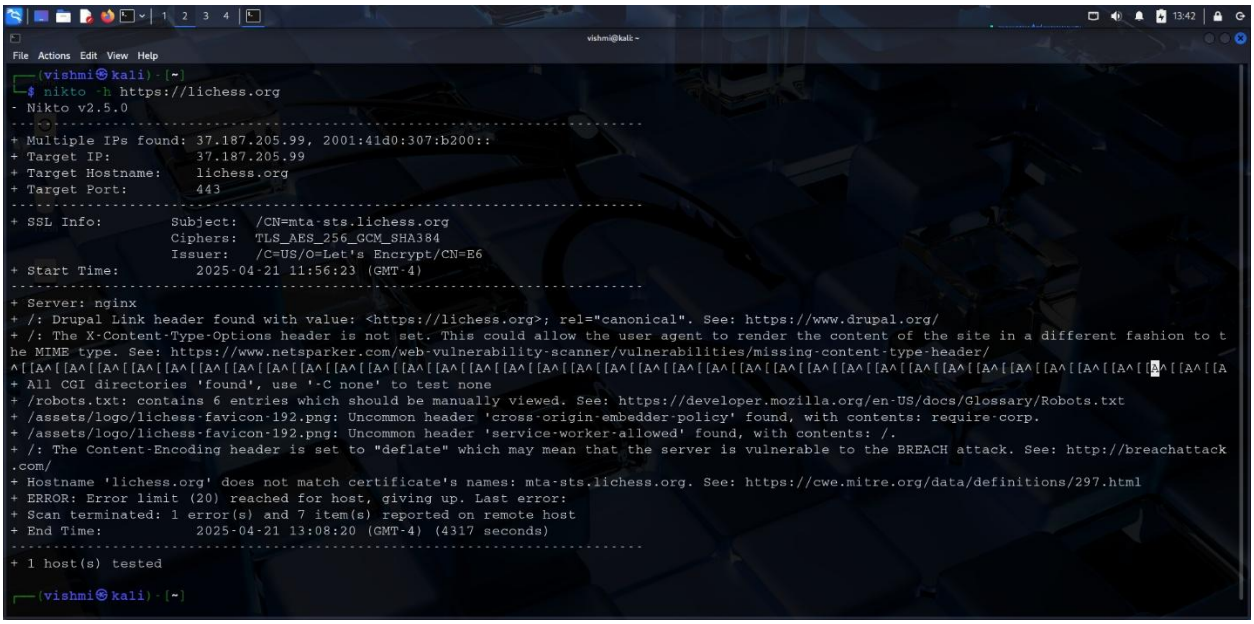
I discovered these details by using Nmap to search *af.lichess.org*.

PORT	STATE	SERVICE
22/tcp	open	ssh
25/tcp	open	smtp
80/tcp	open	http
443/tcp	open	https

PORT	SERVICE	Vulnerabilities
22/tcp	ssh	Vulnerable to outdated versions with known exploits and brute-force attacks.
25/tcp	smtp	Abuseable for spoofing/phishing attacks or as an open relay
80/tcp	http	Vulnerable to popular online threats such as SQLi and XSS, as well as unencrypted data transfer.
443/tcp	https	Risks include outdated libraries like Heartbleed-prone OpenSSL and SSL/TLS misconfigurations.

Nikto

An open-source program called Nikto scans web servers for common vulnerabilities, malicious files, outdated software, and improperly configured settings, among other potential security issues. It is widely used for penetration testing and assessments, but it functions best when combined with other tools.



Security issues found on ***https://lichess.org's*** by Nikto Scan

***** The X-Content-Type-Options header is not set.

***** The certificate name "mta-sts.lichess.org" and the hostname "lichess.org" are not the same.

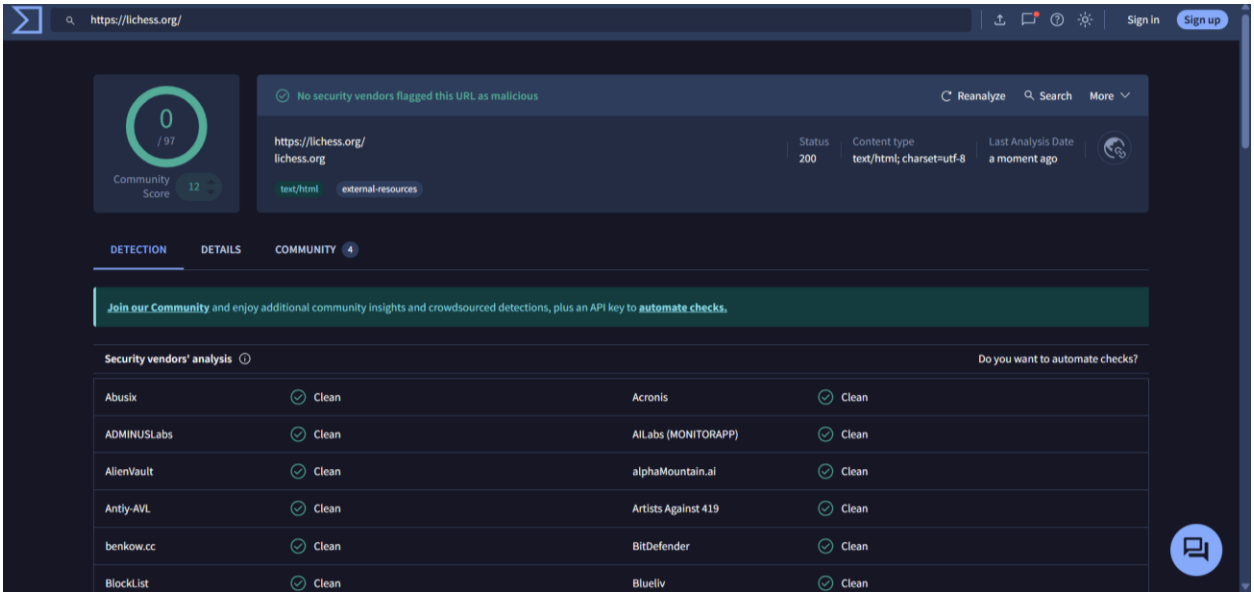
***** robots.txt contains 6 entries that should be manually viewed .

***** The resources 'cross-origin-embedder-policy' and'service-worker-allowed' were found to have uncommon headers.

Virustotal

Virustotal is a free web service called VirusTotal employs 70 antivirus engines and URL blocklisting services to scan files and URLs for malware, adware, and other malicious content.
I entered https://lichess.org in URL section .

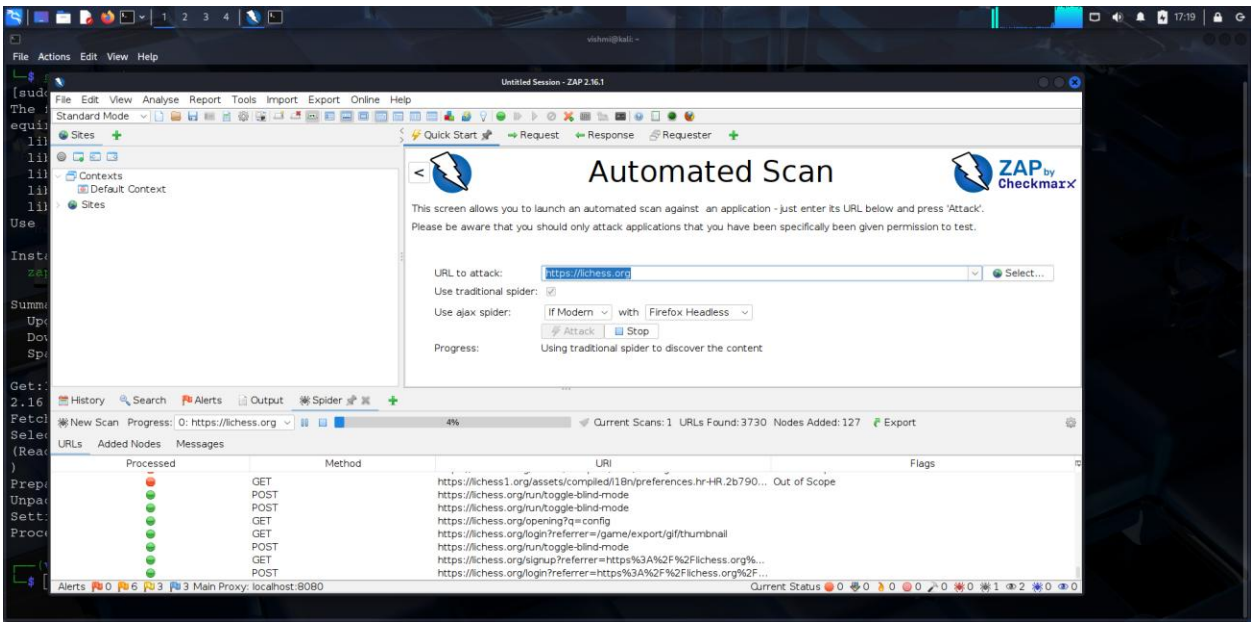
As a result, I got this summary .



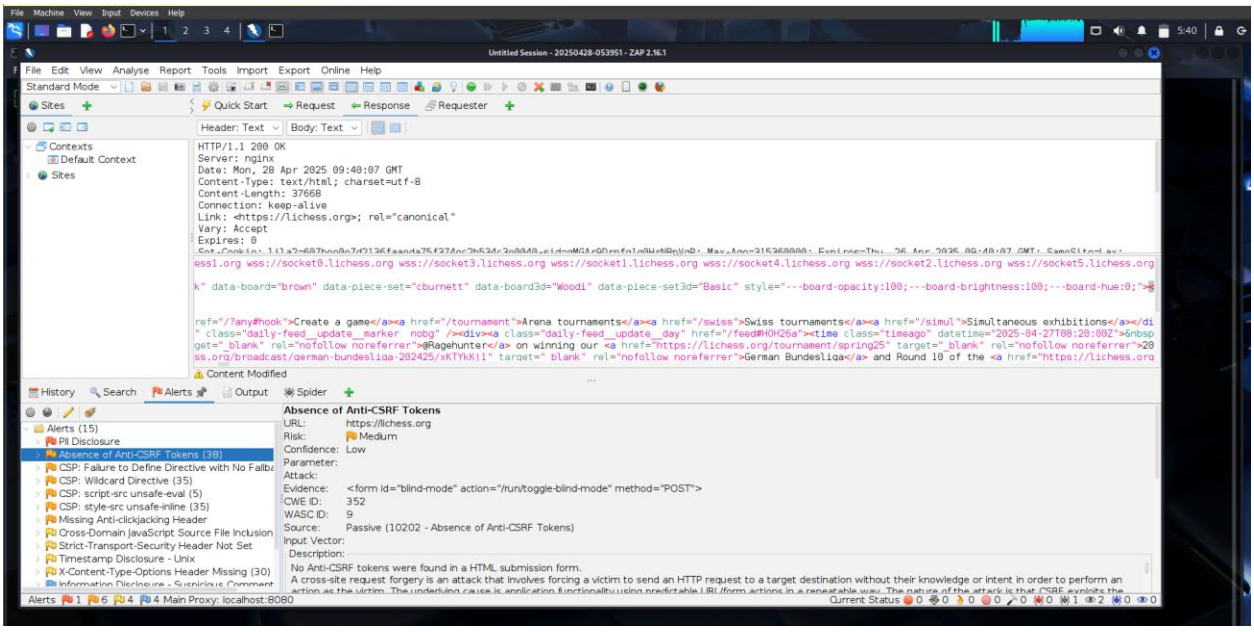
OWASP ZAP

A free and open-source security tool called ***OWASP ZAP (Zed Attack Proxy)*** simulates attacks and examines how an application behaves when it is running to help in discovering and fixing vulnerabilities in web applications.

In here, I entered the target URL [***https://lichess.org***] designated textbox, simply select "Attack" to initiate the scanning process.



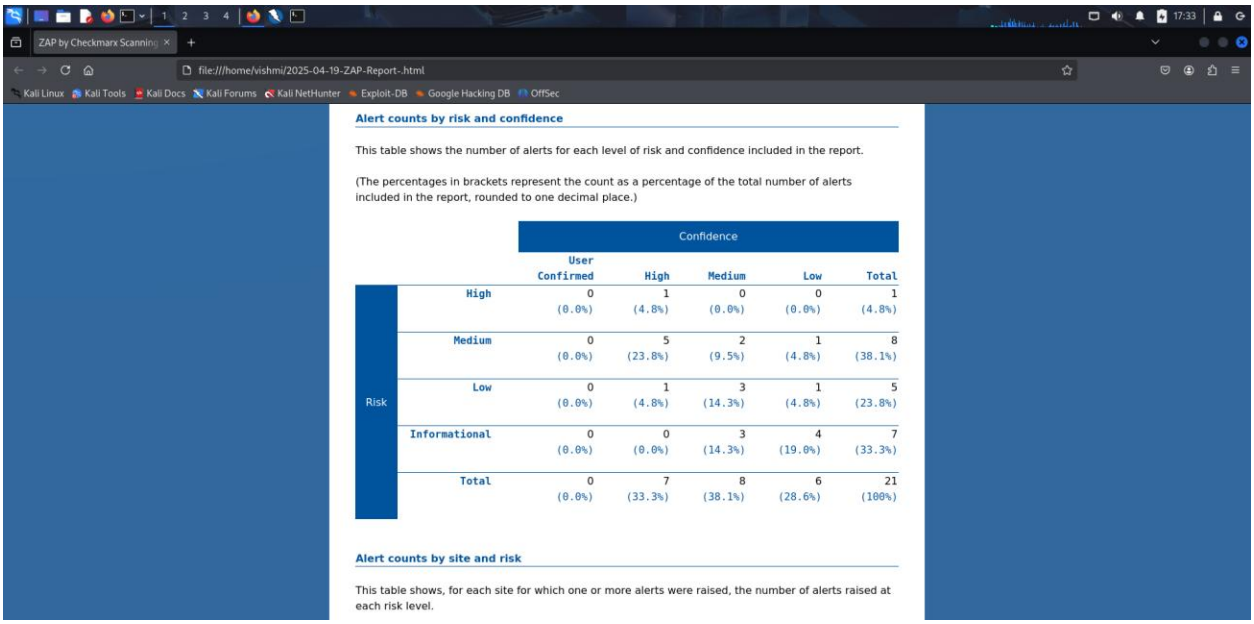
As next step, I entered to the Alerts tab. Here it's detected a vulnerability.



After finishing, it is possible to obtain a thorough report of the results by choosing "Report." The results of scanning many domains are displayed in the screenshots below.

Report = *file:///home/vishmi/2025-04-19-ZAP-Report-.html*

Please take note that these vulnerabilities have been rated using the OWASP risk rating methodology, which is available at this link.[*OWASP Risk Rating Methodology*]



Alert counts by risk and confidence

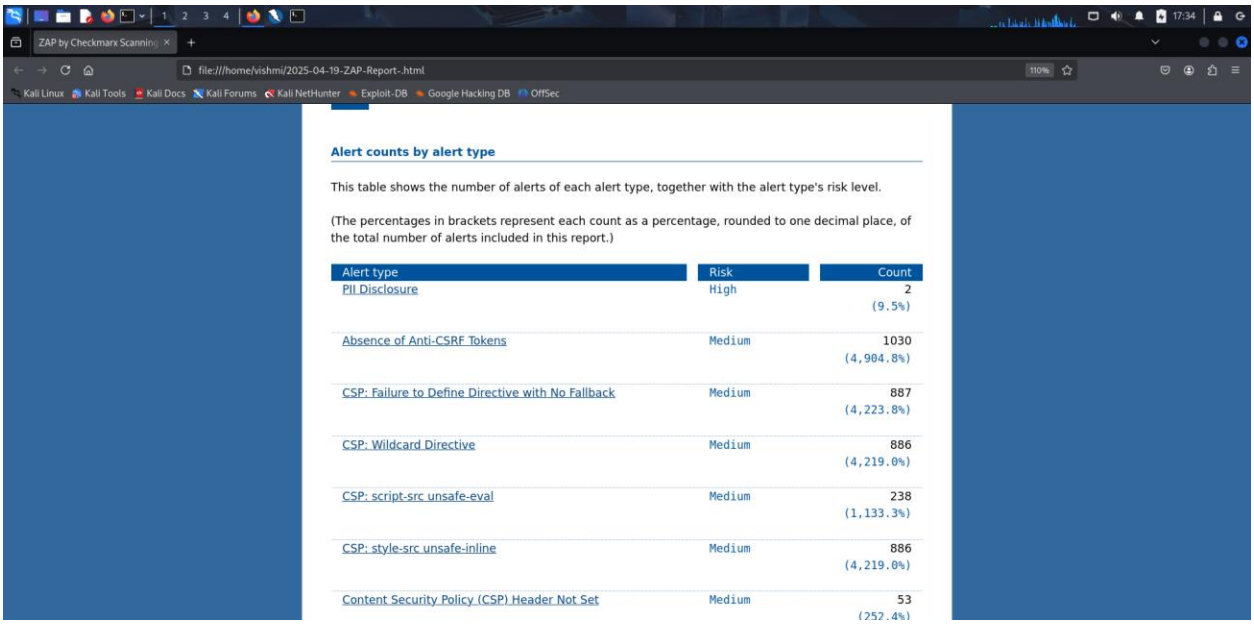
This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	1 (4.8%)	0 (0.0%)	0 (0.0%)	1 (4.8%)
	Medium	0 (0.0%)	5 (23.8%)	2 (9.5%)	1 (4.8%)	8 (38.1%)
	Low	0 (0.0%)	1 (4.8%)	3 (14.3%)	1 (4.8%)	5 (23.8%)
	Informational	0 (0.0%)	0 (0.0%)	3 (14.3%)	4 (19.0%)	7 (33.3%)
	Total	0 (0.0%)	7 (33.3%)	8 (38.1%)	6 (28.6%)	21 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

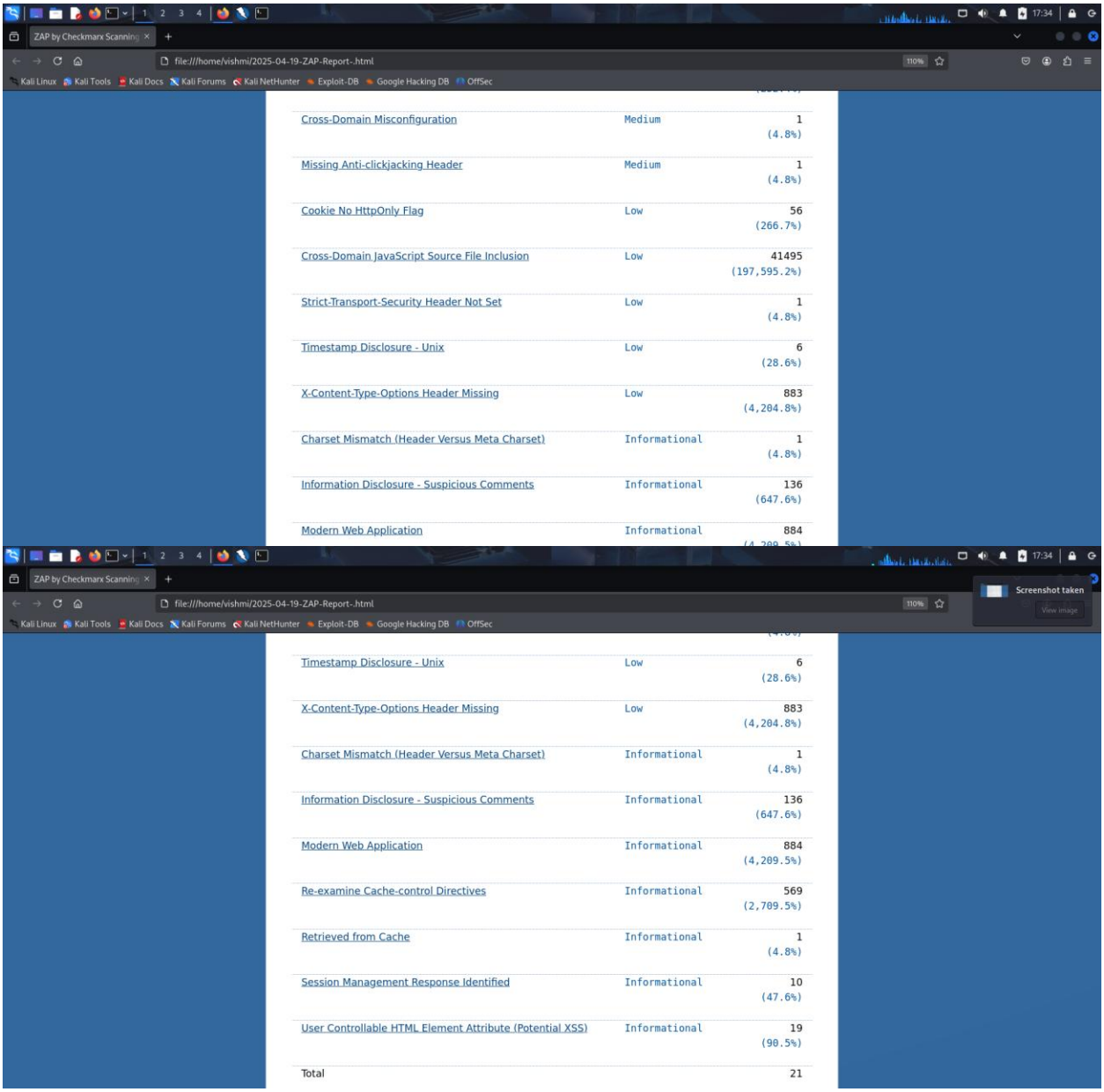


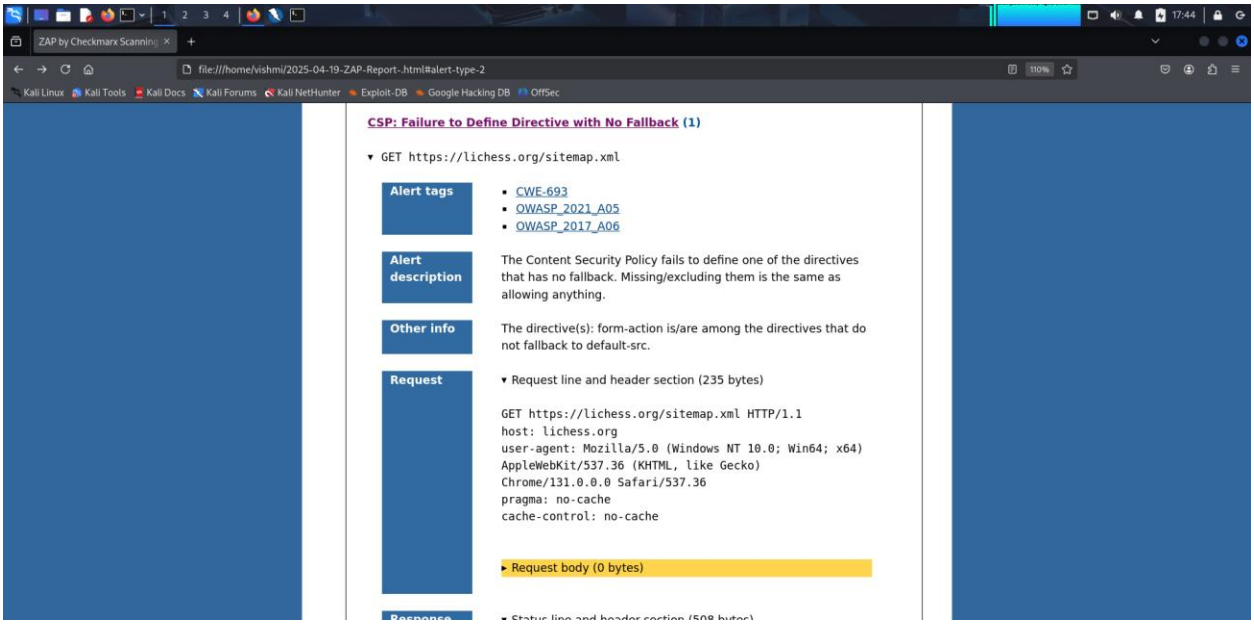
Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
PII Disclosure	High	2 (9.5%)
Absence of Anti-CSRF Tokens	Medium	1030 (4,904.8%)
CSP: Failure to Define Directive with No Fallback	Medium	887 (4,223.8%)
CSP: Wildcard Directive	Medium	886 (4,219.0%)
CSP: script-src unsafe-eval	Medium	238 (1,133.3%)
CSP: style-src unsafe-inline	Medium	886 (4,219.0%)
Content Security Policy (CSP) Header Not Set	Medium	53 (252.4%)


ZAP by Checkmarx Scanning
file:///home/vishmi/2025-04-19-ZAP-Report-.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Cross-Domain Misconfiguration Medium 1 (4.8%)
Missing Anti-clickjacking Header Medium 1 (4.8%)
Cookie No HttpOnly Flag Low 56 (266.7%)
Cross-Domain JavaScript Source File Inclusion Low 41495 (197,595.2%)
Strict-Transport-Security Header Not Set Low 1 (4.8%)
Timestamp Disclosure - Unix Low 6 (28.6%)
X-Content-Type-Options Header Missing Low 883 (4,204.8%)
Charset Mismatch (Header Versus Meta Charset) Informational 1 (4.8%)
Information Disclosure - Suspicious Comments Informational 136 (647.6%)
Modern Web Application Informational 884
Screenshot taken
Timestamp Disclosure - Unix Low 6 (28.6%)
X-Content-Type-Options Header Missing Low 883 (4,204.8%)
Charset Mismatch (Header Versus Meta Charset) Informational 1 (4.8%)
Information Disclosure - Suspicious Comments Informational 136 (647.6%)
Modern Web Application Informational 884 (4,209.5%)
Re-examine Cache-control Directives Informational 569 (2,709.5%)
Retrieved from Cache Informational 1 (4.8%)
Session Management Response Identified Informational 10 (47.6%)
User Controllable HTML Element Attribute (Potential XSS) Informational 19 (90.5%)
Total 21


ZAP by Checkmarx Scanning
file:///home/vishmi/2025-04-19-ZAP-Report-.html#alert-type-2
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
CSP: Failure to Define Directive with No Fallback (1)
GET https://lichess.org/sitemap.xml
Alert tags
CWE-693
OWASP_2021_A05
OWASP_2017_A06
Alert description
The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding them is the same as allowing anything.
Other info
The directive(s): form-action is/are among the directives that do not fallback to default-src.
Request
Request line and header section (235 bytes)
GET https://lichess.org/sitemap.xml HTTP/1.1
host: lichess.org
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
Request body (0 bytes)

Vulnerabilities

a.Vulnerability Title	**Absence of Anti-CSRF Tokens**
b.Vulnerability Description	Many application forms lack Anti-CSRF tokens, allowing server to determine if request was forged or purposefully performed by the authenticated user, exposing the application to CSRF attacks.
c.Affected Components	Any state-changing HTTP endpoint (such as POST, PUT, or DELETE requests) or HTML form that lacks an anti-CSRF token and is not validated. For instance, forms for changing a password or updating a user profile, or any sensitive transaction endpoints.
d.Impact Assessment	Attackers may execute out actions on behalf of authenticated users without their knowledge by taking advantage of the lack of anti-CSRF tokens. Depending on the behaviors reported by the susceptible endpoints, this could result in money loss, privilege escalation, data theft, or unauthorized changes to user accounts.
e.Steps to Reproduce	1. Sign in as an authorized user. 2. Find an endpoint or form (such updating a profile) that is missing an anti-CSRF token. 3. Make a malicious page that sends the identical form data to the intended application by copying the form's HTML. 4. Use a phishing email, for example, to trick a logged-in user into visiting the malicious page. 5. Verify the lack of CSRF protection by noting that the action was carried out on the user's behalf without their consent.
f.Proof of Concept (if applicable)	HTML form without CSRF token: *html <form action="https://vulnerable-app.com/change-email" method="POST"> <input type="email" name="email" value="attacker@example.com"> <input type="submit" value="Change Email"> </form> *
g.Proposed Mitigation or Fix	Implement unique, unpredictable, and validated anti-CSRF tokens in all forms and state-changing requests, use secure libraries, never send CSRF tokens in GET requests, ensure token expiry, and regularly test endpoints.

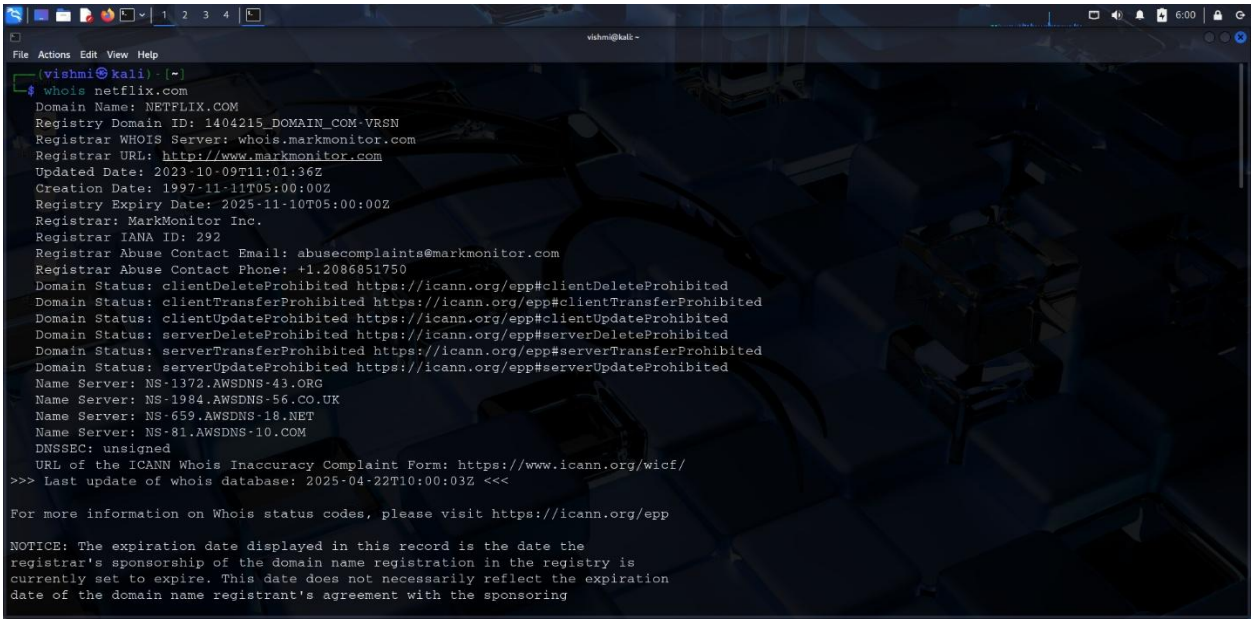
Report-02

Web Audit
netflix.com

Domain = *netflix.com*
Sub-domain = *www.netflix.com*
URL = *https://www.netflix.com*

Target Reconnaissance

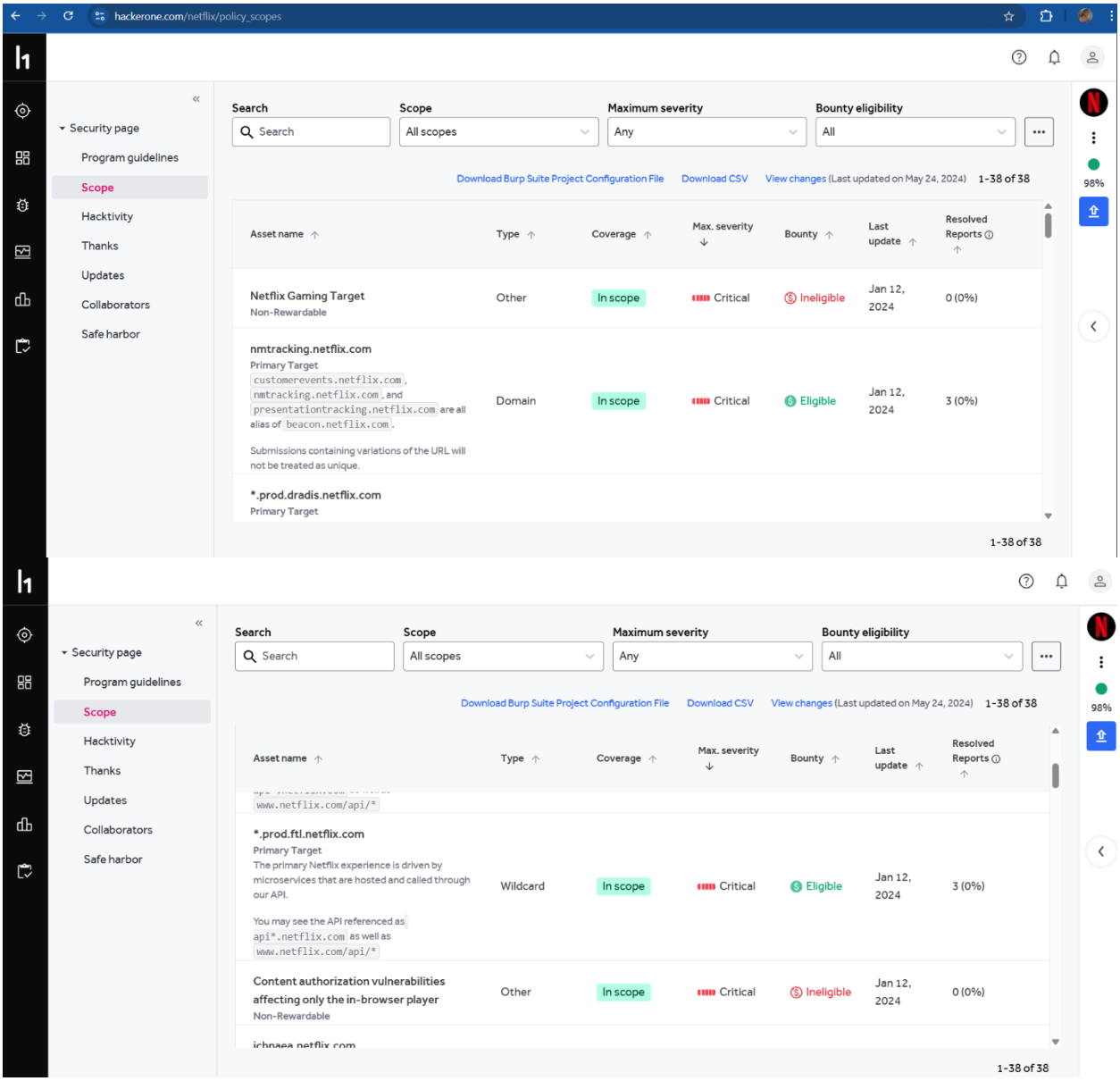
Introduction to Netflix and Audit Scope



“Netflix” was founded in the US and now offers material in a variety of languages and genres. On devices with internet access, users of Netflix's subscription-based streaming service can view a vast selection of TV series, films, documentaries, and original programs. With over 300 million paying customers in more than 190 countries . Apart from streaming, Netflix creates its own highly regarded original material and offers the option to watch whenever you want, download it for offline watching, and customize suggestions based on your viewing preferences.

These subdomains (and all included) have been approved as legitimate subdomains for testing in the **Hackerone** Bug Bounty program .

Eligible in-scope subdomains for bug bounty program are mentioned below



Information gathering phase.

The information-gathering phase, often known as reconnaissance or recon, is essential to both assessments of security and cyberattacks. In order to map out the target's structure and determine how it functions, the target of this stage is to gather as much information as possible about it. Because it helps auditors or attackers identify vulnerabilities that could be exploited later on, this fundamental understanding is essential.

There are two main approaches to information gathering

1.Active Scanning :

Involves direct interaction with the target, which can generate noticeable activity and typically uncovers a wealth of details about the system.

2.Passive Scanning :

Seeks to observe the target without direct engagement, resulting in less detectable activity but often providing more limited information.

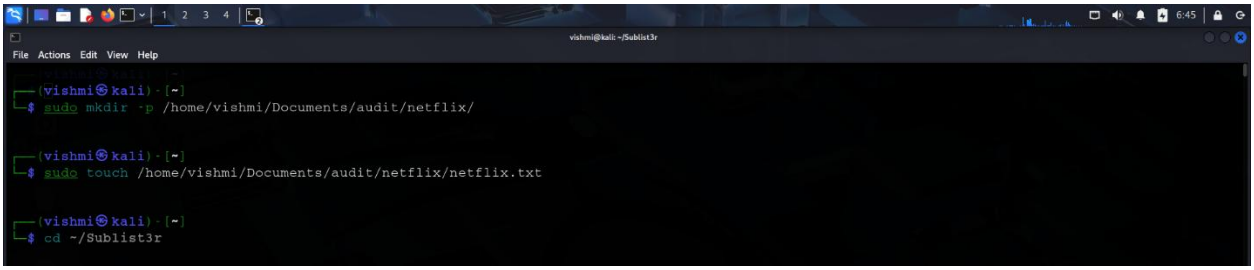
Finding active subdomains and their states

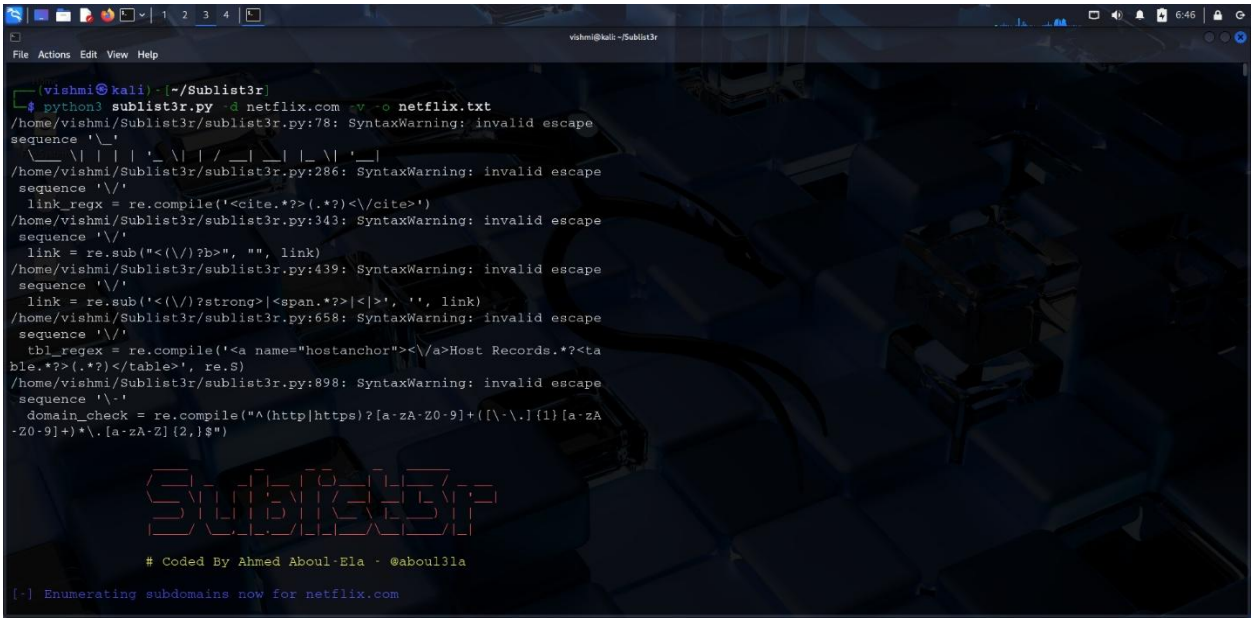
Sublist3r

Sublist3r is an open-source Python application that uses OSINT (Open Source Intelligence) techniques to quickly and effectively scan subdomains. Subdomains linked to a target domain can be found by penetration testers, security researchers, and bug bounty hunters using a variety of search engine queries (including Google, Yahoo, Bing, Baidu, and Ask). Additionally, Sublist3r includes a brute-force module (subbrute) to employ a stronger wordlist to improve the probability of discovering more subdomains.

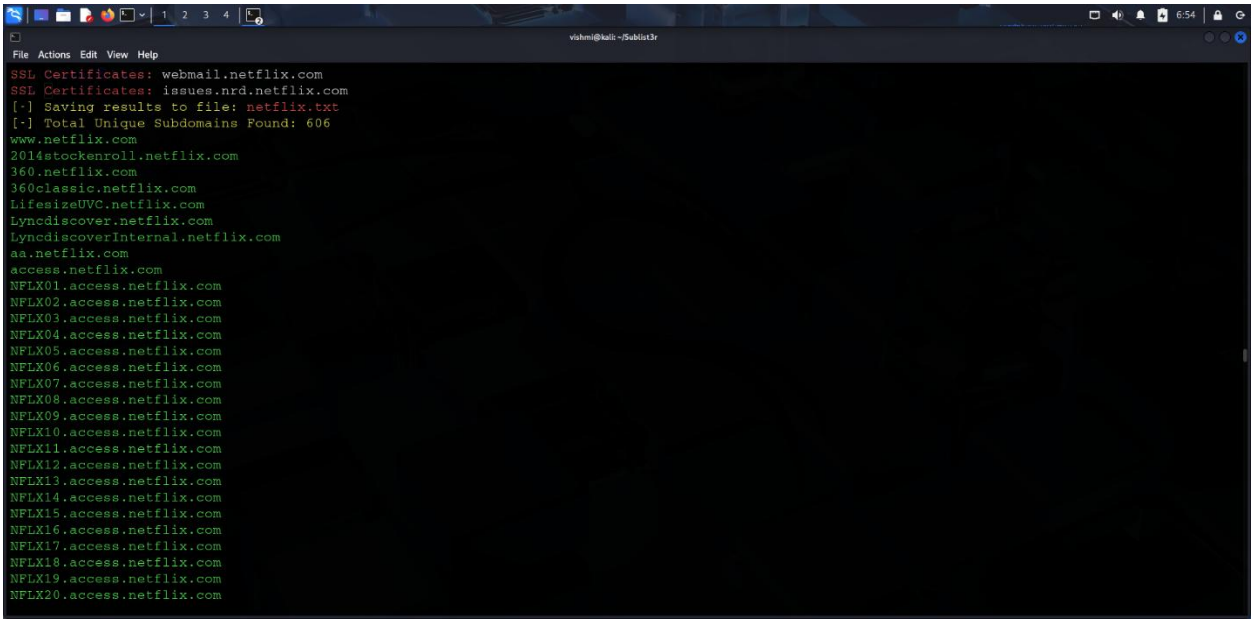
I created a .txt file to store the subdomain headers that were initiated via sublist3r.

Path to .txt file = ***home/vishmi/Documents/audit/netflix/netflix.txt***





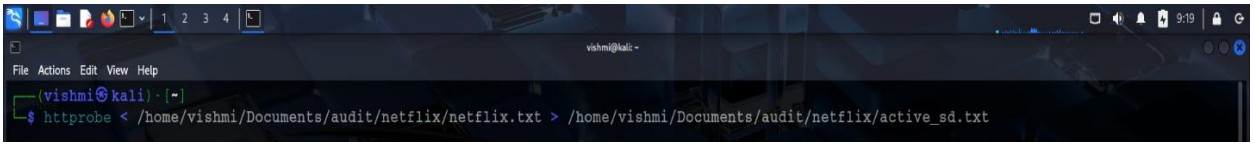
I got, these subdomains according to the ***netflix.com*** domain.



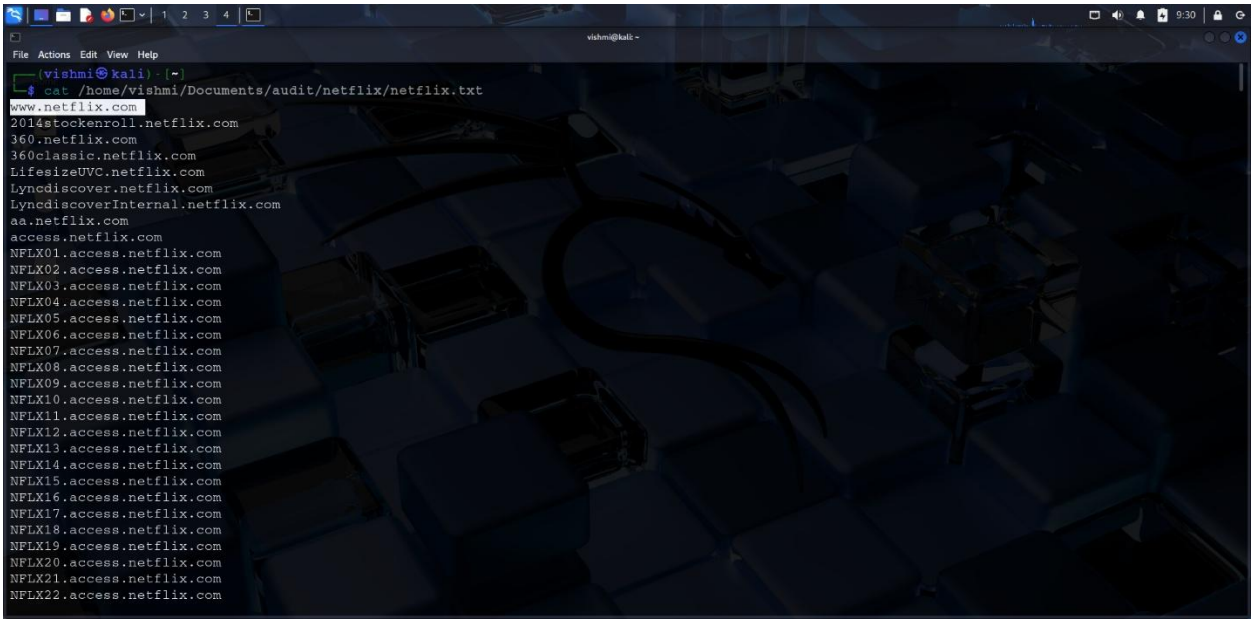
HTTProbe

HTTProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing on achievable goals by providing you with the URLs of active domains.

I am using the text file generated before by the sublist3r and stored the active subdomains to another new
.txt file.



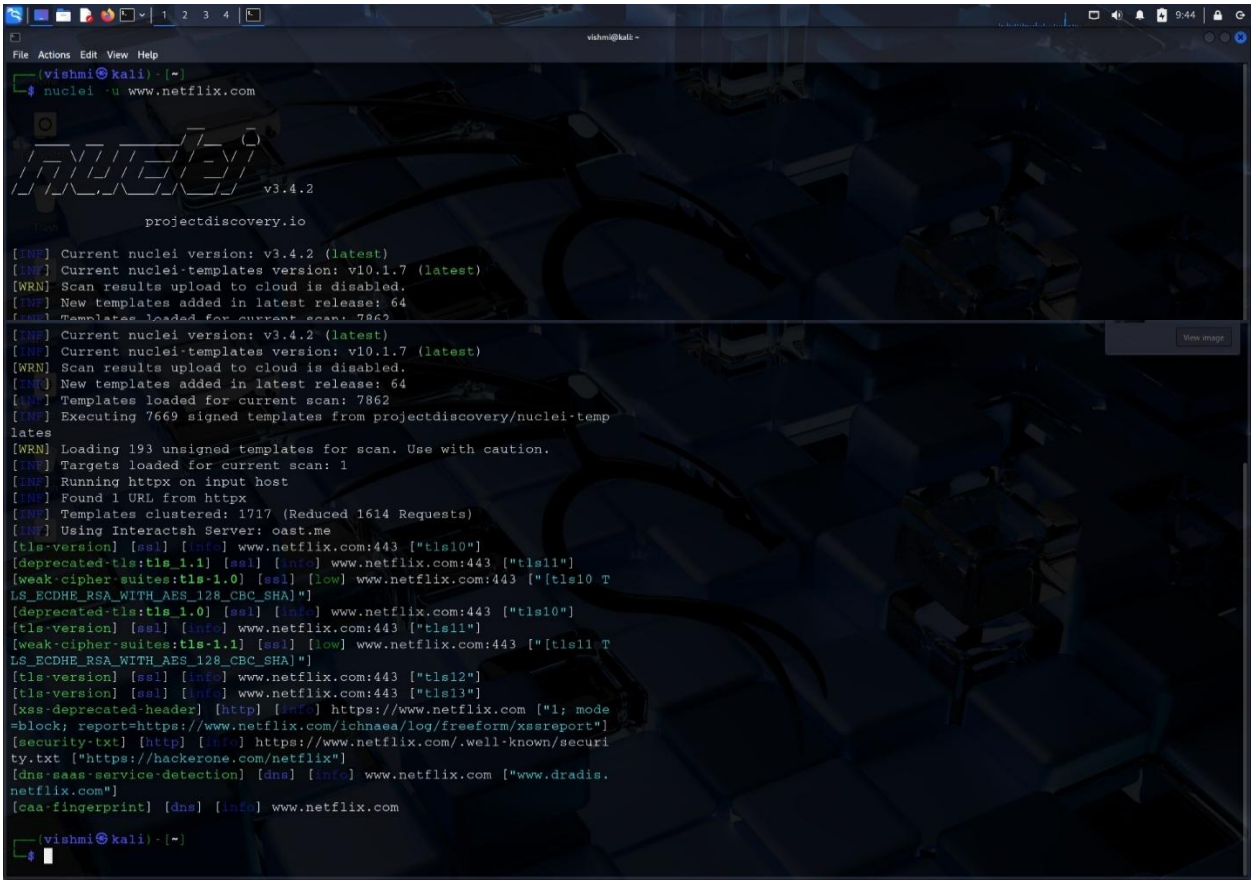
Below, we can see the active subdomains related to the ***netflix.com*** domain.



To move forward, I chose the active subdomain as **“www.netflix.com”.**

Nuclei

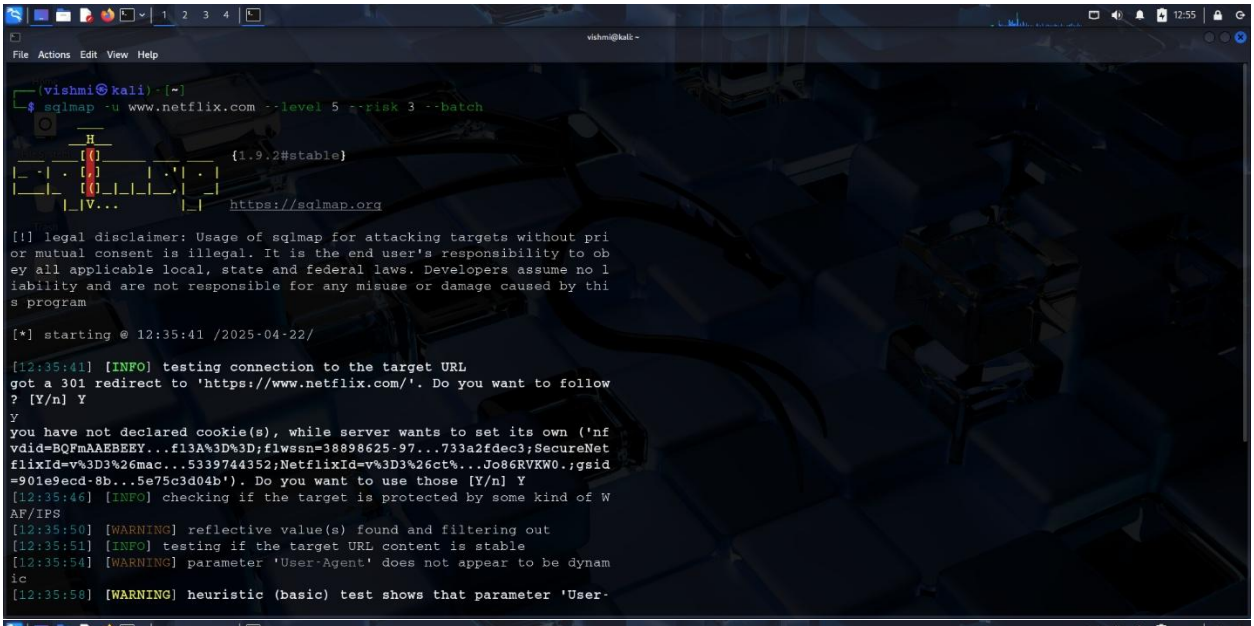
Nuclei is an open-source vulnerability scanner developed by ProjectDiscovery for security professionals, penetration testers, and bug bounty hunters. It uses customizable YAML("Yet Another Markup Language") -based templates to identify vulnerabilities such as misconfigurations, outdated software, and known CVEs (Common Vulnerabilities and Exposures).

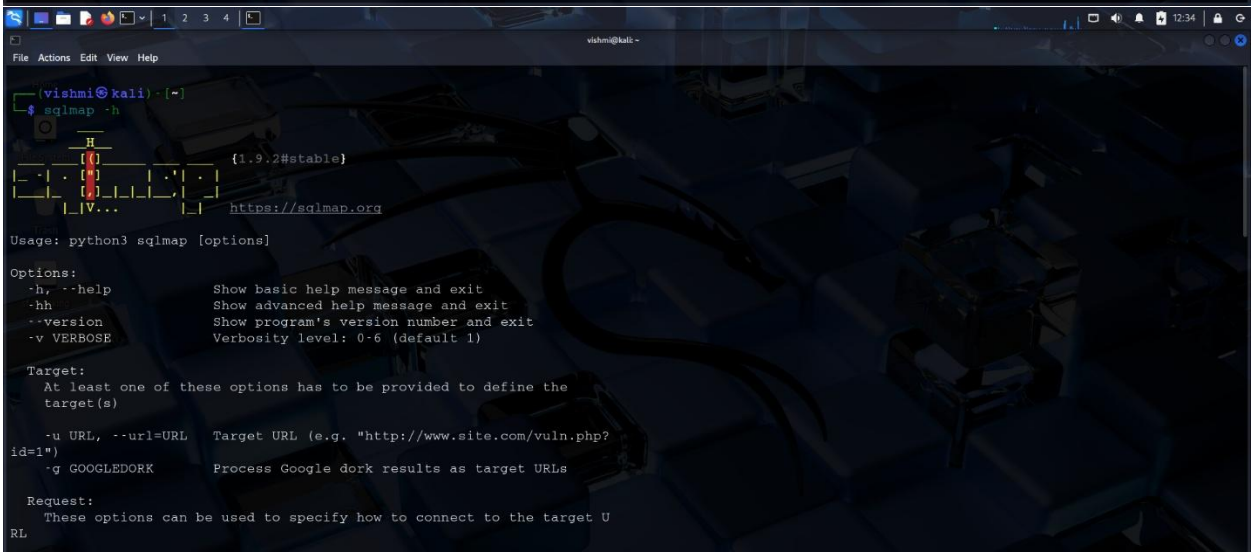


Vulnerable Title	Description	Risk
Deprecated TLS: TLS 1.1	The server is running TLS (1.1), an outdated version that is vulnerable to a number of cryptographic attacks and does not support current security features.	Low
Weak Cipher Suites: TLS 1.0	The server is vulnerable to cryptographic attacks like BEAST and POODLE since it uses TLS 1.0 and weak encryption techniques.	Low
Deprecated TLS: TLS 1.0	Because TLS 1.0 has known weaknesses, it should no longer be maintained as it is an antiquated and unsafe protocol.	Low
Weak Cipher Suites: TLS 1.1	Despite being marginally more secure than TLS 1.0, TLS 1.1 continues to use outdated cypher suites that are not regarded as robust by contemporary standards.	Low
XSS Deprecated Header	The server's outdated X-XSS-Protection header provides insufficient protection against cross-site scripting attacks, which is now deprecated and may create a false sense of security.	Medium
Security.txt Missing or Misconfigured	The security.txt file provides instructions for ethical hackers to report security concerns but may not be sufficient for security researchers to inform site owners of vulnerabilities.	Low
DNS SaaS Service Detection	The domain's DNS records reveal the use of third-party DNS SaaS providers, which could potentially expand the attack surface or reveal infrastructure information.	Low
CAA Fingerprint Found	The Certificate Authority Authorization (CAA) record lists the Certificate Authorities authorized to issue domain certificates, which can provide attackers with information about SSL configuration.	Low

SQLmap

An open-source penetration testing tool called SQLmap makes it easier to find and take advantage of SQL injection flaws in web apps. If the database permits, it can even access the underlying file system or run commands on the server in addition to identifying the type of database and extracting data. Security experts frequently use it to evaluate and protect web apps from SQL injection attacks.





Option	Meaning
-u	For basic testing, the target URL is required.
--level5	Increases the number of payloads and tests that are done (maximum is 5).
--risk3	Increase the danger level of the payloads used (maximum is 3)
--batch	Executes SQLMap in a non-interactive mode, selecting default responses automatically.

Detected Information

* ***[WARNING] heuristic (basic) test shows that parameter 'User-Agent' might be injectable***

[This is a *potential* vulnerability, but not confirmed.]

* ***[INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'***

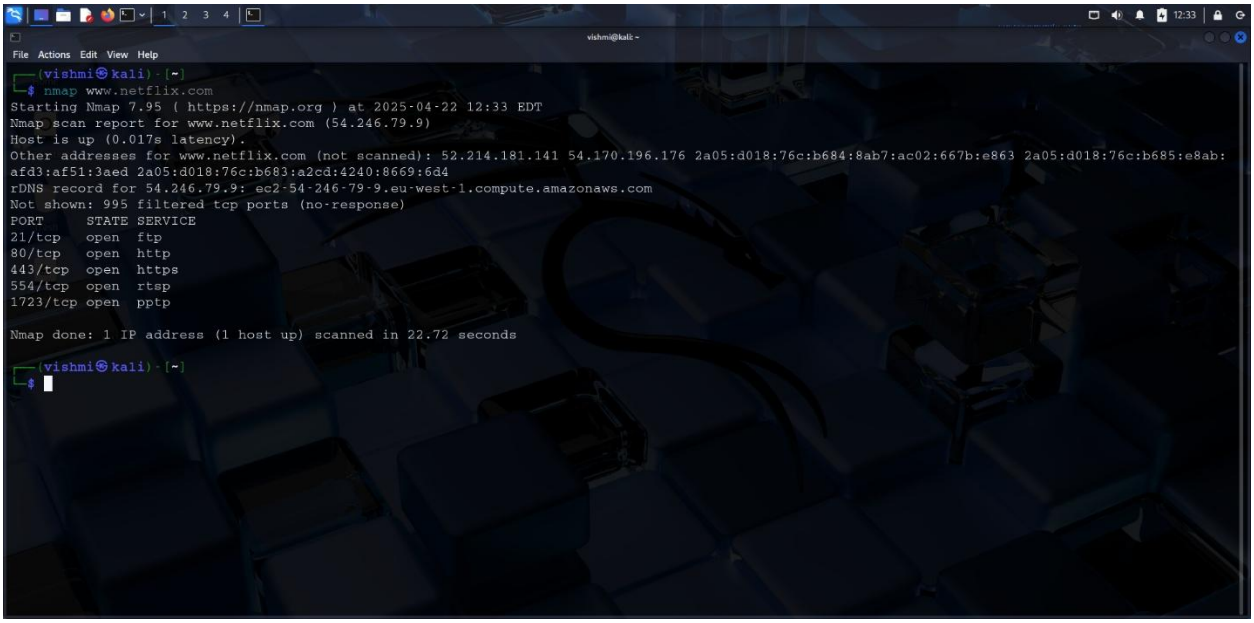
[SQLmap is still in the process of testing for SQL injection using Boolean-based techniques.]

**** [CRITICAL] Can't establish SSL connection.***

Searching for vulnerabilities

Nmap

Nmap (Network Mapper) is a strong, open-source network scanning program that uses packet transmission and response analysis to find hosts and services on a computer network. To find open ports, running services, operating systems, and active devices on a network, network managers and security experts utilize Nmap. Network inventory, vulnerability assessment, security auditing, and penetration testing are among its many uses.



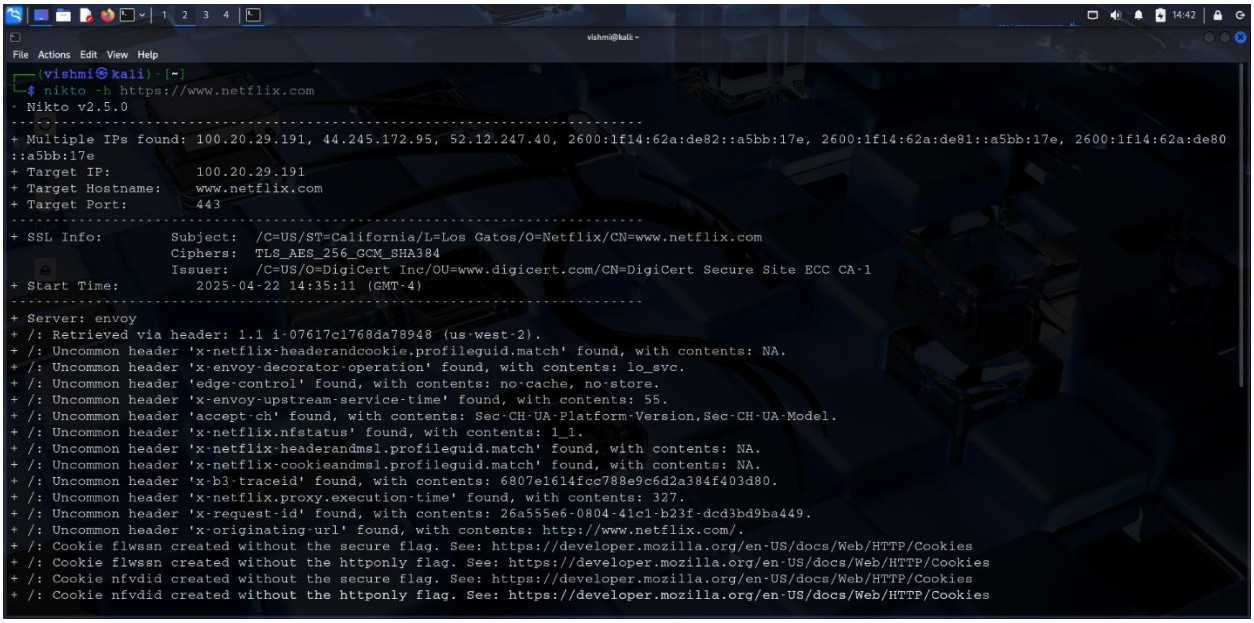
I discovered these details by using Nmap to search *www.netflix.com.*

PORT	STATE	SERVICE
21/tcp	open	ftp
80/tcp	open	http
443/tcp	open	https
554/tcp	open	rtsp
1723/tcp	open	pptp

PORT	SERVICE	Vulnerabilities
21/tcp	ftp	Unencrypted credentials are accepted.
80/tcp	http	Transmits plain text data.
443/tcp	https	Deprecated TLS versions are supported.
554/tcp	Rtsp	Usually doesn't have authenticity.
1723/tcp	pptp	Makes use of a weak encryption

Nikto

An open-source program called Nikto scans web servers for common vulnerabilities, malicious files, outdated software, and improperly configured settings, among other potential security issues. It is widely used for penetration testing and assessments, but it functions best when combined with other tools.



Security issues found on ***https://netiflix.com's*** by Nikto Scan.

*Uncommon header 'x-netflix-headerandcookieprofileguid.match' found.

*Uncommon header 'x-envoy-decorator-operation' found.

*Uncommon header 'edge-control' found.

*Uncommon header 'x-envoy-upstream-service-time' found.

*Uncommon header 'accept-ch' found.

*Uncommon header 'x-netflix.nfstatus' found.

*Cookie 'flwssn' created without the HTTPOnly and Secure flag.

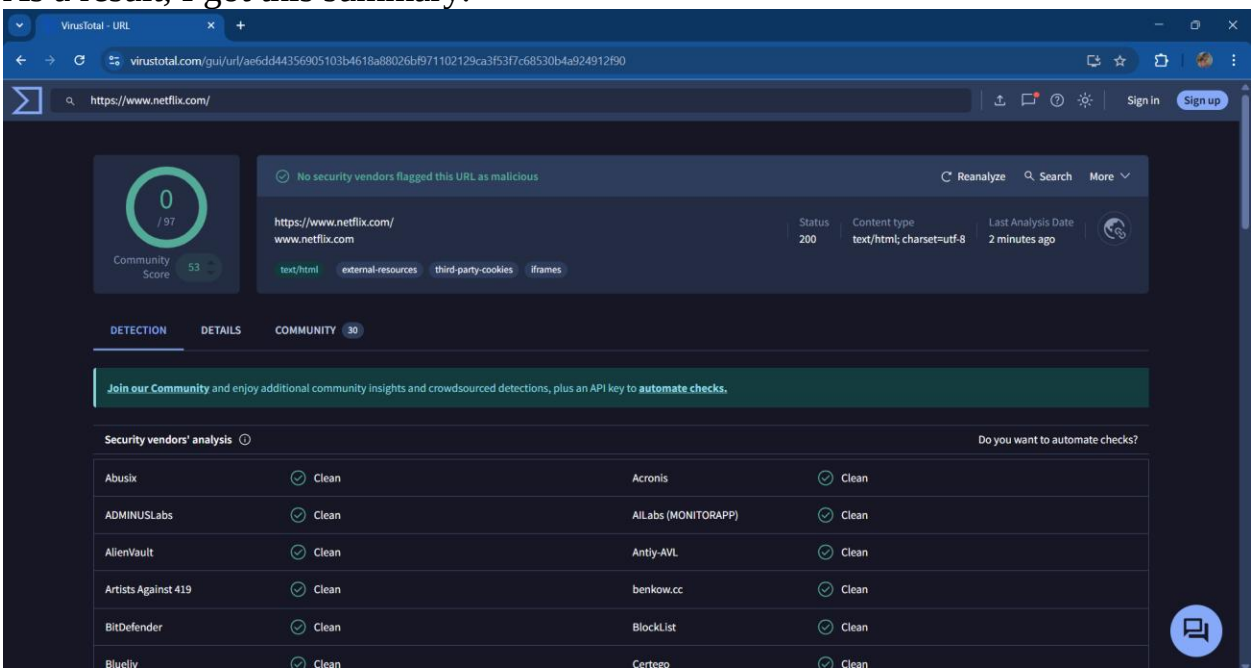
*Cookie 'nfvdid' created without the HTTPOnly and Secure flag.

Virustotal

Virustotal is a free web service called VirusTotal employs 70 antivirus engines and URL blocklisting services to scan files and URLs for malware, adware, and other malicious content.

I entered https://www.netflix.com in URL section .

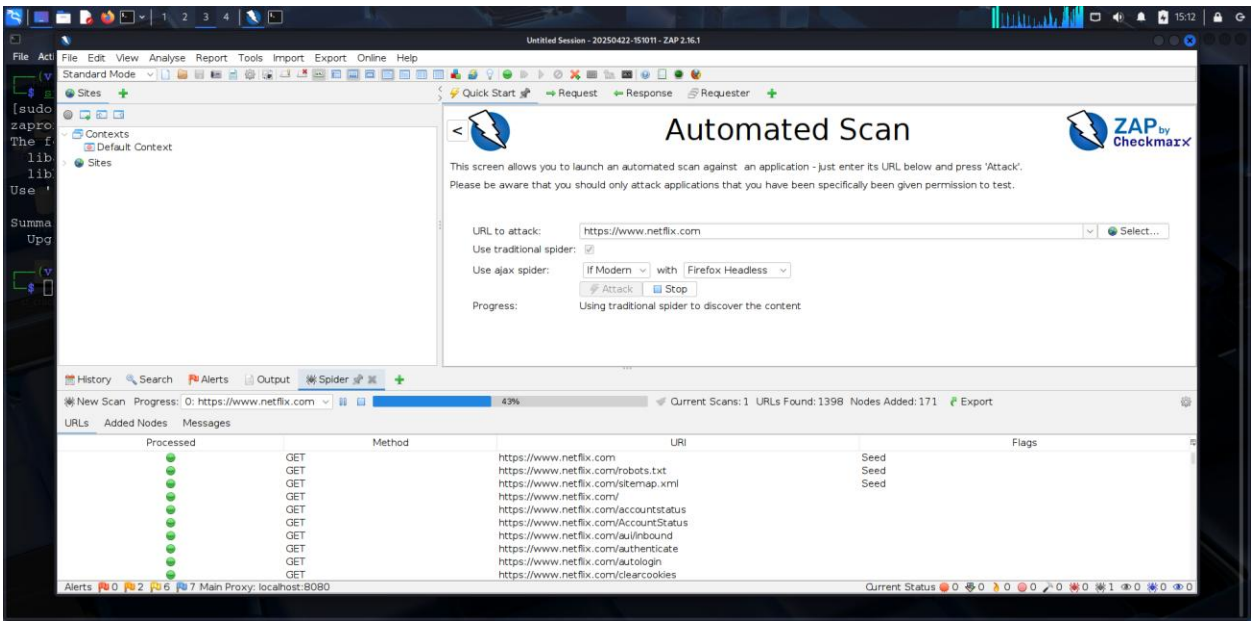
As a result, I got this summary.



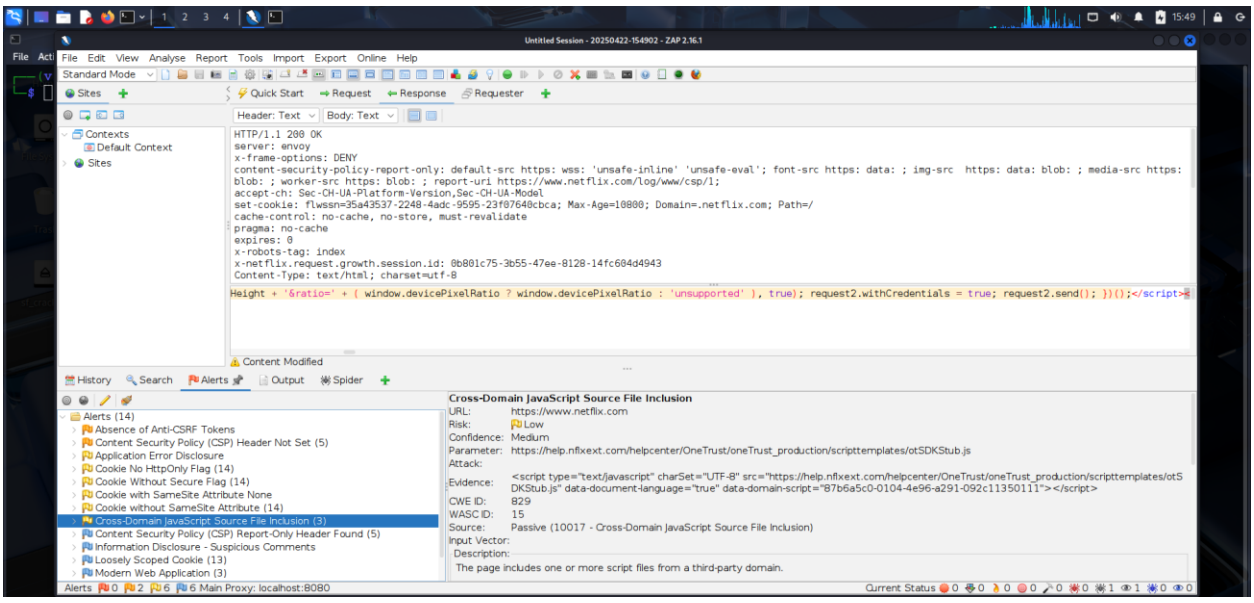
OWASP ZAP

A free and open-source security tool called ***OWASP ZAP (Zed Attack Proxy)*** simulates attacks and examines how an application behaves when it is running to help in discovering and fixing vulnerabilities in web applications.

In here, I entered the target URL [***https://www.netflix.com***] designated textbox, simply select "Attack" to initiate the scanning process.



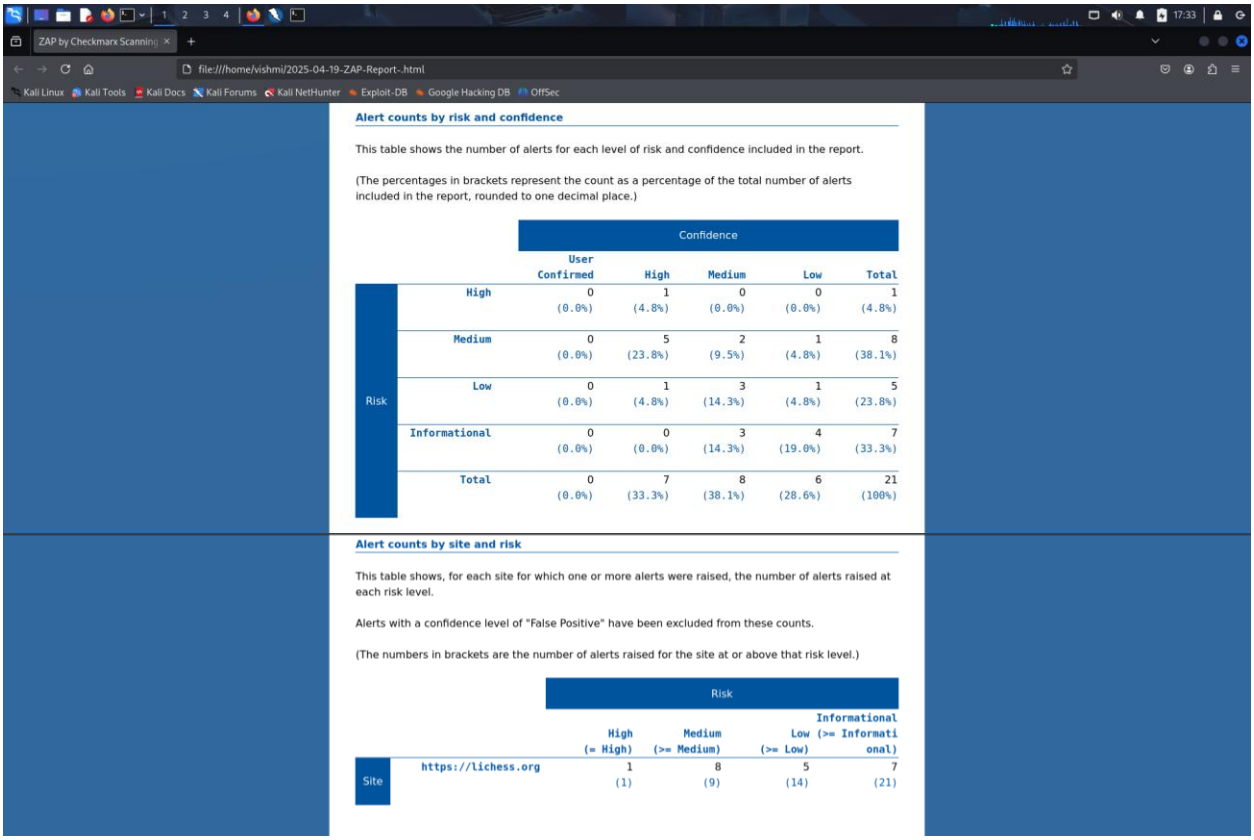
As next step, I entered to the Alerts tab. Here it's detected a vulnerability.



After finishing, it is possible to obtain a thorough report of the results by choosing "Report." The results of scanning many domains are displayed in the screenshots below.

Report = *file:///home/vishmi/2025-04-22-ZAP-Report-.html*

Please take note that these vulnerabilities have been rated using the OWASP risk rating methodology, which is available at this link.[*OWASP Risk Rating Methodology*]



Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	1 (4.8%)	0 (0.0%)	0 (0.0%)	1 (4.8%)
	Medium	0 (0.0%)	5 (23.8%)	2 (9.5%)	1 (4.8%)	8 (38.1%)
	Low	0 (0.0%)	1 (4.8%)	3 (14.3%)	1 (4.8%)	5 (23.8%)
	Informational	0 (0.0%)	0 (0.0%)	3 (14.3%)	4 (19.0%)	7 (33.3%)
	Total	0 (0.0%)	7 (33.3%)	8 (38.1%)	6 (28.6%)	21 (100%)

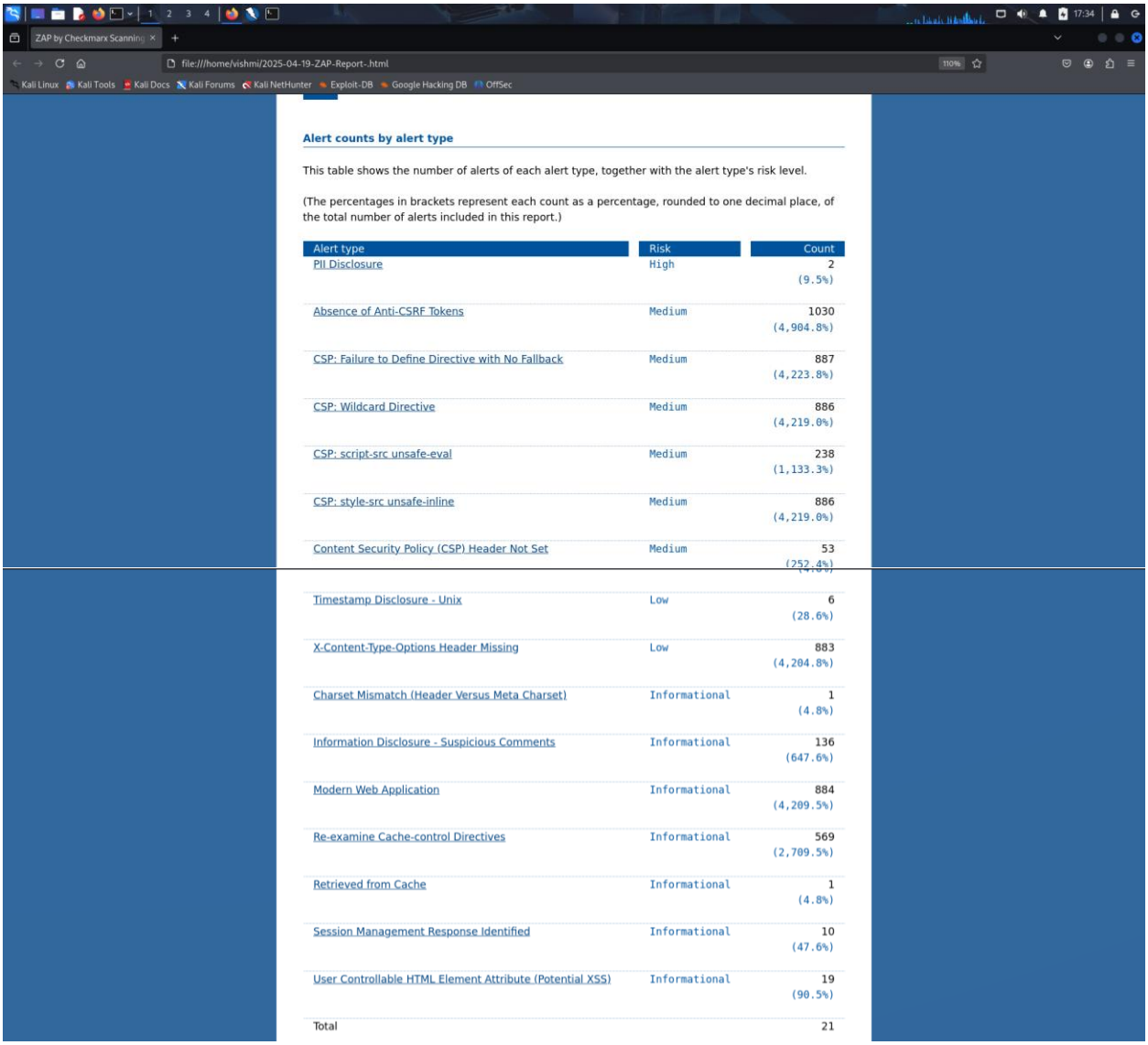
Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://lichess.org	1 (1)	8 (9)	5 (14)	7 (21)



Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
PII Disclosure	High	2 (9.5%)
Absence of Anti-CSRF Tokens	Medium	1030 (4,904.8%)
CSP: Failure to Define Directive with No Fallback	Medium	887 (4,223.8%)
CSP: Wildcard Directive	Medium	886 (4,219.0%)
CSP: script-src unsafe-eval	Medium	238 (1,133.3%)
CSP: style-src unsafe-inline	Medium	886 (4,219.0%)
Content Security Policy (CSP) Header Not Set	Medium	53 (252.4%)
Timestamp Disclosure - Unix	Low	6 (28.6%)
X-Content-Type-Options Header Missing	Low	883 (4,204.8%)
Charset Mismatch (Header Versus Meta Charset)	Informational	1 (4.8%)
Information Disclosure - Suspicious Comments	Informational	136 (647.6%)
Modern Web Application	Informational	884 (4,209.5%)
Re-examine Cache-control Directives	Informational	569 (2,709.5%)
Retrieved from Cache	Informational	1 (4.8%)
Session Management Response Identified	Informational	10 (47.6%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	19 (90.5%)
Total		21

Vulnerabilities

a.Vulnerability Title	**Cross-Domain JavaScript Source File Inclusion**
b.Vulnerability Description	JavaScript files from cross-domain sources are included in applications without sufficient validation, potentially allowing attackers to insert harmful programs, potentially leading to data theft or illegal activities.
c.Affected Components	Cross-domain JavaScript file sources in the HTTP response
d.Impact Assessment	This might be used by attackers to run malicious JavaScript, which could result in phishing, data negotiate, or illegal access.
e.Steps to Reproduce	1. The HTTP response body and headers with development tools or a proxy. 2. If any JavaScript source files are being loaded from outside domains, note them down. 3. To verify these files' vulnerability to malicious injections, try altering or intercepting them.
f.Proof of Concept (if applicable)	Add a malicious payload by altering or replacing a JavaScript file from the external domain. To check if the script runs successfully, load the page.
g.Proposed Mitigation or Fix	Switch off support for outdated TLS versions, such as TLS 1.0 and 1.1. Set up the server to use just strong cypher suites.

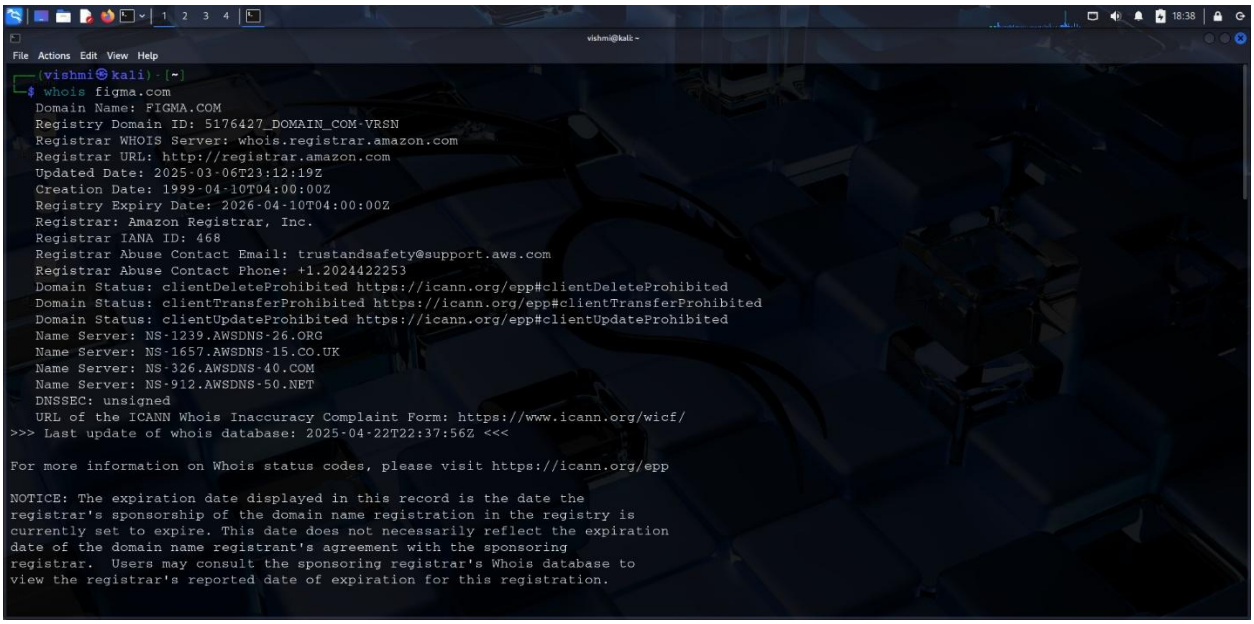
Report-03

Web Audit
figma.com

Domain = *figma.com*
Sub-domain = *go.figma.com*
URL = *https://www.figma.com*

Target Reconnaissance

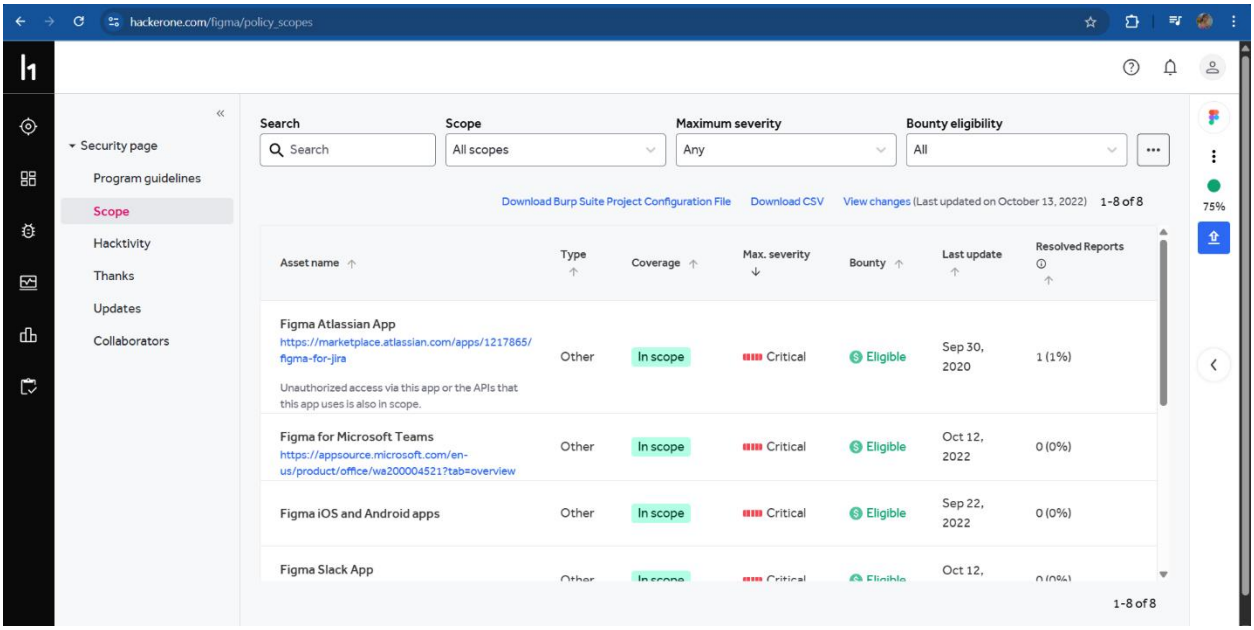
Introduction to Figma and Audit Scope

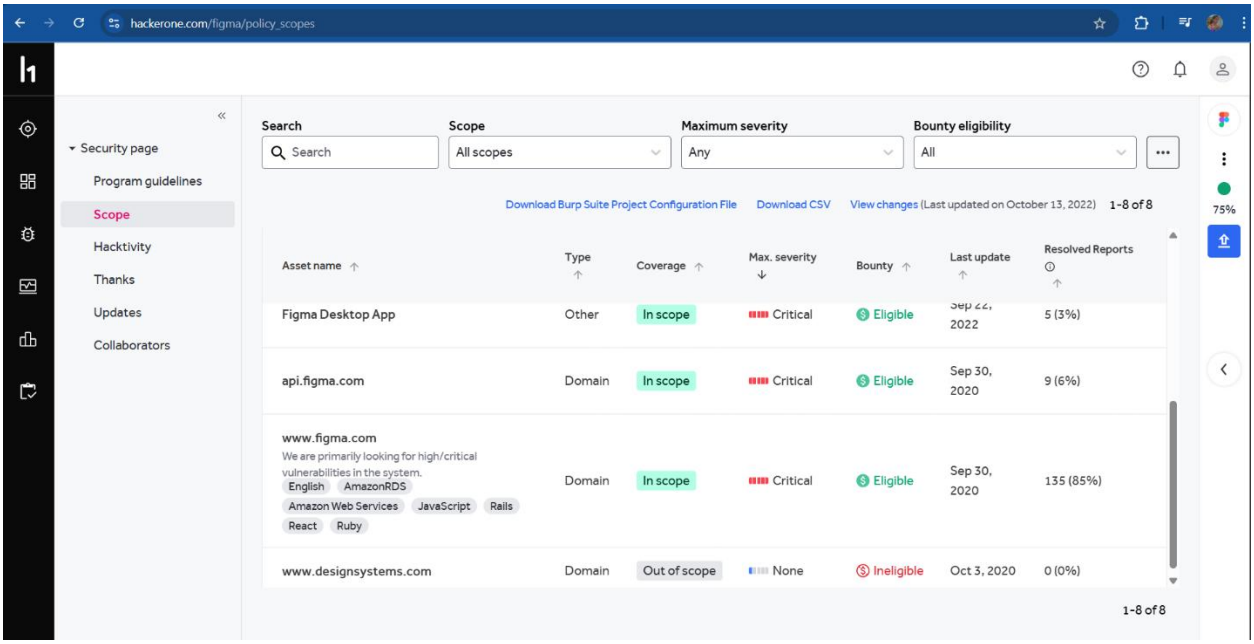


The cloud-based design tool "**Figma"** is used to create user interfaces (UI) and user experiences (UX) for mobile apps and websites. Like Google Docs, but for design, Figma operates directly in the browser, unlike typical design tools, making real-time team collaboration incredibly simple. For wireframing, prototyping, and creating design systems, it is particularly well-liked by product teams, designers, and developers.

These subdomains (and all included) have been approved as legitimate subdomains for testing in the **Hackerone** Bug Bounty program.

Eligible in-scope subdomains for bug bounty program are mentioned below.





Information gathering phase.

The information-gathering phase, often known as reconnaissance or recon, is essential to both assessments of security and cyberattacks. In order to map out the target's structure and determine how it functions, the target of this stage is to gather as much information as possible about it. Because it helps auditors or attackers identify vulnerabilities that could be exploited later on, this fundamental understanding is essential.

There are two main approaches to information gathering

1.Active Scanning :

Involves direct interaction with the target, which can generate noticeable activity and typically uncovers a wealth of details about the system.

2.Passive Scanning :

Seeks to observe the target without direct engagement, resulting in less detectable activity but often providing more limited information

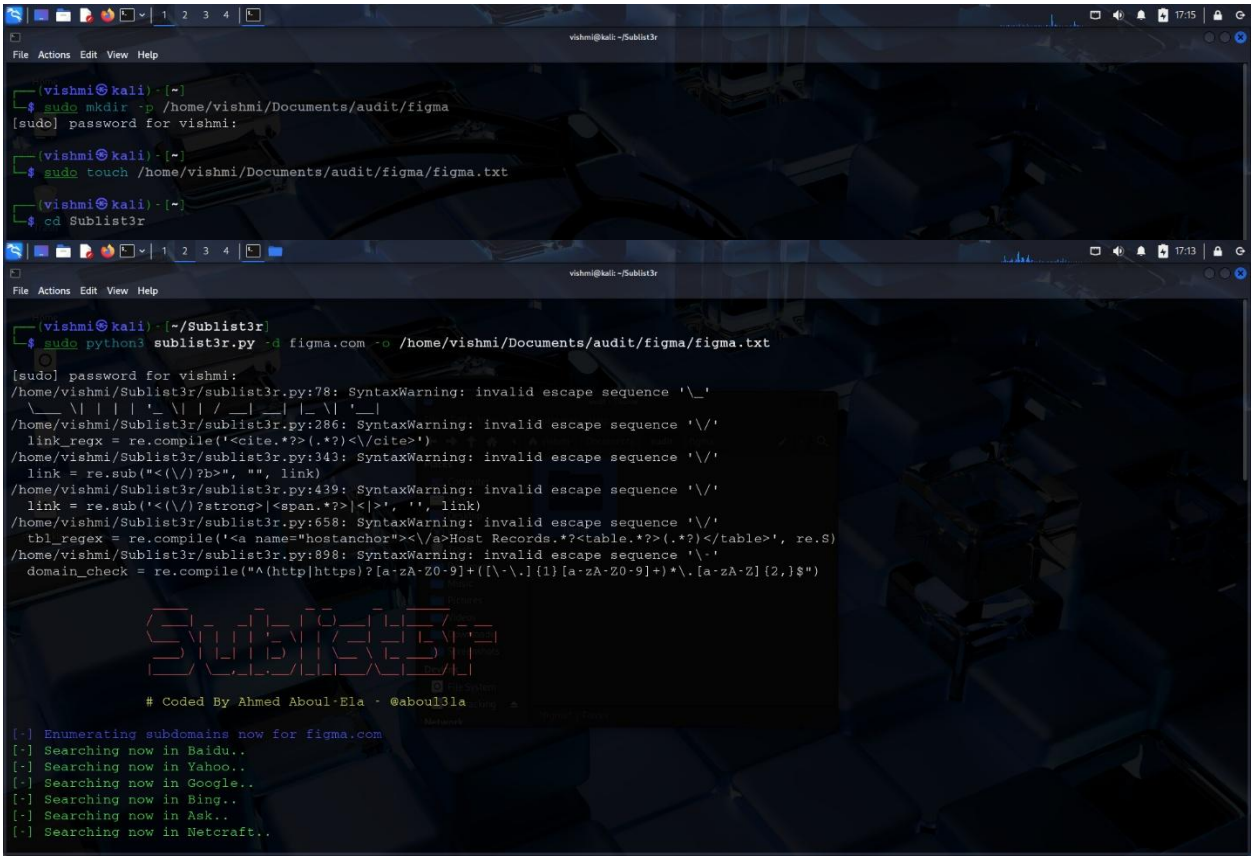
Finding active subdomains and their states

Sublist3r

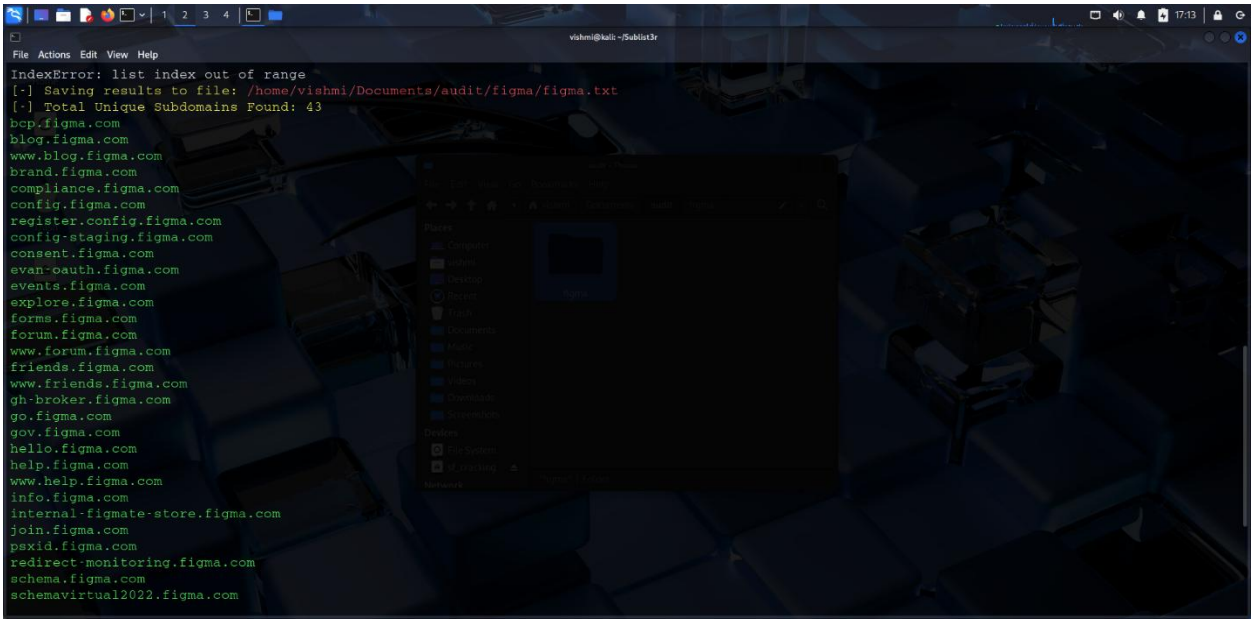
Sublist3r is an open-source Python application that uses OSINT (Open Source Intelligence) techniques to quickly and effectively scan subdomains. Subdomains linked to a target domain can be found by penetration testers, security researchers, and bug bounty hunters using a variety of search engine queries (including Google, Yahoo, Bing, Baidu, and Ask). Additionally, Sublist3r includes a brute-force module (subbrute) to employ a stronger wordlist to improve the probability of discovering more subdomains.

I created a .txt file to store the subdomain headers that were initiated via sublist3r.

Path to .txt file = ***home/vishmi/Documents/audit/figma/figma.txt***



I got, these subdomains according to the ***figma.com*** domain.

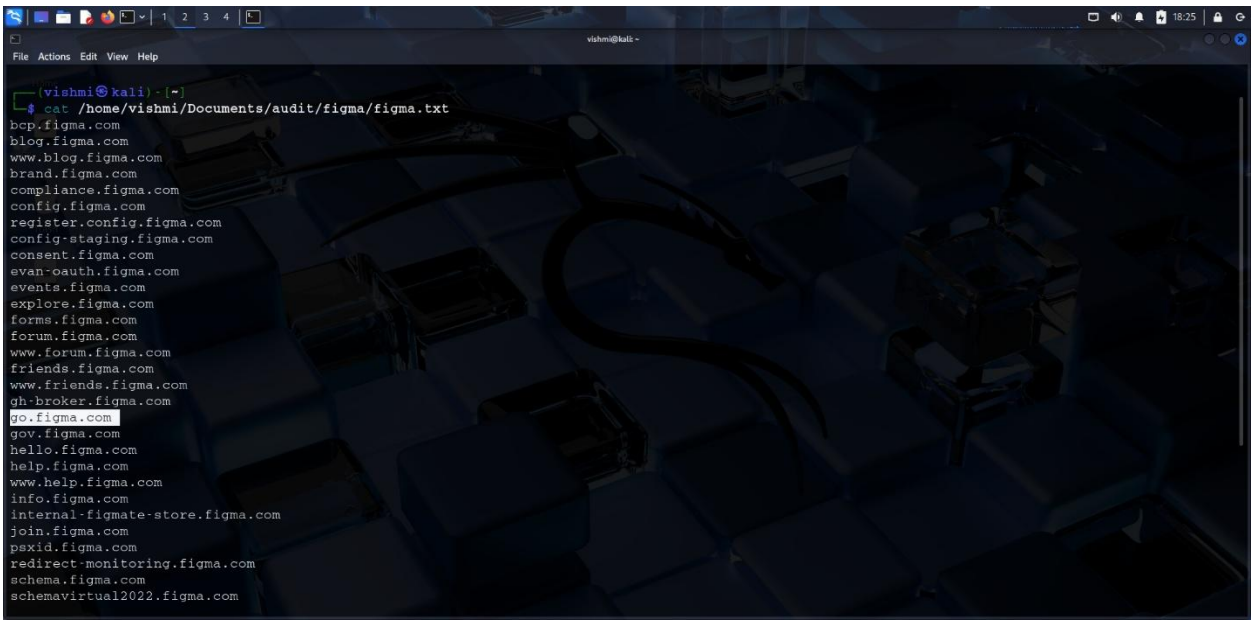

File Actions Edit View Help
IndexError: list index out of range
[-] Saving results to file: /home/vishmi/Documents/audit/figma/figma.txt
[-] Total Unique Subdomains Found: 43
bcp.figma.com
blog.figma.com
www.blog.figma.com
brand.figma.com
compliance.figma.com
config.figma.com
register.config.figma.com
config-staging.figma.com
consent.figma.com
evan-oauth.figma.com
events.figma.com
explore.figma.com
forms.figma.com
forum.figma.com
www.forum.figma.com
friends.figma.com
www.friends.figma.com
gh-broker.figma.com
go.figma.com
gov.figma.com
hello.figma.com
help.figma.com
www.help.figma.com
info.figma.com
internal-figmate-store.figma.com
join.figma.com
psxid.figma.com
redirect-monitoring.figma.com
schema.figma.com
schemavirtual2022.figma.com

HTTProbe

HTTProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing on achievable goals by providing you with the URLs of active domains.

I am using the text file generated before by the sublist3r and stored the active subdomains to another new .txt file.

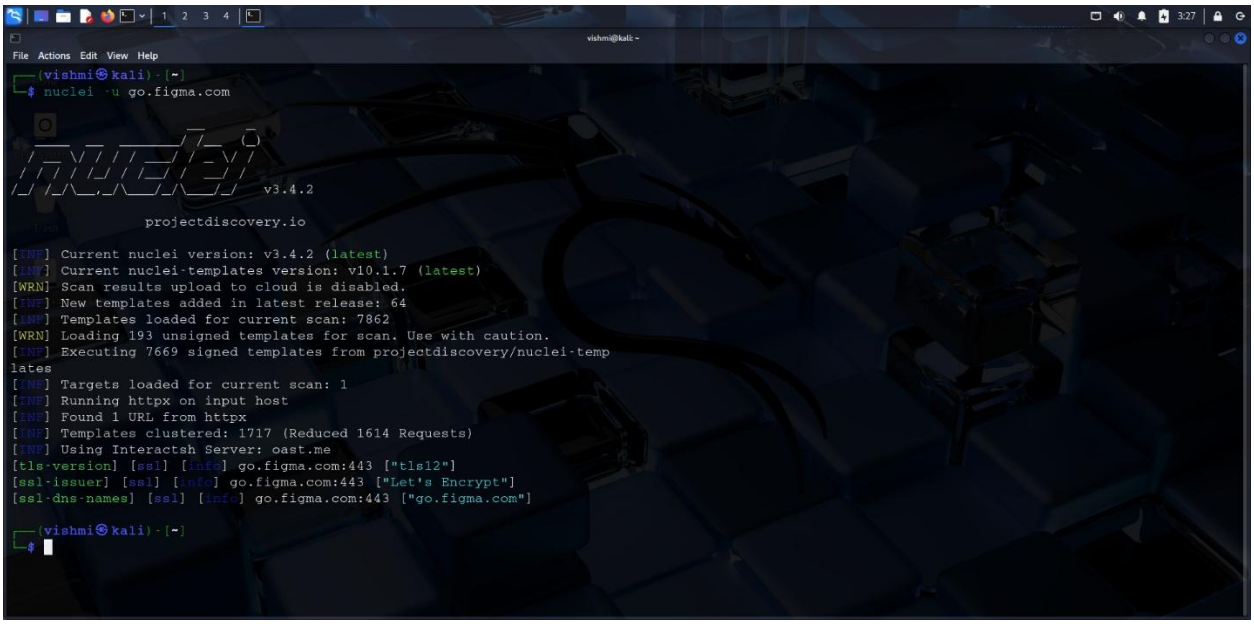
Below, we can see the active subdomains related to the ***figma.com*** domain.



To move forward, I chose the active subdomain as **"go.figma.com".**

Nuclei

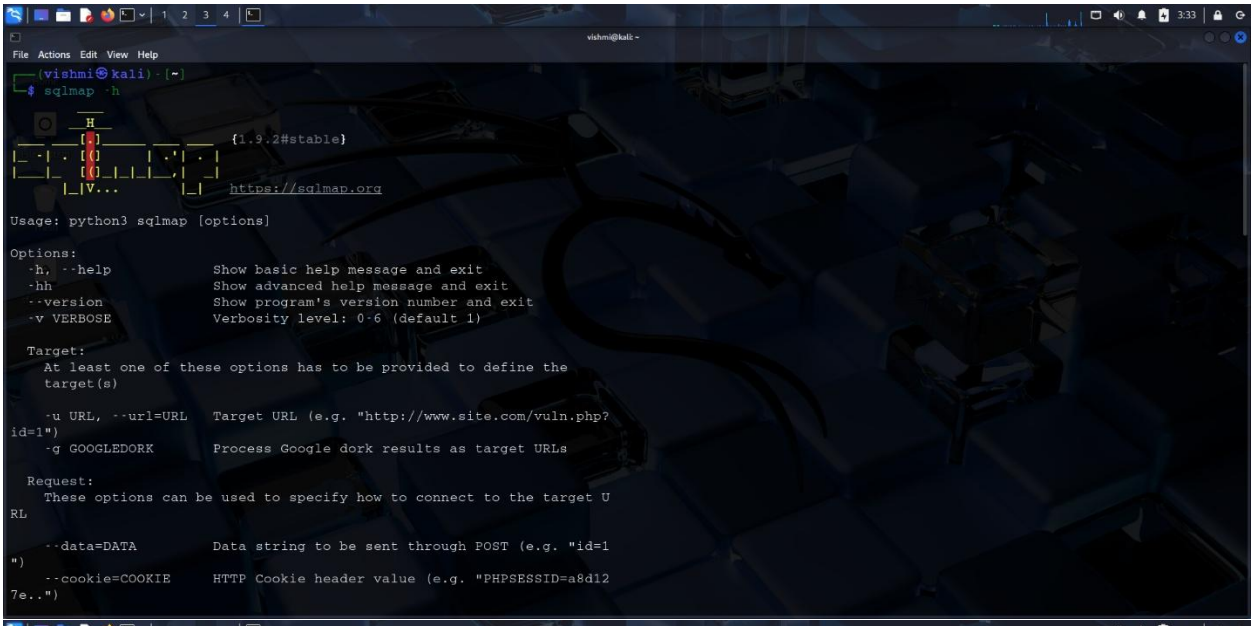
Nuclei is an open-source vulnerability scanner developed by ProjectDiscovery for security professionals, penetration testers, and bug bounty hunters. It uses customizable YAML("Yet Another Markup Language") -based templates to identify vulnerabilities such as misconfigurations, outdated software, and known CVEs (Common Vulnerabilities and Exposures).

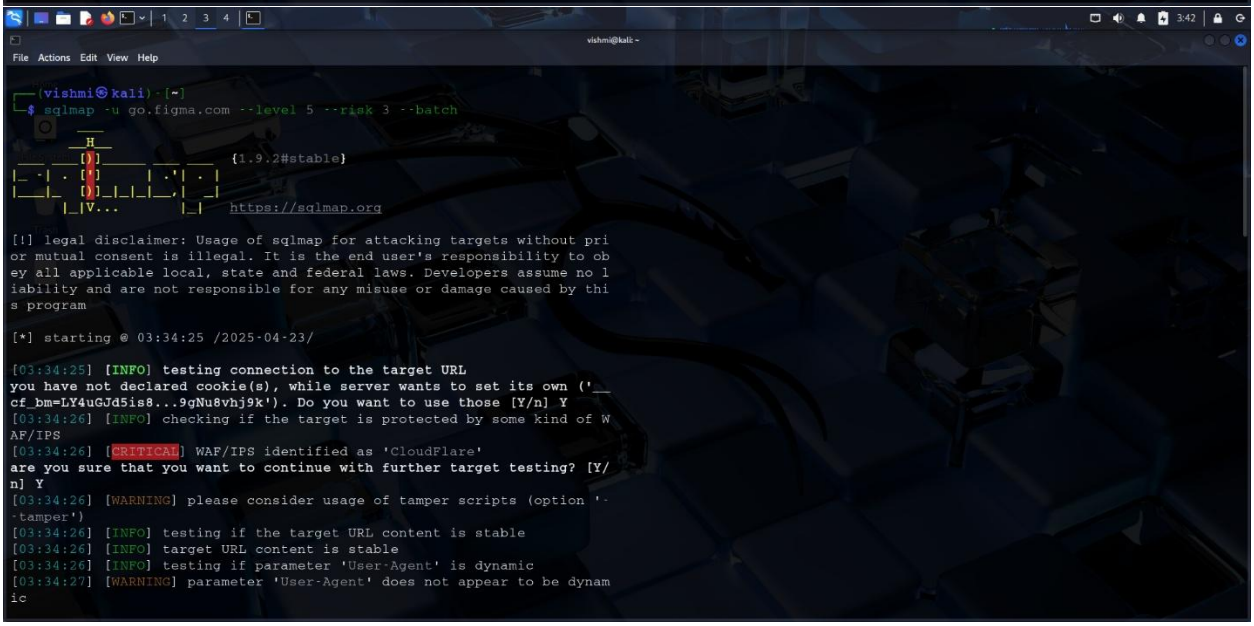


Vulnerable Title	Description	Risk
SSL/TLS Certificate Expiry	SSL/TLS certificate expired for go.figma.com:443.	High
Mismatched SSL Certificate	SSL certificate domain doesn't match the actual domain.	High
Self-Signed SSL Certificate	SSL certificate isn't signed by a trusted authority.	Medium

SQLmap

An open-source penetration testing tool called **SQLmap** makes it easier to find and take advantage of SQL injection flaws in web apps. If the database permits, it can even access the underlying file system or run commands on the server in addition to identifying the type of database and extracting data. Security experts frequently use it to evaluate and protect web apps from SQL injection attacks.





Option	Meaning
-u	For basic testing, the target URL is required.
--level5	Increases the number of payloads and tests that are done (maximum is 5).
--risk3	Increase the danger level of the payloads used (maximum is 3)
--batch	Executes SQLMap in a non-interactive mode, selecting default responses automatically.

Detected Information

* ***[WARNING] heuristic (basic) test shows that parameter 'User-Agent' might be injectable***

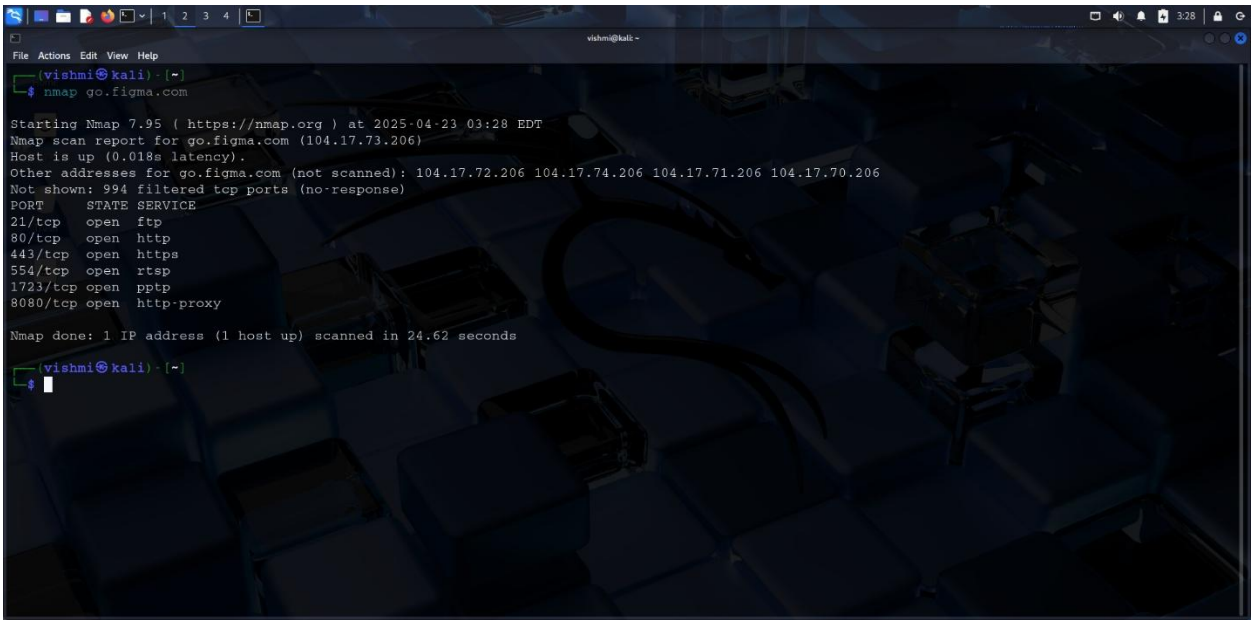
[This is a *potential* vulnerability, but not confirmed.]

* ***[critical]WAF/IPS identified as a CloudFlare.***

Searching for vulnerabilities

Nmap

Nmap (Network Mapper) is a strong, open-source network scanning program that uses packet transmission and response analysis to find hosts and services on a computer network. To find open ports, running services, operating systems, and active devices on a network, network managers and security experts utilize Nmap. Network inventory, vulnerability assessment, security auditing, and penetration testing are among its many uses.



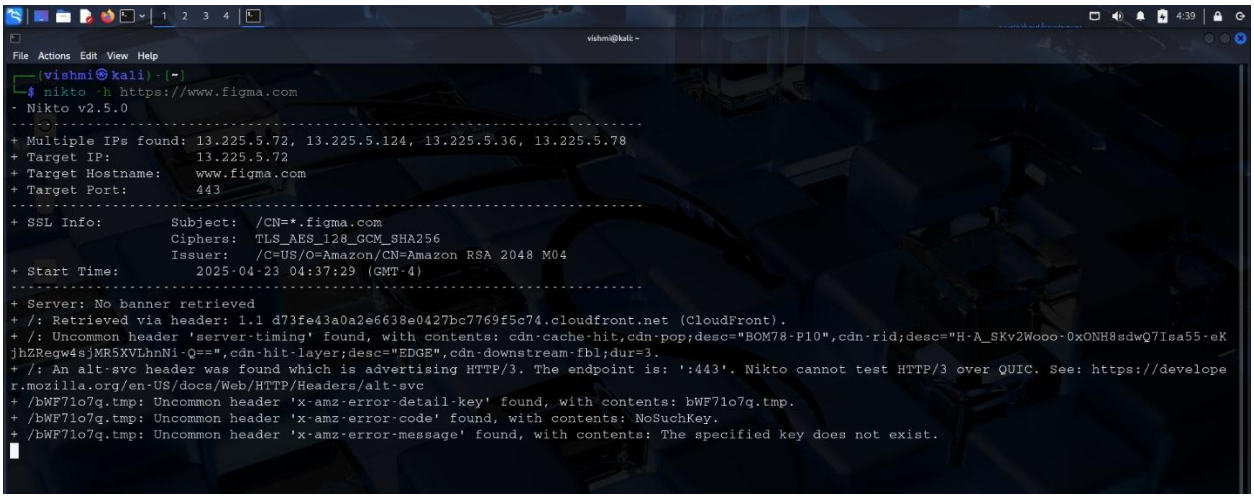
I discovered these details by using Nmap to search *go.figma.com.*

PORT	STATE	SERVICE
21/tcp	open	ftp
80/tcp	open	http
443/tcp	open	https
554/tcp	open	rtsp
1723/tcp	open	pptp
8080/tcp	open	http.proxy

PORT	SERVICE	Vulnerabilities
21/tcp	ftp	Unencrypted credentials are accepted.
80/tcp	http	Transmits plain text data.
443/tcp	https	Deprecated TLS versions are supported.
554/tcp	Rtsp	Usually doesn't have authenticity.
1723/tcp	pptp	Makes use of a weak encryption
8080/tcp	http.proxy	Can act as an open proxy if misconfigured.

Nikto

An open-source program called Nikto scans web servers for common vulnerabilities, malicious files, outdated software, and improperly configured settings, among other potential security issues. It is widely used for penetration testing and assessments, but it functions best when combined with other tools.



Security issues found on ***https://www.figma.com's*** by Nikto Scan

* Uncommon header 'server-timing' found.

* Uncommon header 'server-timing' found.

*Uncommon header 'server-timing' found.

*Uncommon header 'x-amz-error-message' found.

*No CGI Directories found.

*Uncommon header 'critical-origin-trial' found.

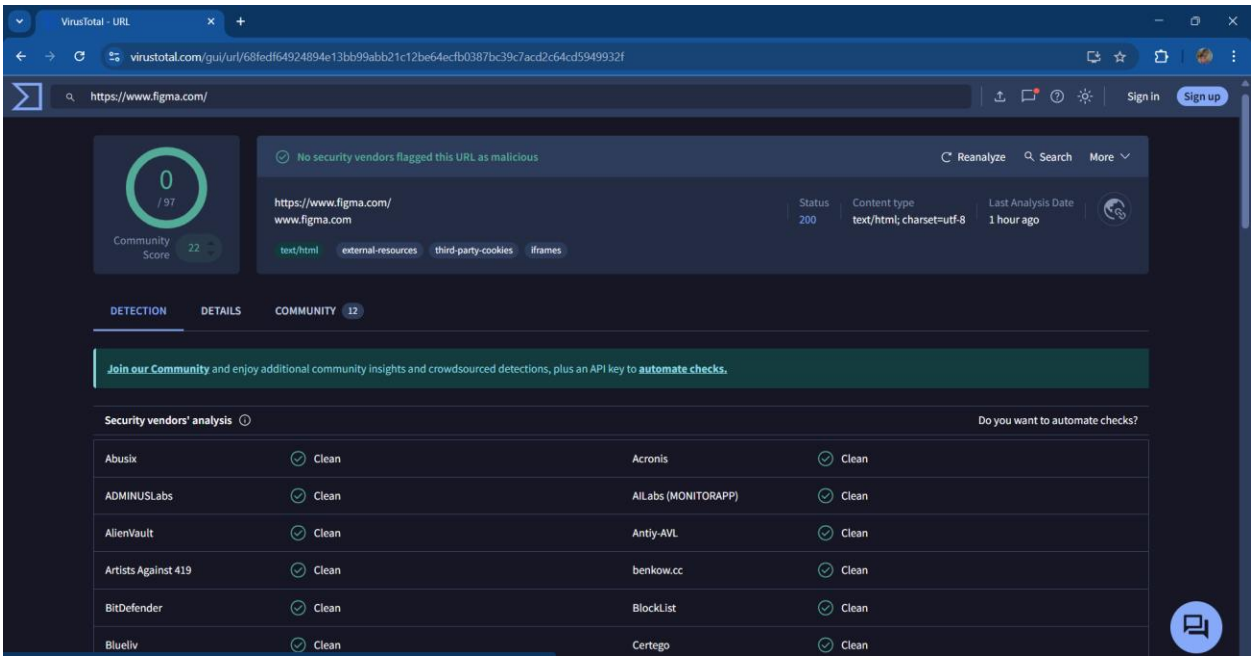
*Uncommon header 'reporting-endpoints' found.

*Uncommon header 'origin-trial' found.

Virustotal

Virustotal is a free web service called VirusTotal employs 70 antivirus engines and URL blocklisting services to scan files and URLs for malware, adware, and other malicious content.

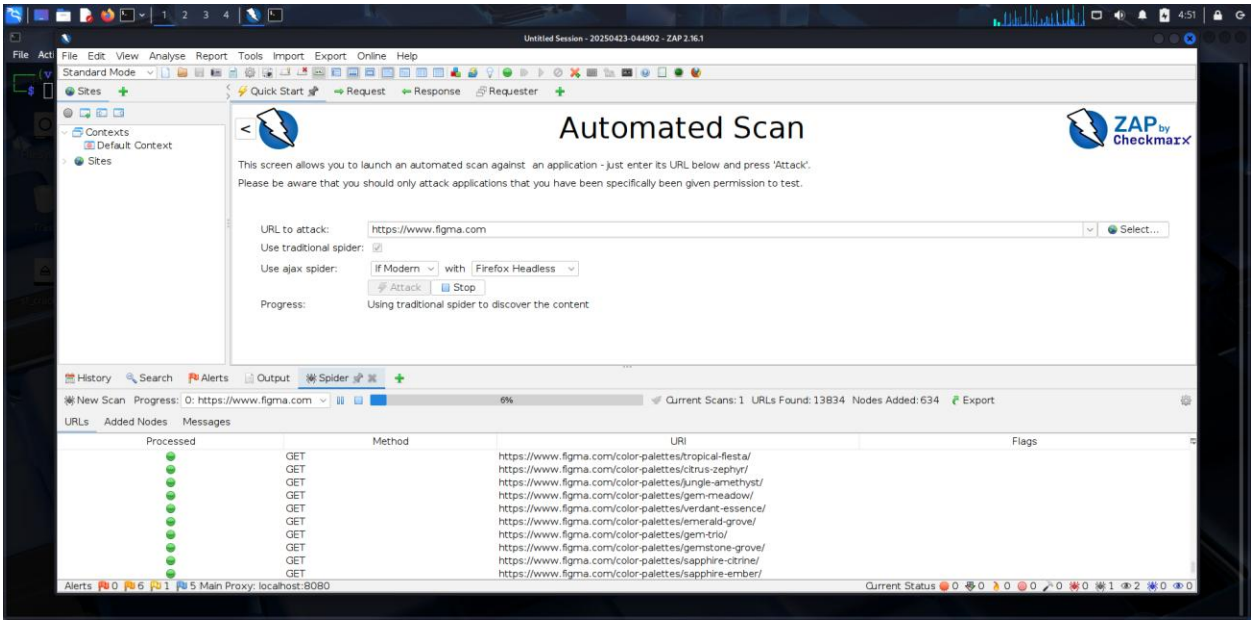
I entered https://www.figma.com in URL section .



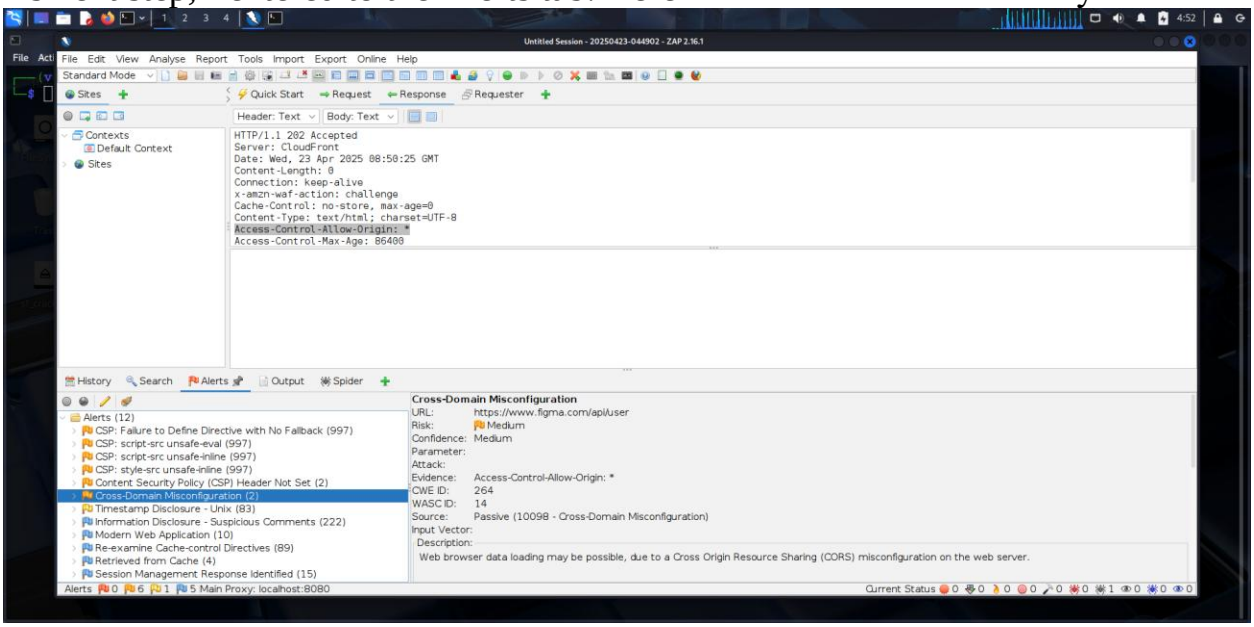
OWASP ZAP

A free and open-source security tool called ***OWASP ZAP (Zed Attack Proxy)*** simulates attacks and examines how an application behaves when it is running to help in discovering and fixing vulnerabilities in web applications.

In here, I entered the target URL [***https://www.figma.com***] designated textbox, simply select "Attack" to initiate the scanning process.



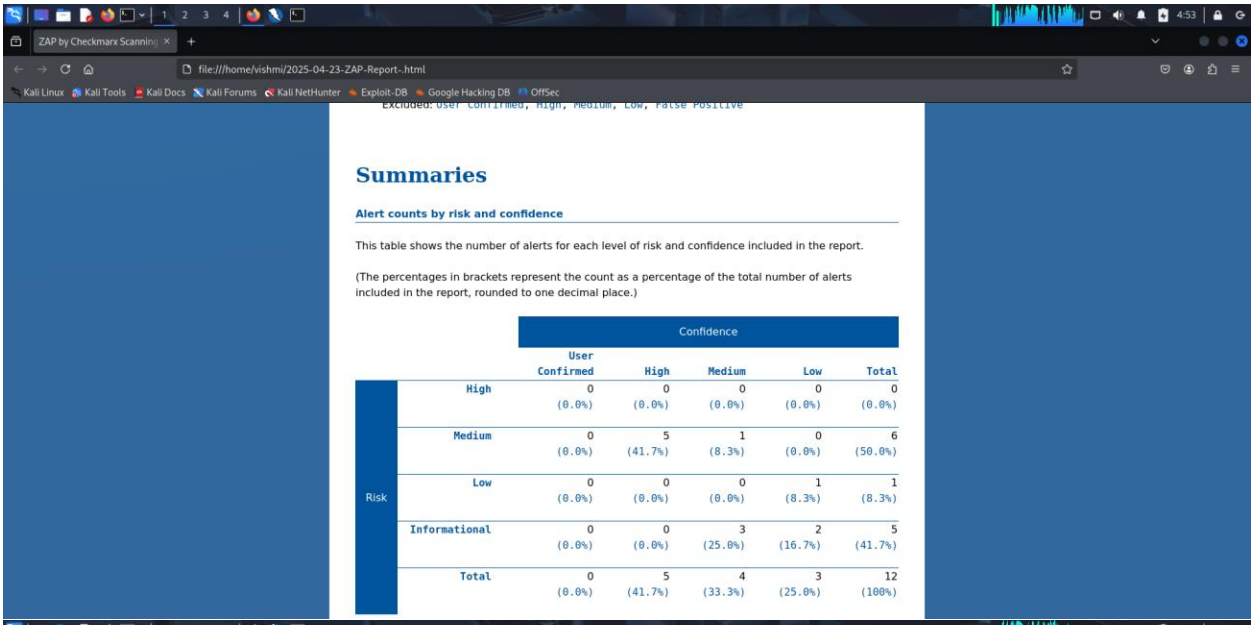
As next step, I entered to the Alerts tab. Here it's detected a vulnerability.

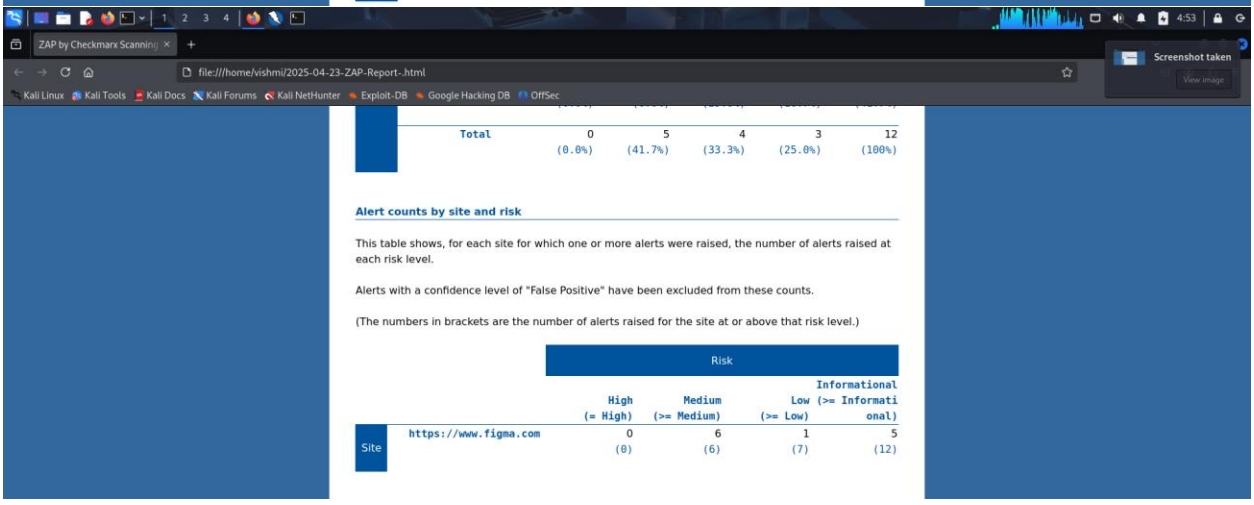


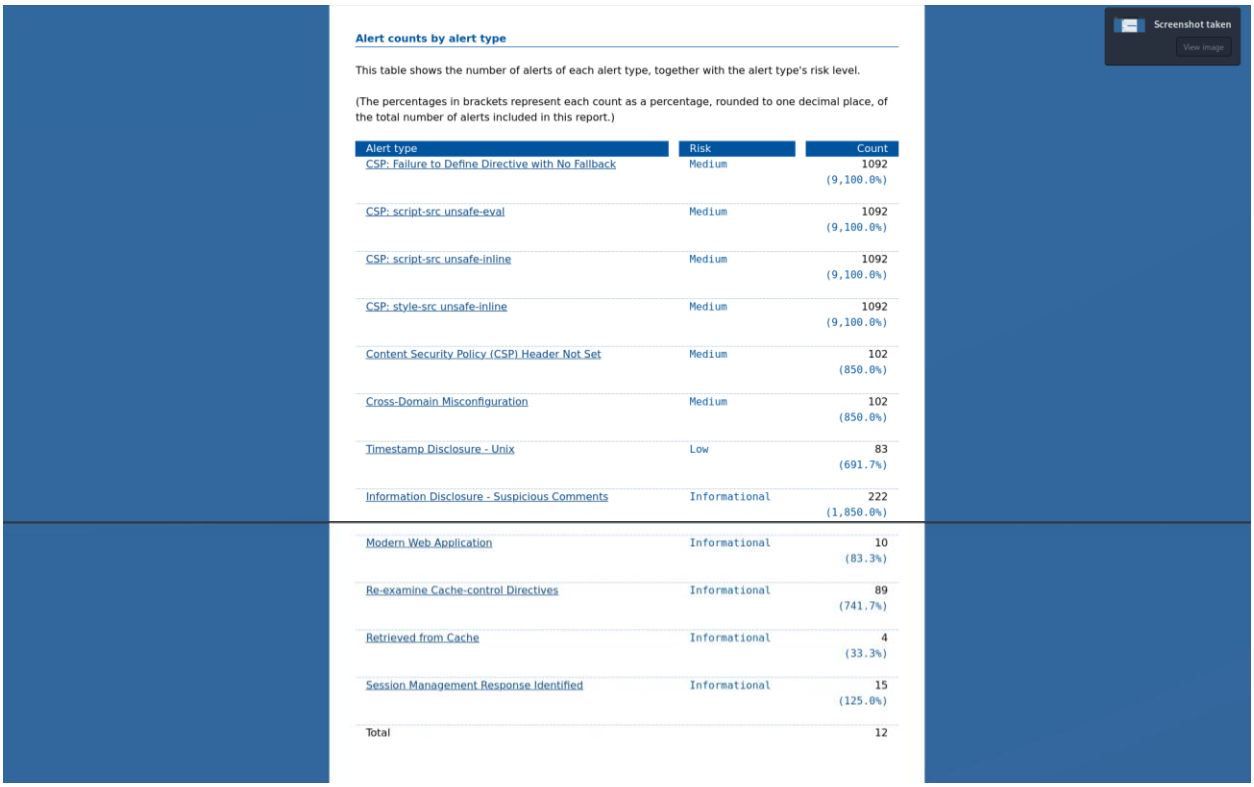
After finishing, it is possible to obtain a thorough report of the results by choosing "Report." The results of scanning many domains are displayed in the screenshots below.

Report = file:///home/vishmi/2025-04-23-ZAP-Report-.html

Please take note that these vulnerabilities have been rated using the OWASP risk rating methodology, which is available at this link.[*OWASP Risk Rating Methodology*]







Screenshot taken

View image

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
CSP: Failure to Define Directive with No Fallback	Medium	1092 (9,100.0%)
CSP: script-src unsafe-eval	Medium	1092 (9,100.0%)
CSP: script-src unsafe-inline	Medium	1092 (9,100.0%)
CSP: style-src unsafe-inline	Medium	1092 (9,100.0%)
Content Security Policy (CSP) Header Not Set	Medium	102 (850.0%)
Cross-Domain Misconfiguration	Medium	102 (850.0%)
Timestamp Disclosure - Unix	Low	83 (691.7%)
Information Disclosure - Suspicious Comments	Informational	222 (1,850.0%)
Modern Web Application	Informational	10 (83.3%)
Re-examine Cache-control Directives	Informational	89 (741.7%)
Retrieved from Cache	Informational	4 (33.3%)
Session Management Response Identified	Informational	15 (125.0%)
Total		12

Vulnerabilities

a.Vulnerability Title	**Cross-Domain Misconfiguration**
b.Vulnerability Description	The server allows unrestricted cross-origin requests via *Access-Control-Allow-Origin: **, potentially exposing sensitive data.
c.Affected Components	Web server and CORS configuration.
d.Impact Assessment	High risk of data exfiltration or unauthorized access.
e.Steps to Reproduce	1.Send a request from a different origin. 2.Observe that the server accepts and processes the request without restriction.
f.Proof of Concept (if applicable)	Exploit cross-origin sharing to read sensitive data using a different domain.
g.Proposed Mitigation or Fix	Restrict *Access-Control-Allow-Origin* to trusted domains only.

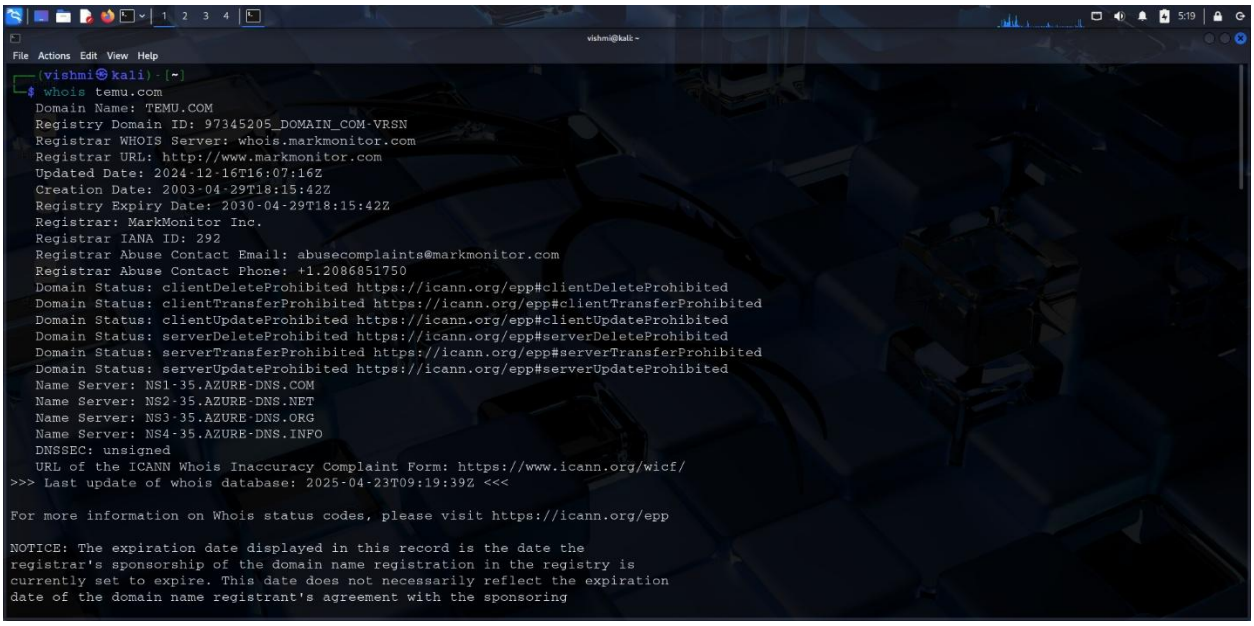
Report-04

Web Audit
temu.com

Domain = *temu.com*
Sub-domain = *ads.temu.com*
URL = *https://www.temu.com*

Target Reconnaissance

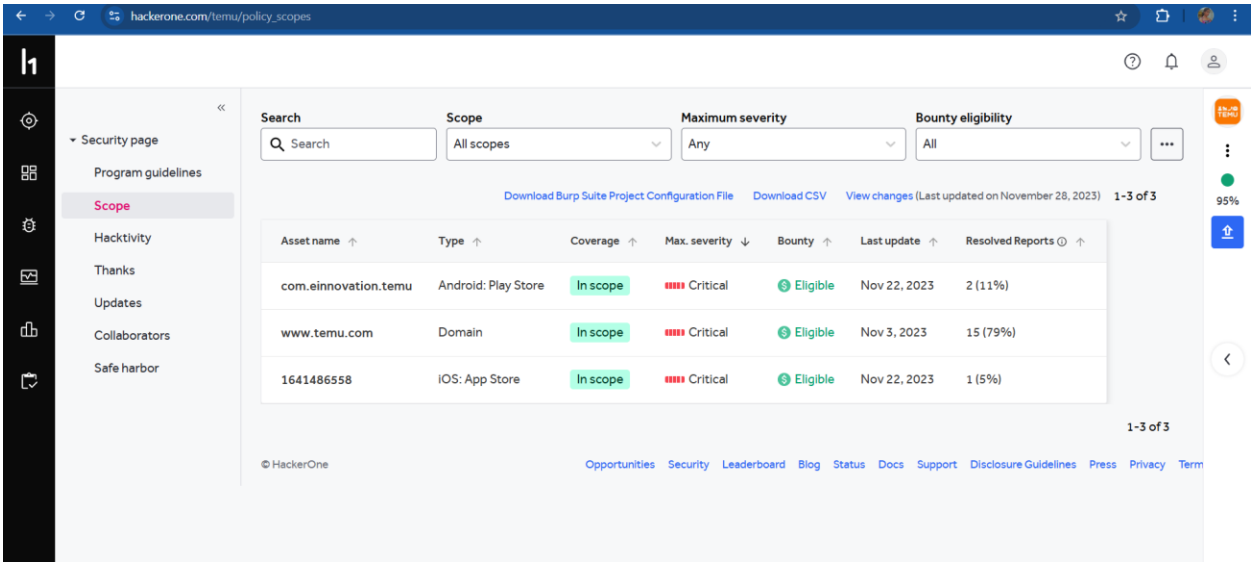
Introduction to Temu and Audit Scope



Temu is an international e-commerce site that sells a large range of reasonably priced goods, such as apparel, electronics, home goods, cosmetics, and more. **Temu**, which was introduced in 2022 by PDD Holdings (which also owns the massive Chinese e-commerce platform Pinduoduo), immediately became well-known for its extremely low prices and extensive assortment. It links customers and producers directly, frequently eliminating middlemen to provide steep discounts. The platform primarily targets consumers on a budget worldwide through its website and app.

These subdomains (and all included) have been approved as legitimate subdomains for testing in the **Hackerone** Bug Bounty program.

Eligible in-scope subdomains for bug bounty program are mentioned below.



Information gathering phase.

The information-gathering phase, often known as reconnaissance or recon, is essential to both assessments of security and cyberattacks. In order to map out the target's structure and determine how it functions, the target of this stage is to gather as much information as possible about it. Because it helps auditors or attackers identify vulnerabilities that could be exploited later on, this fundamental understanding is essential.

There are two main approaches to information gathering

1. **Active Scanning :**

   Involves direct interaction with the target, which can generate noticeable activity and typically uncovers a wealth of details about the system.

2. **Passive Scanning :**

   Seeks to observe the target without direct engagement, resulting in less detectable activity but often providing more limited information

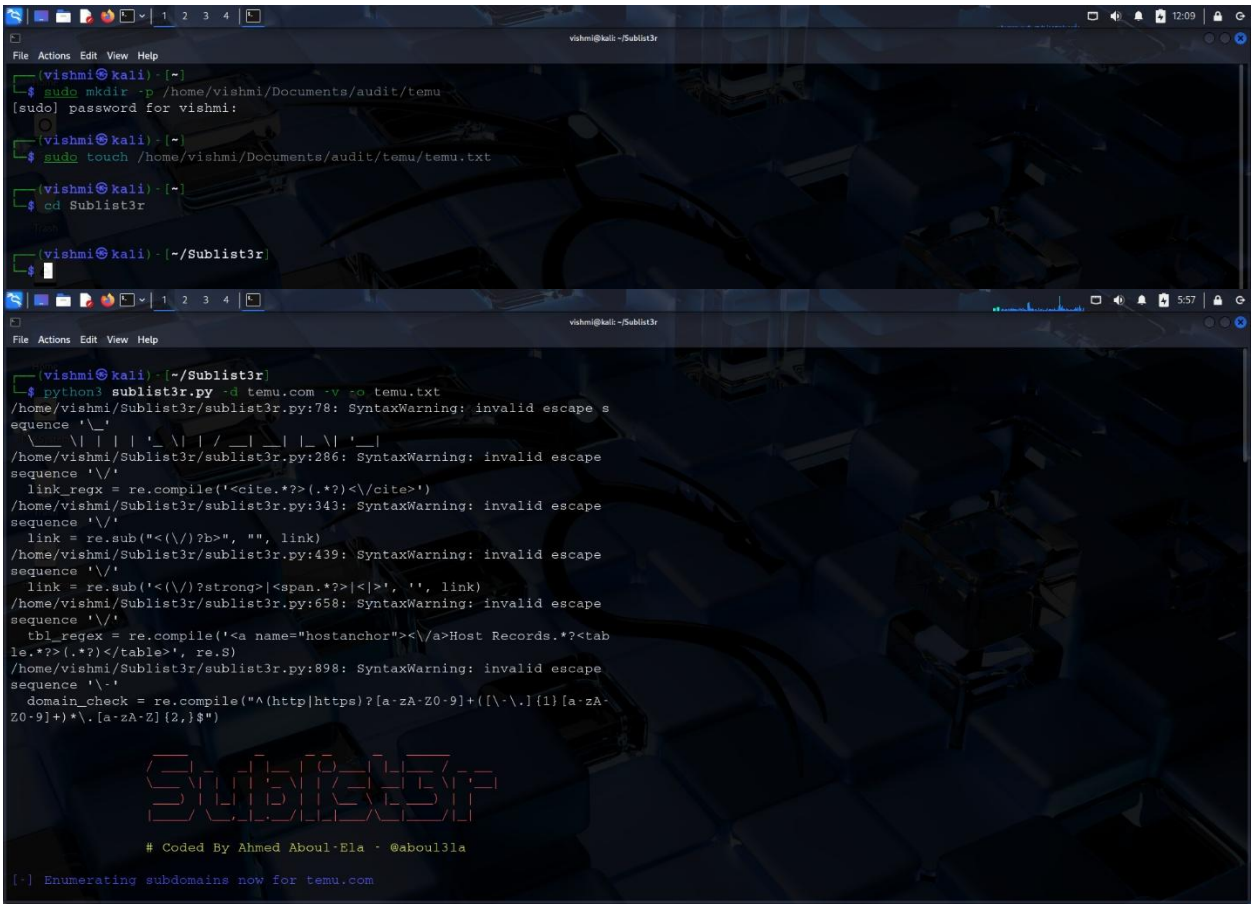
Finding active subdomains and their states

Sublist3r

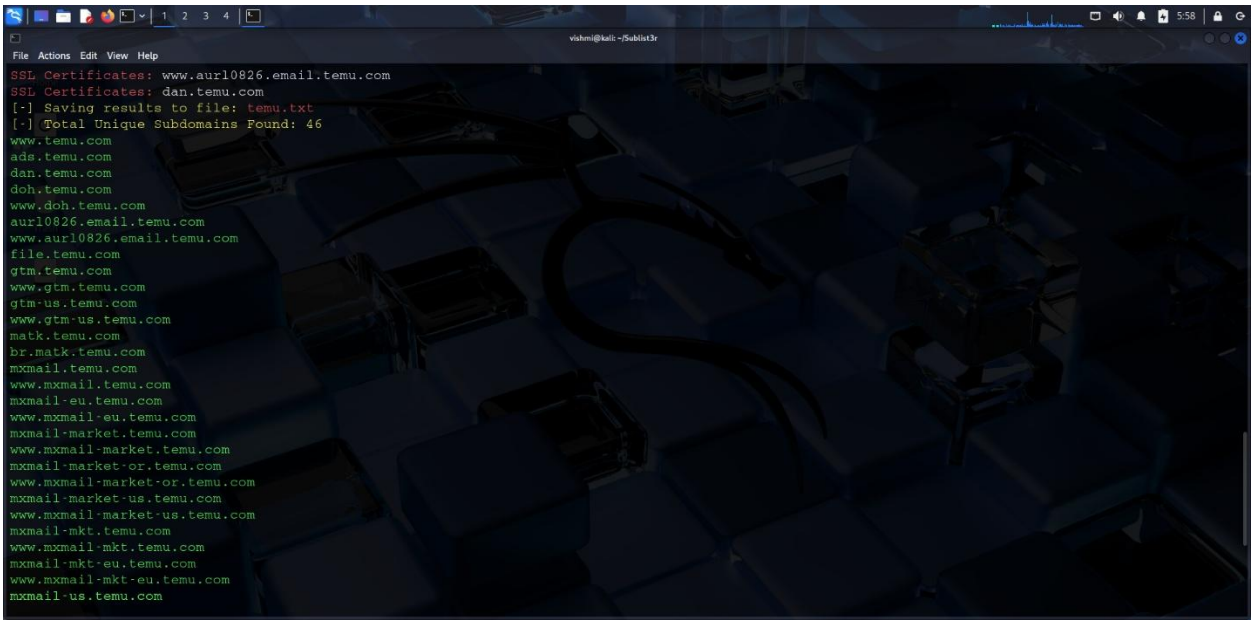
Sublist3r is an open-source Python application that uses OSINT (Open Source Intelligence) techniques to quickly and effectively scan subdomains. Subdomains linked to a target domain can be found by penetration testers, security researchers, and bug bounty hunters using a variety of search engine queries (including Google, Yahoo, Bing, Baidu, and Ask). Additionally, Sublist3r includes a brute-force module (subbrute) to employ a stronger wordlist to improve the probability of discovering more subdomains.

I created a .txt file to store the subdomain headers that were initiated via sublist3r.

Path to .txt file = ***home/vishmi/Documents/audit/temu/temu.txt***



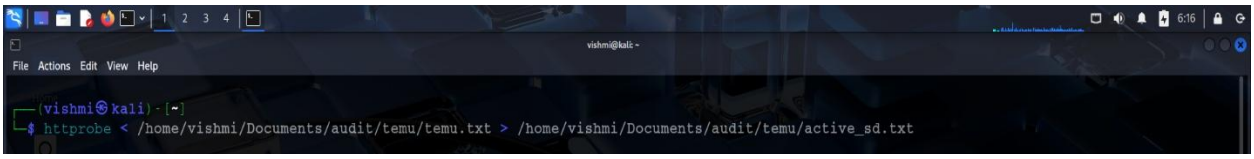
I got, these subdomains according to the ***temu.com*** domain.



HTTProbe

HTTProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing on achievable goals by providing you with the URLs of active domains.

I am using the text file generated before by the sublist3r and stored the active subdomains to another new .txt file.

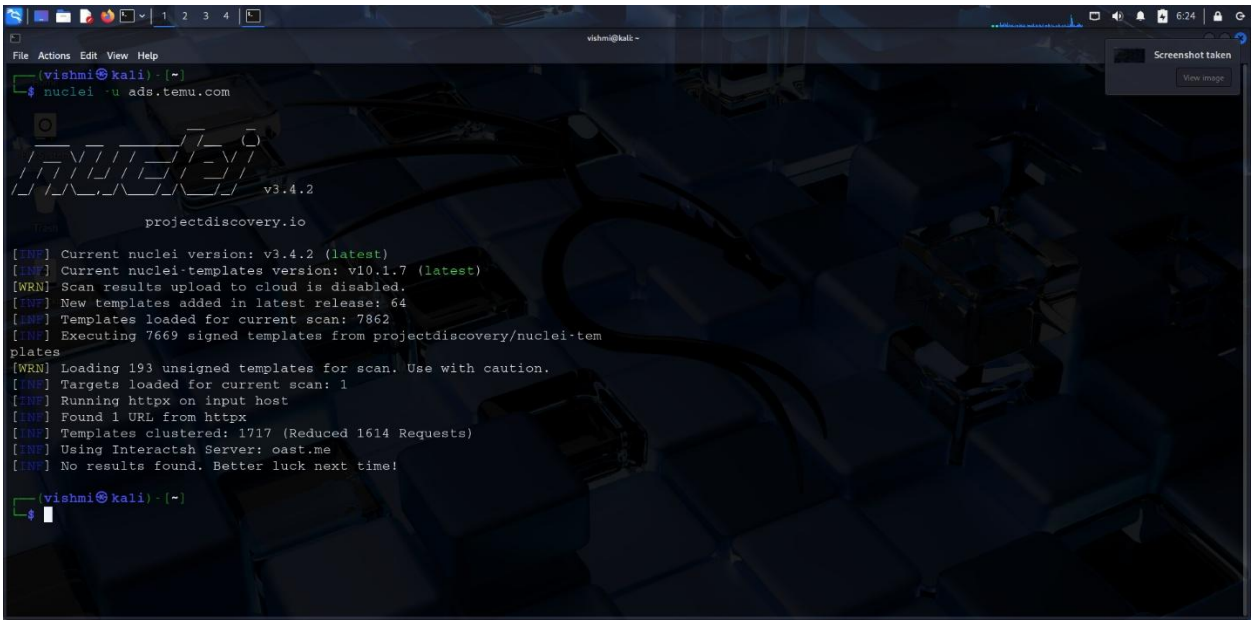


Below, we can see the active subdomains related to the ***temu.com*** domain.

To move forward, I chose the active subdomain as **“ads.temu.com”.**

Nuclei

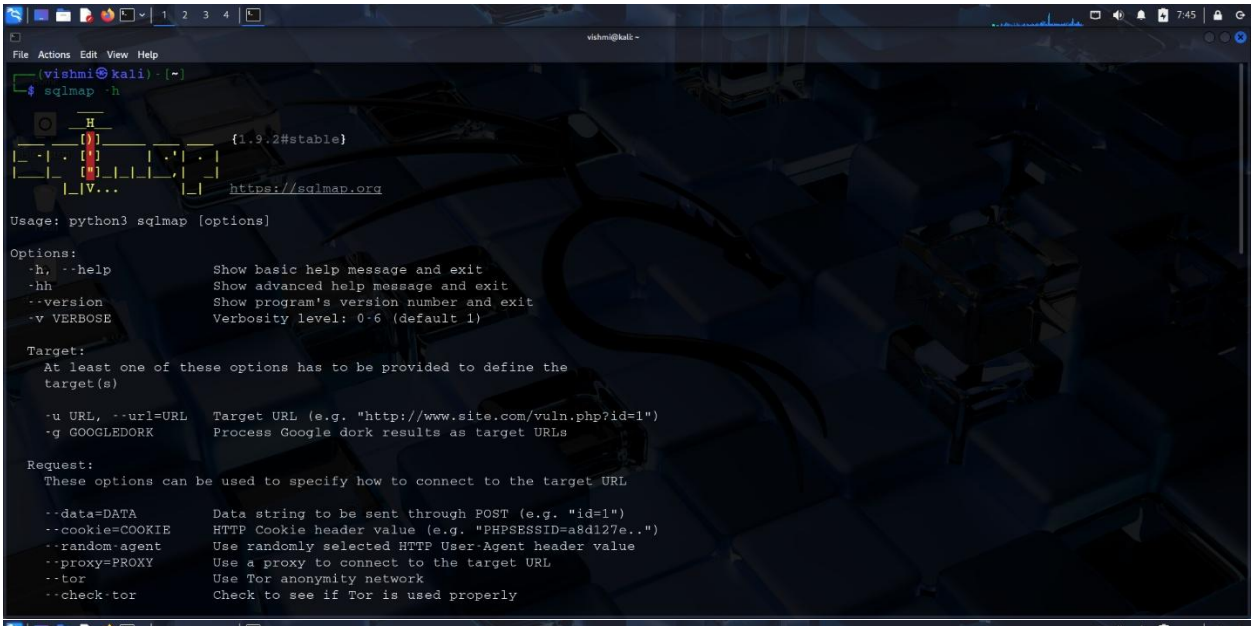
Nuclei is an open-source vulnerability scanner developed by ProjectDiscovery for security professionals, penetration testers, and bug bounty hunters. It uses customizable YAML("Yet Another Markup Language") -based templates to identify vulnerabilities such as misconfigurations, outdated software, and known CVEs (Common Vulnerabilities and Exposures).

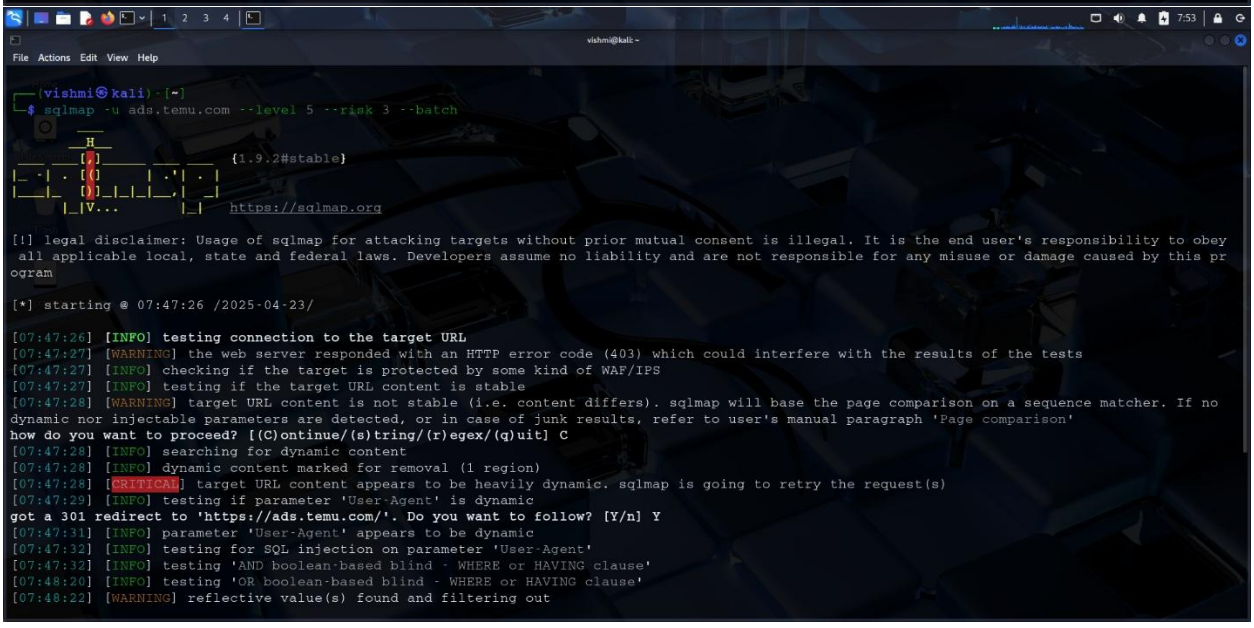


Here, the nuclei scan found no issue.

SQLmap

An open-source penetration testing tool called SQLmap makes it easier to find and take advantage of SQL injection flaws in web apps. If the database permits, it can even access the underlying file system or run commands on the server in addition to identifying the type of database and extracting data. Security experts frequently use it to evaluate and protect web apps from SQL injection attacks.





Option	Meaning
-u	For basic testing, the target URL is required.
--level5	Increases the number of payloads and tests that are done (maximum is 5).
--risk3	Increase the danger level of the payloads used (maximum is 3)
--batch	Executes SQLMap in a non-interactive mode, selecting default responses automatically.

Detected Information

* ***[WARNING] the web server responded with an HTTP error code.***

* ***[WARNING]target URL content is not stable.***

* ***[WARNING]reflective value(s) found and filtering out.***

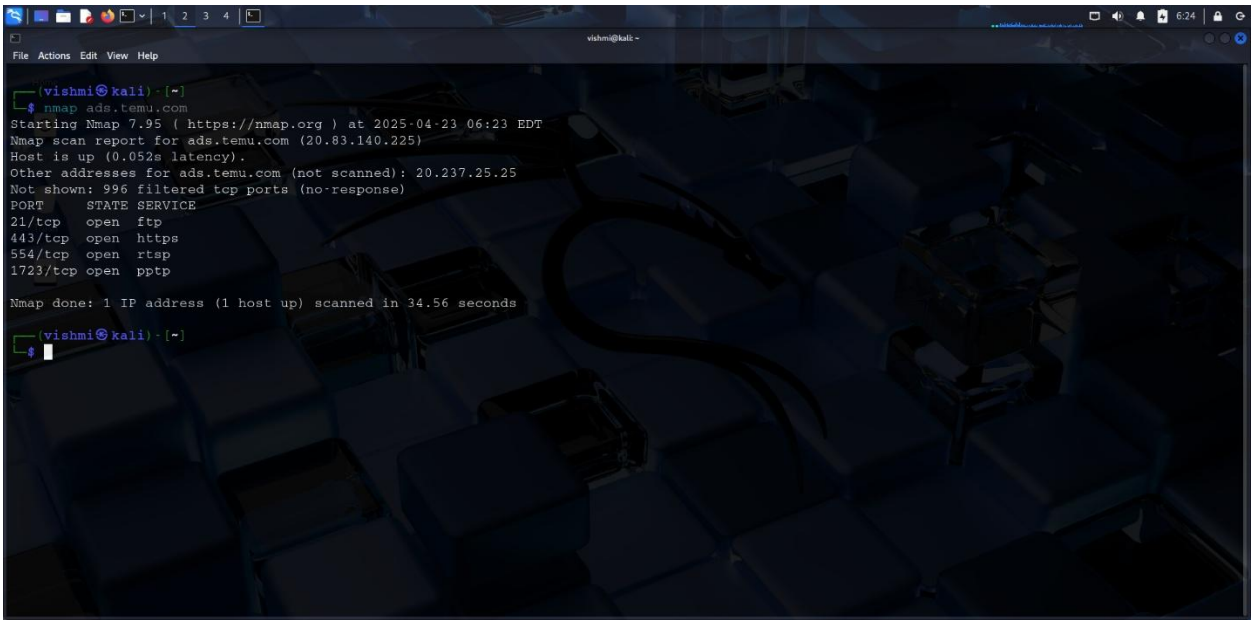
* ***[INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'***
[SQLmap is still in the process of testing for SQL injection using Boolean-based techniques.]

**** [CRITICAL] target URL content appears to be heavily dynamic.***

Searching for vulnerabilities

Nmap

Nmap (Network Mapper) is a strong, open-source network scanning program that uses packet transmission and response analysis to find hosts and services on a computer network. To find open ports, running services, operating systems, and active devices on a network, network managers and security experts utilize Nmap. Network inventory, vulnerability assessment, security auditing, and penetration testing are among its many uses.



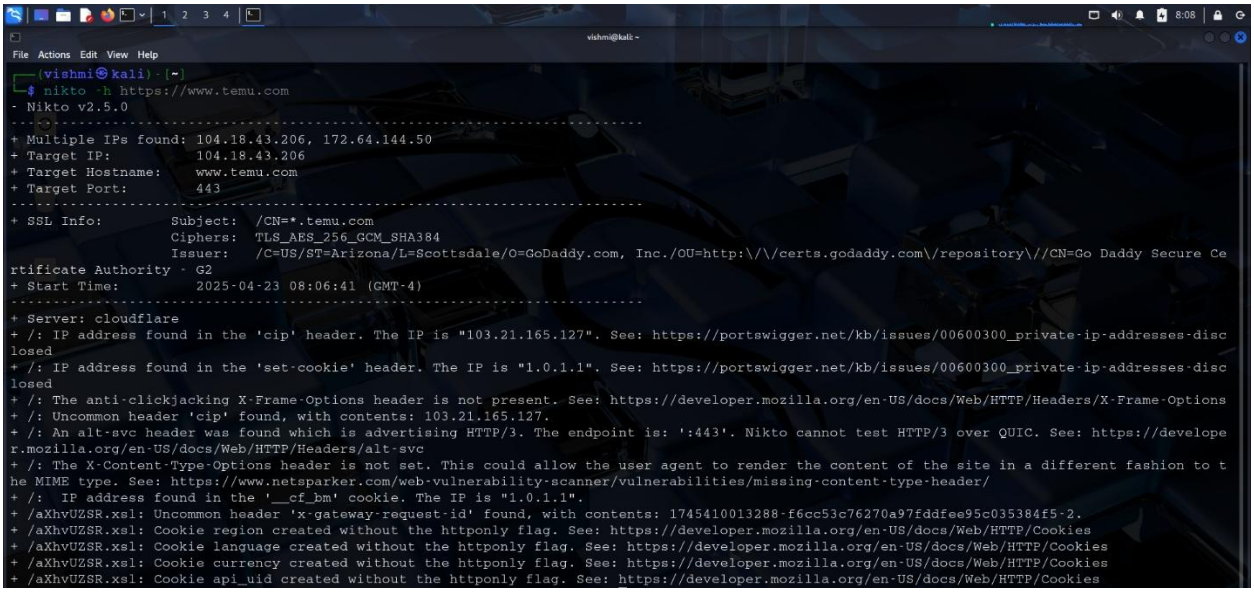
I discovered these details by using Nmap to search *ads.temu.org*.

PORT	STATE	SERVICE
21/tcp	open	ftp
443/tcp	open	https
554/tcp	open	rtsp
1723/tcp	open	pptp

PORT	SERVICE	Vulnerabilities
21/tcp	ftp	Unencrypted credentials are accepted.
443/tcp	https	Deprecated TLS versions are supported.
554/tcp	Rtsp	Usually doesn't have authenticity.
1723/tcp	pptp	Makes use of a weak encryption

Nikto

An open-source program called Nikto scans web servers for common vulnerabilities, malicious files, outdated software, and improperly configured settings, among other potential security issues. It is widely used for penetration testing and assessments, but it functions best when combined with other tools.



Security issues found on ***https://www.temu.com's*** by Nikto Scan

*IP address are found in the ‘cip’ and ‘set-cookie’ header.

*The anti-clickjacking x-frame-options header is not present.

*Uncommon header ‘x-gateway-request-id’ found.

*The x-content-type-options header is not set.

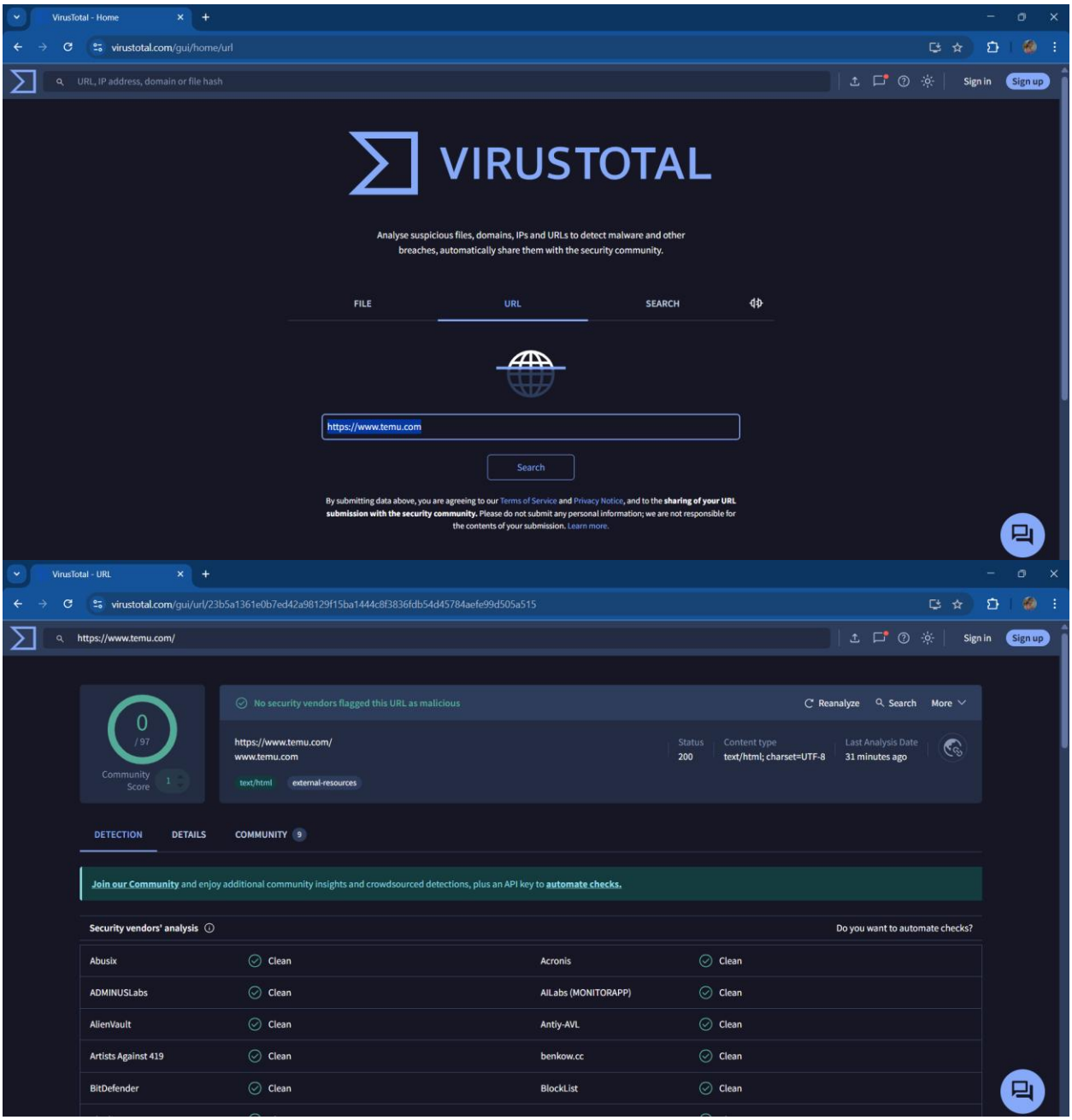
*Cookie language created without the httponly flag.

*Cookie currency created without the httponly flag.

Virustotal

Virustotal is a free web service called VirusTotal employs 70 antivirus engines and URL blocklisting services to scan files and URLs for malware, adware, and other malicious content.

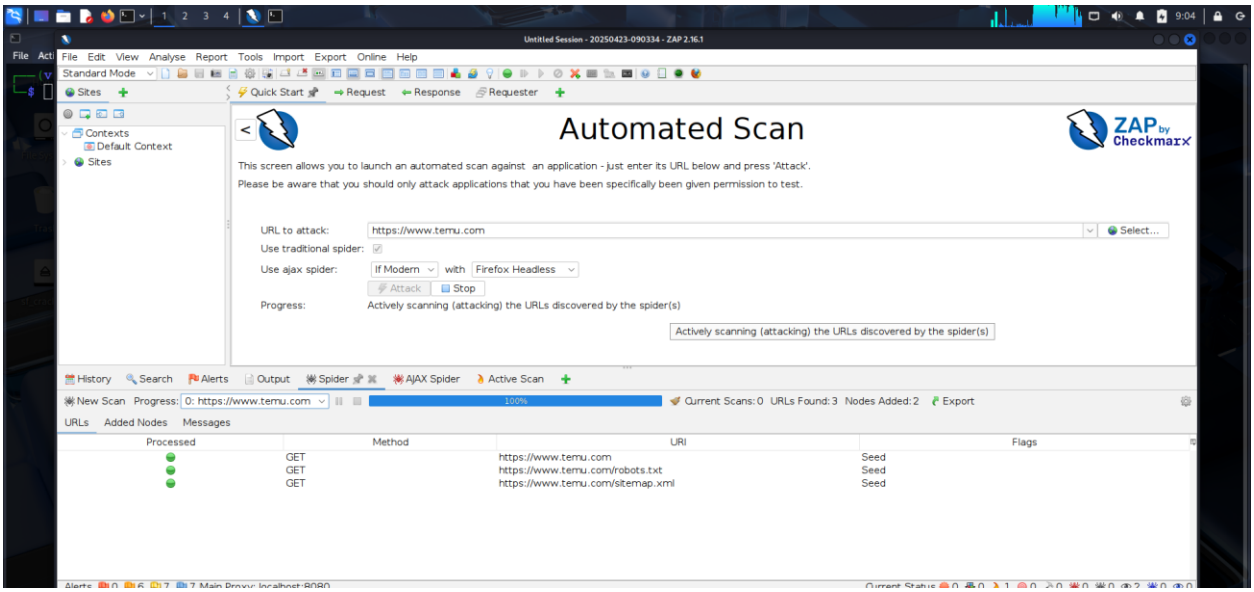
I entered https://www.temu.com in URL section .



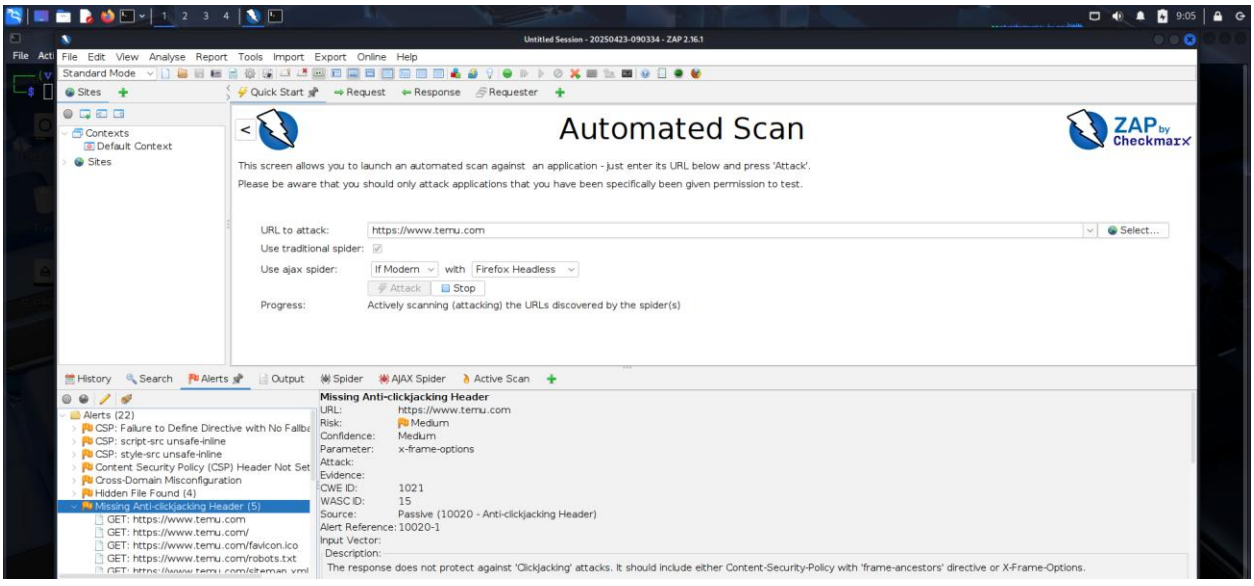
OWASP ZAP

A free and open-source security tool called ***OWASP ZAP (Zed Attack Proxy)*** simulates attacks and examines how an application behaves when it is running to help in discovering and fixing vulnerabilities in web applications.

In here, I entered the target URL [***https://www.temu.com***] designated textbox, simply select "Attack" to initiate the scanning process.



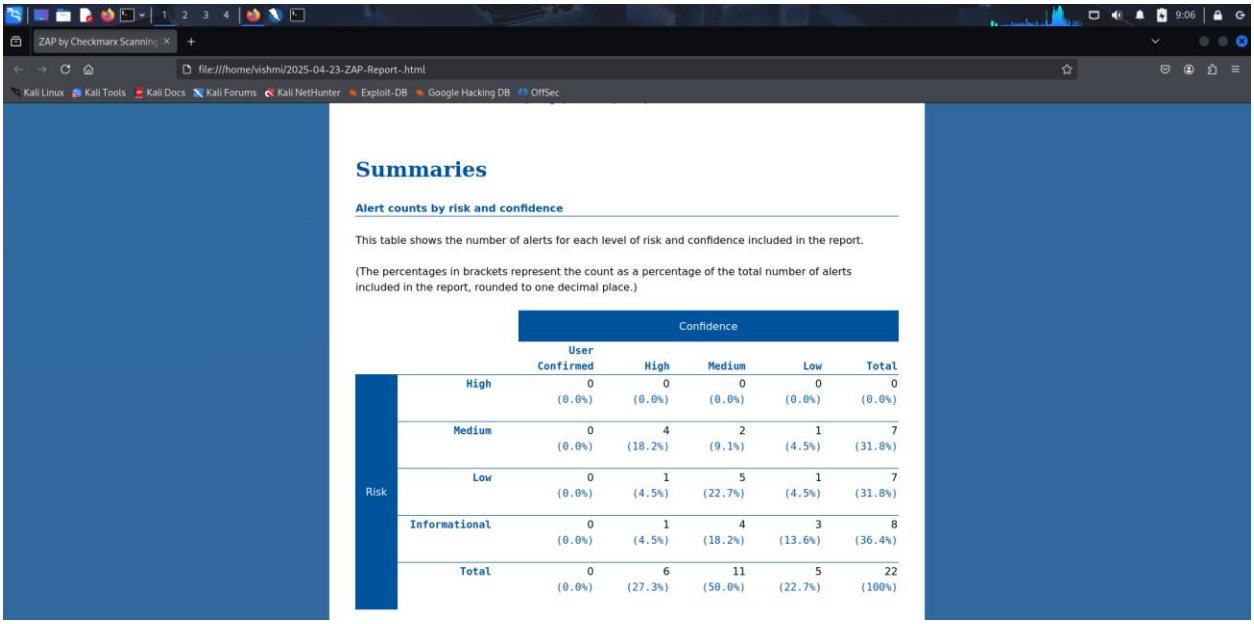
As next step, I entered to the Alerts tab. Here it’s detected a vulnerability.



After finishing, it is possible to obtain a thorough report of the results by choosing "Report." The results of scanning many domains are displayed in the screenshots below.

Report = file:///home/vishmi/2025-04-23-ZAP-Report-.html

Please take note that these vulnerabilities have been rated using the OWASP risk rating methodology, which is available at this link.[*OWASP Risk Rating Methodology*]



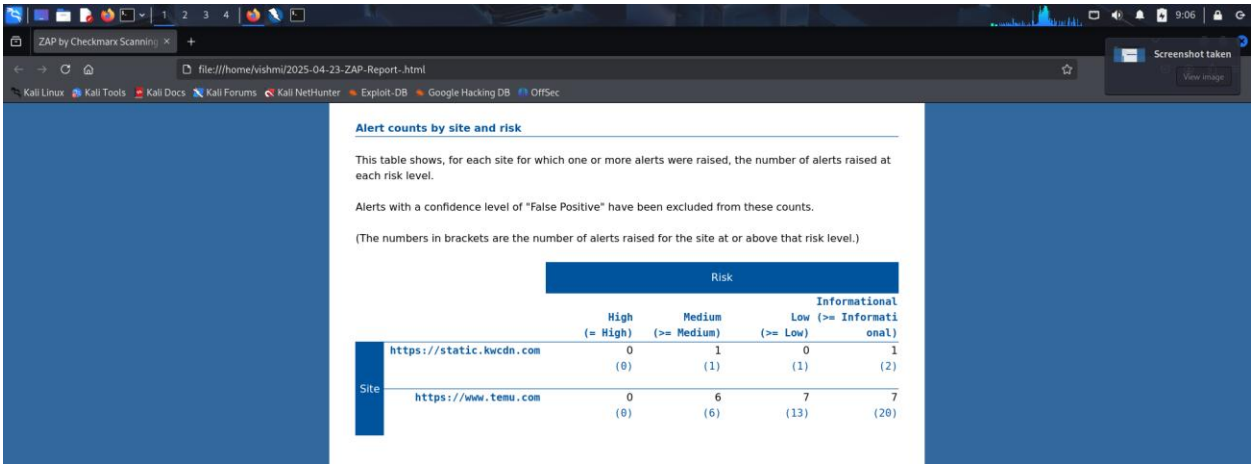
Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	4 (18.2%)	2 (9.1%)	1 (4.5%)	7 (31.8%)
	Low	0 (0.0%)	1 (4.5%)	5 (22.7%)	1 (4.5%)	7 (31.8%)
	Informational	0 (0.0%)	1 (4.5%)	4 (18.2%)	3 (13.6%)	8 (36.4%)
	Total	0 (0.0%)	6 (27.3%)	11 (50.0%)	5 (22.7%)	22 (100%)



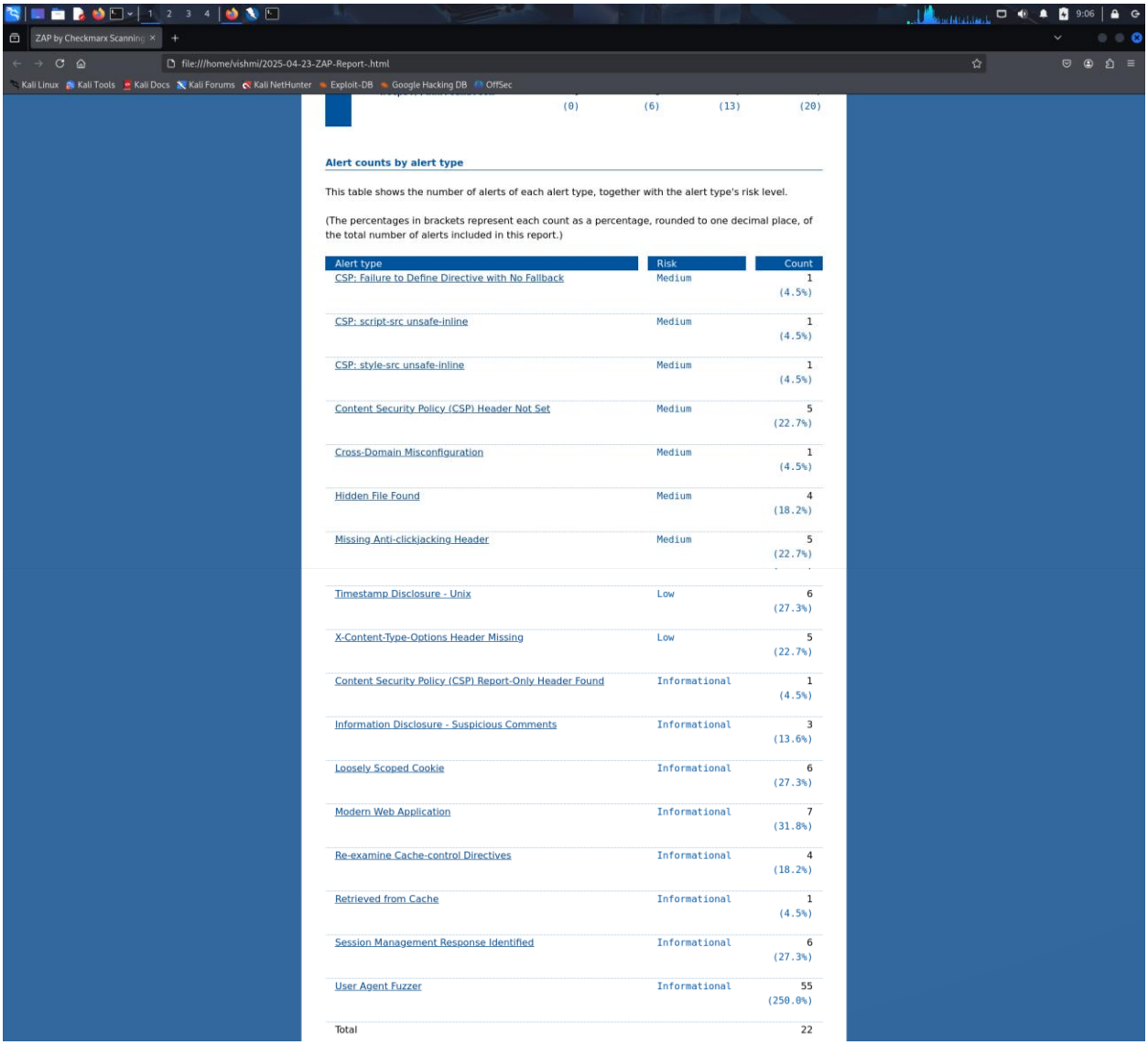
Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://static.kwcdn.com	0 (0)	1 (1)	0 (1)	1 (2)
	https://www.temu.com	0 (0)	6 (6)	7 (13)	7 (20)


ZAP by Checkmarx Scanning
file:///home/vishmi/2025-04-23-ZAP-Report-.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
(0)
(6)
(13)
(20)
Alert counts by alert type
This table shows the number of alerts of each alert type, together with the alert type's risk level.
(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)
Alert type
Risk
Count
CSP: Failure to Define Directive with No Fallback
Medium
1 (4.5%)
CSP: script-src unsafe-inline
Medium
1 (4.5%)
CSP: style-src unsafe-inline
Medium
1 (4.5%)
Content Security Policy (CSP) Header Not Set
Medium
5 (22.7%)
Cross-Domain Misconfiguration
Medium
1 (4.5%)
Hidden File Found
Medium
4 (18.2%)
Missing Anti-clickjacking Header
Medium
5 (22.7%)
Timestamp Disclosure - Unix
Low
6 (27.3%)
X-Content-Type-Options Header Missing
Low
5 (22.7%)
Content Security Policy (CSP) Report-Only Header Found
Informational
1 (4.5%)
Information Disclosure - Suspicious Comments
Informational
3 (13.6%)
Loosely Scoped Cookie
Informational
6 (27.3%)
Modern Web Application
Informational
7 (31.8%)
Re-examine Cache-control Directives
Informational
4 (18.2%)
Retrieved from Cache
Informational
1 (4.5%)
Session Management Response Identified
Informational
6 (27.3%)
User Agent Fuzzer
Informational
55 (250.0%)
Total
22

Vulnerabilities

a.Vulnerability Title	**Missing Anti-Clickjacking Header**
b.Vulnerability Description	The target domain's HTTP response headers lack crucial X-Frame-Options or Content-Security-Policy headers, exposing it to clickjacking attacks, potentially tricking users into interacting with hidden elements.
c.Affected Components	The target domain's server configuration and response headers.
d.Impact Assessment	Anti-clickjacking headers prevent users from unknowingly engaging with malicious site frames, potentially leading to unauthorized actions like financial transactions, login theft, or sensitive information changes.
e.Steps to Reproduce	1.Create a simple HTML page embedding the target site in an iframe: html=***<iframe src="http://target-site.com" style="width:100%; height:100%;"></iframe>*** 2.Load the HTML page in a browser. 3.Verify that the embedded site loads successfully within the iframe, confirming the absence of an anti-clickjacking mechanism.
f.Proof of Concept (if applicable)	Include a screenshot showing the site successfully embedded within an iframe, demonstrating its vulnerability to clickjacking.
g.Proposed Mitigation or Fix	Add the ***X-Frame-Options*** header to HTTP responses to prevent embedding

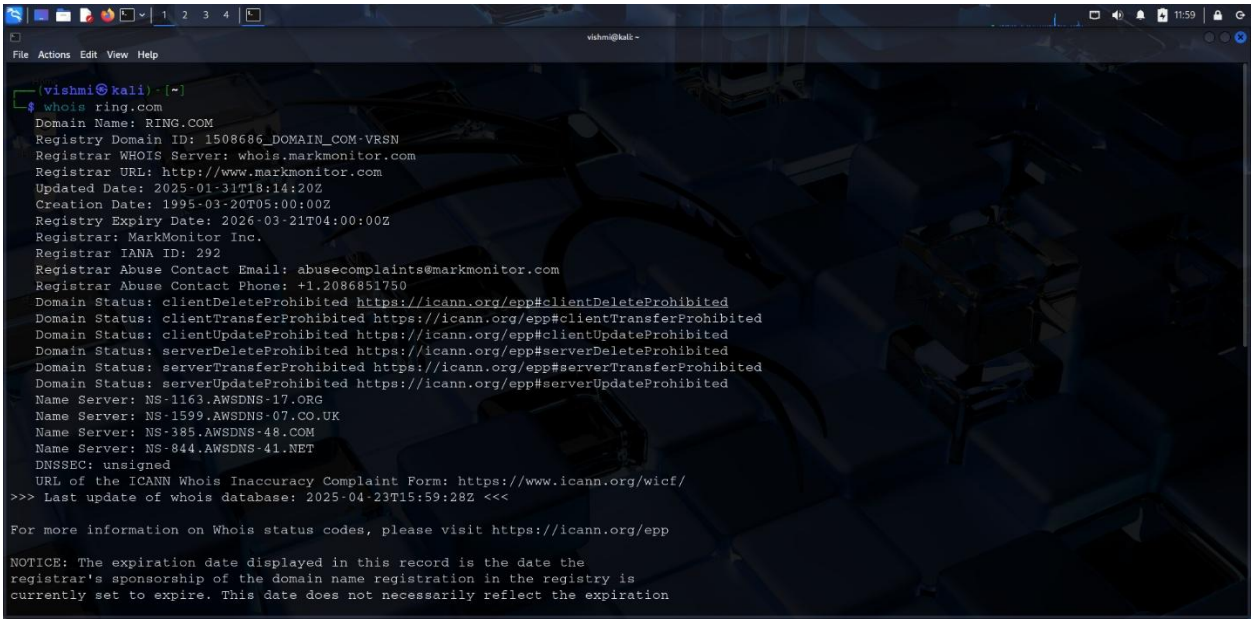
Report-05

Web Audit
ring.com

Domain = *ring.com*
Sub-domain = *admin.ring.com*
URL = *https://www.ring.com*

Target Reconnaissance

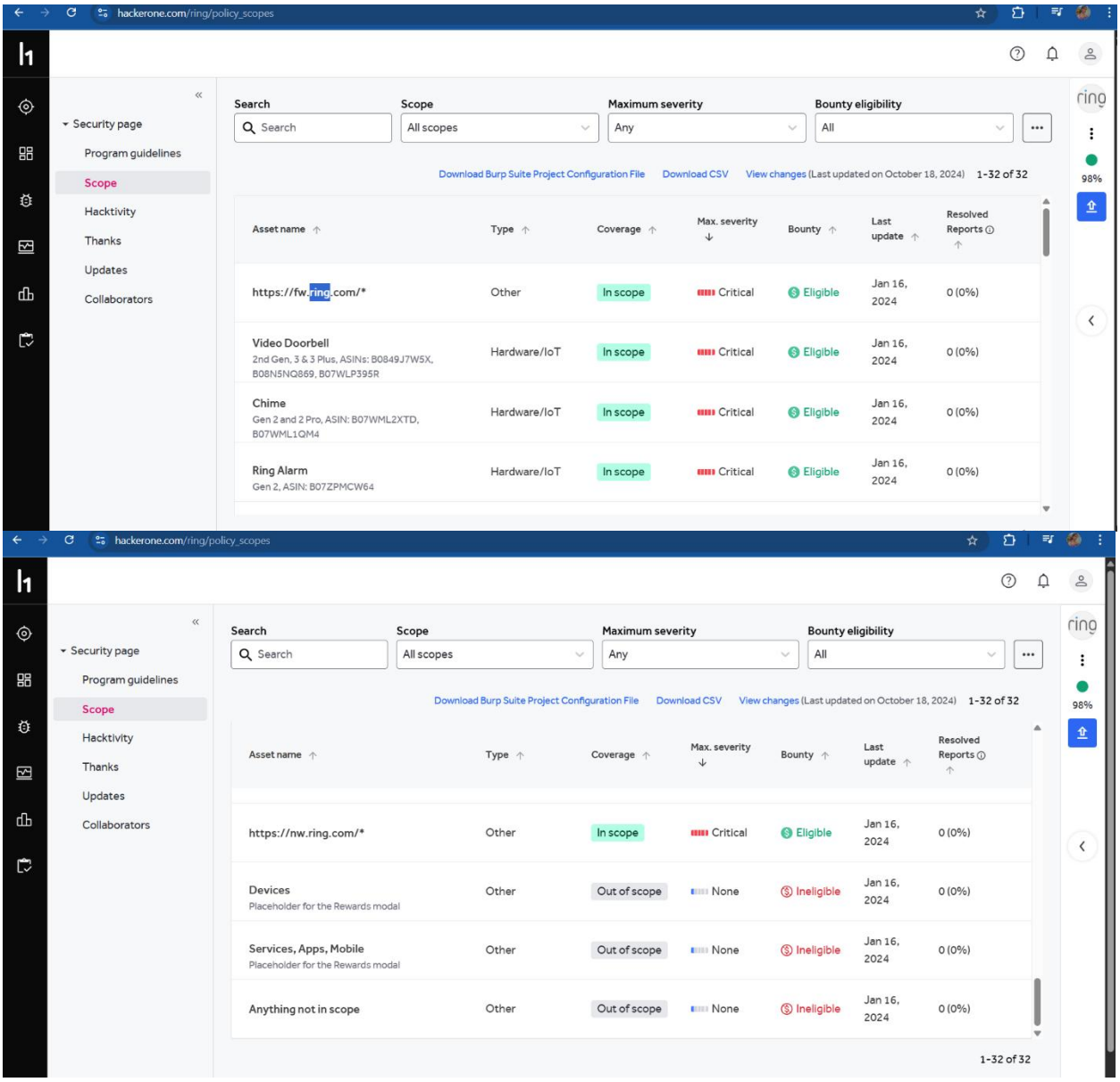
Introduction to Sony and Audit Scope



The most well-known products from home security company **Ring** are its security cameras and smart video doorbells. Ring, which was founded in 2013 and subsequently purchased by Amazon, gives homeowners mobile access and real-time monitoring capabilities so they can keep an eye on their property from anywhere. For consumers who are worried about safety and security, its product ecosystem-which includes video doorbells, floodlight cameras, alarm systems, and connectivity with Amazon Alexa-offers ease and peace of mind.

These subdomains (and all included) have been approved as legitimate subdomains for testing in the **Hackerone** Bug Bounty program.

Eligible in-scope subdomains for bug bounty program are mentioned below



Information gathering phase.

The information-gathering phase, often known as reconnaissance or recon, is essential to both assessments of security and cyberattacks. In order to map out the target's structure and determine how it functions, the target of this stage is to gather as much information as possible about it. Because it helps auditors or attackers identify vulnerabilities that could be exploited later on, this fundamental understanding is essential.

There are two main approaches to information gathering

1.Active Scanning :

Involves direct interaction with the target, which can generate noticeable activity and typically uncovers a wealth of details about the system.

2.Passive Scanning :

Seeks to observe the target without direct engagement, resulting in less detectable activity but often providing more limited information

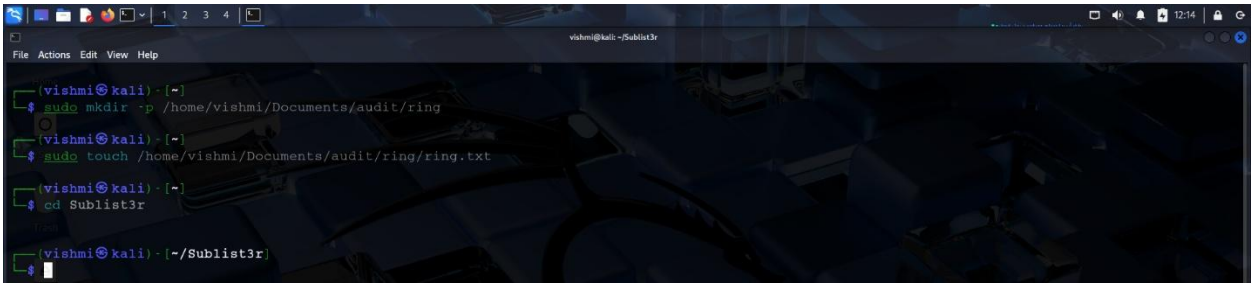
Finding active subdomains and their states

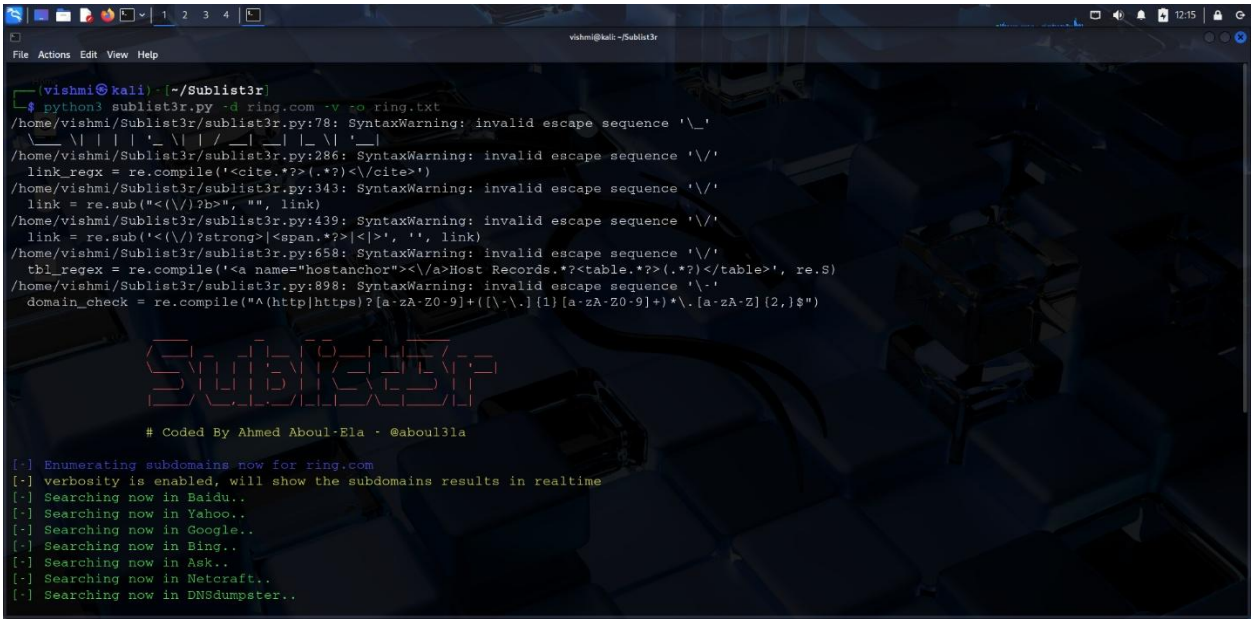
Sublist3r

Sublist3r is an open-source Python application that uses OSINT (Open Source Intelligence) techniques to quickly and effectively scan subdomains. Subdomains linked to a target domain can be found by penetration testers, security researchers, and bug bounty hunters using a variety of search engine queries (including Google, Yahoo, Bing, Baidu, and Ask). Additionally, Sublist3r includes a brute-force module (subbrute) to employ a stronger wordlist to improve the probability of discovering more subdomains.

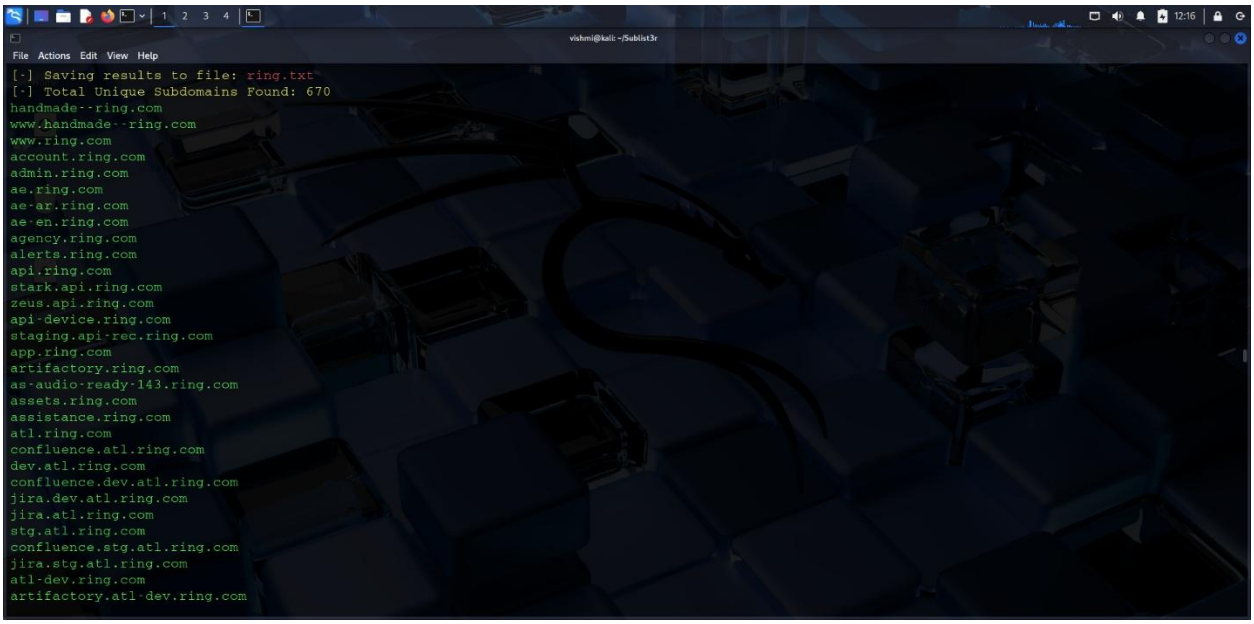
I created a .txt file to store the subdomain headers that were initiated via sublist3r.

Path to .txt file = ***home/vishmi/Documents/audit/ring/ ring.txt***





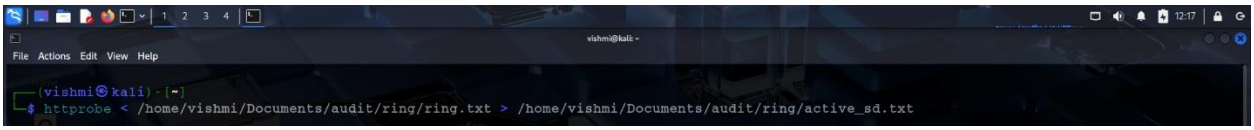
I got, these subdomains according to the ***ring.com*** domain.



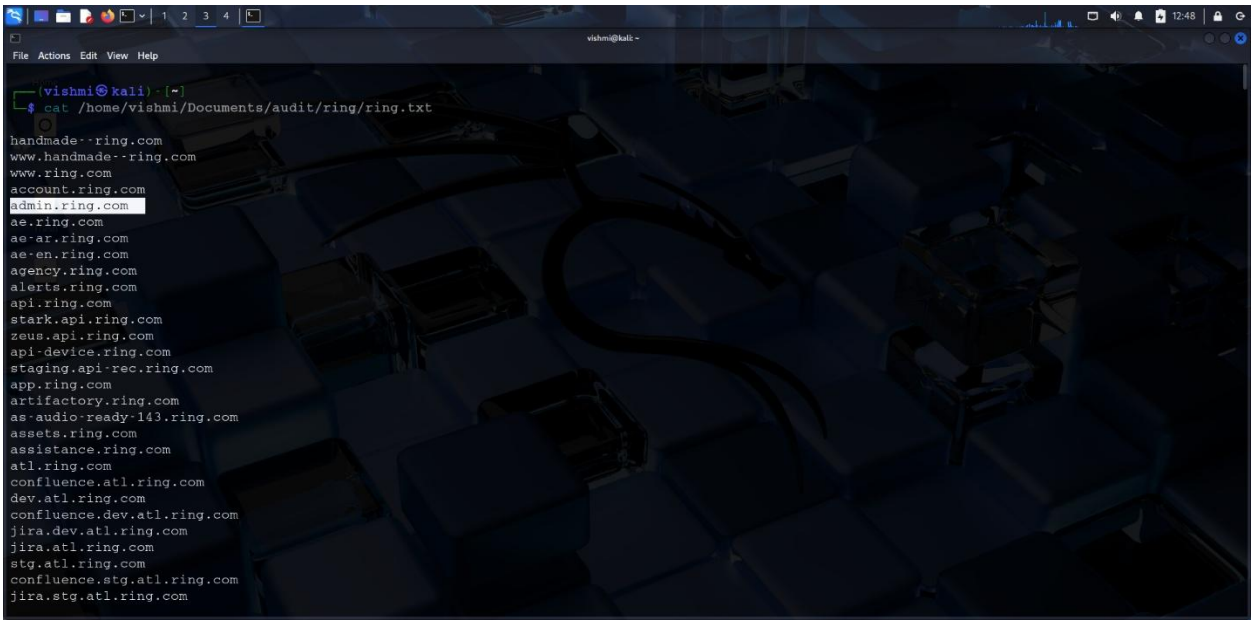
HTTProbe

HTTProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing on achievable goals by providing you with the URLs of active domains.

I am using the text file generated before by the sublist3r and stored the active subdomains to another new .txt file.



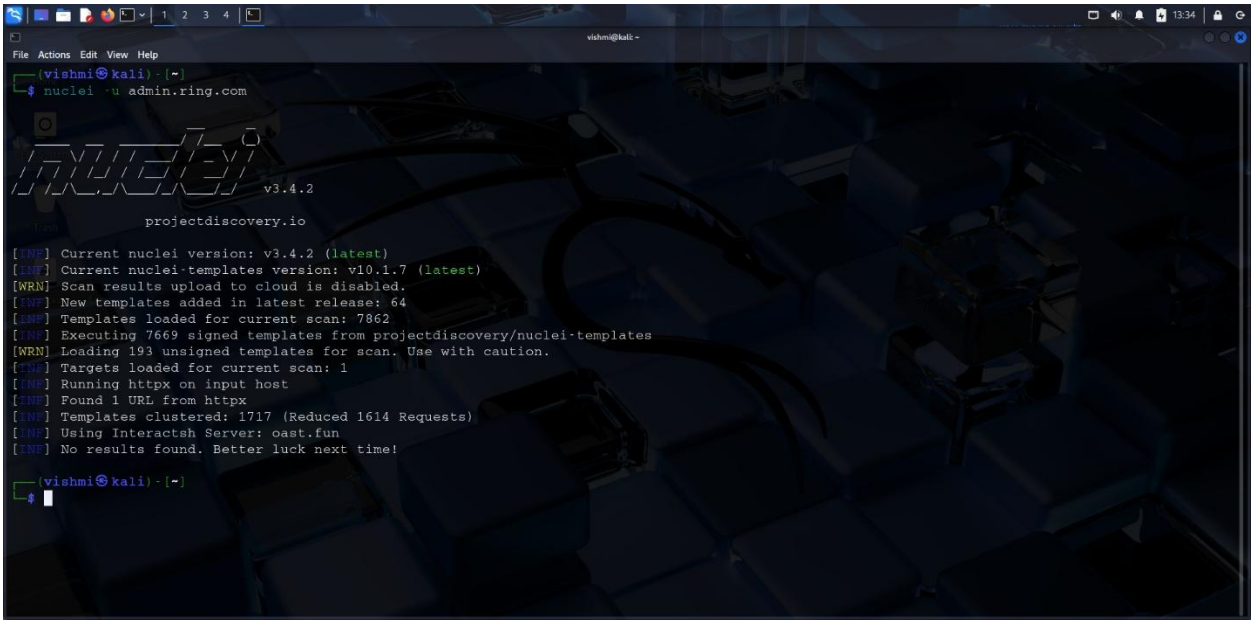
Below, we can see the active subdomains related to the ***ring.com*** domain.



To move forward, I chose the active subdomain as **“admin.*ring*.com”.**

Nuclei

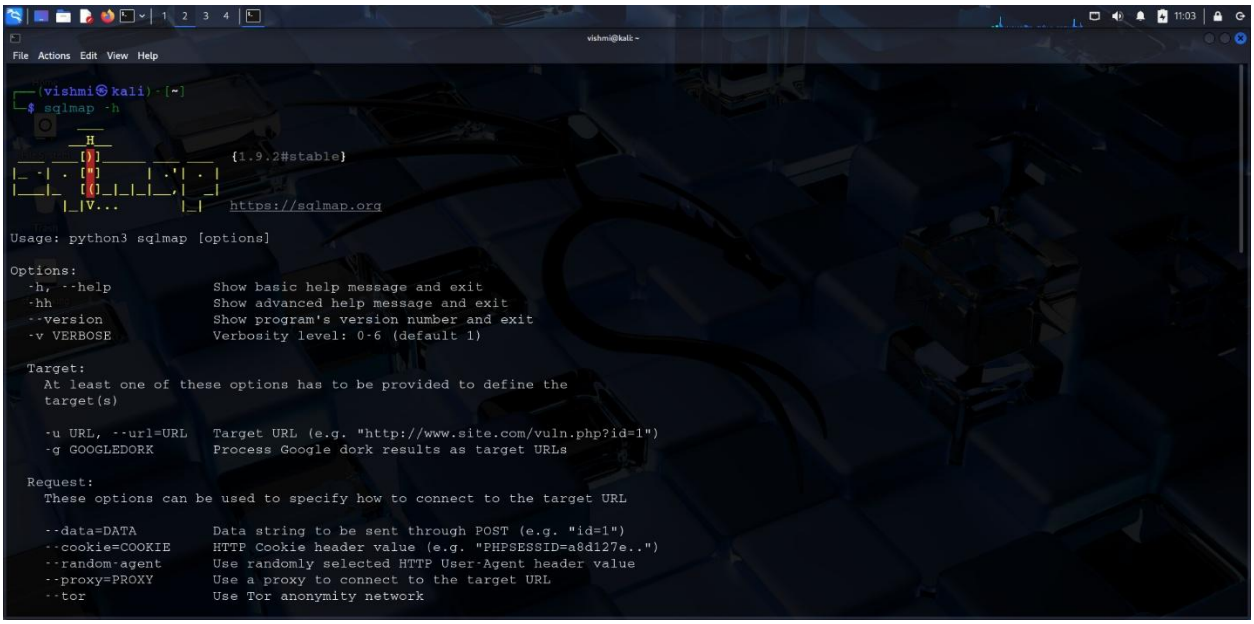
Nuclei is an open-source vulnerability scanner developed by ProjectDiscovery for security professionals, penetration testers, and bug bounty hunters. It uses customizable YAML("Yet Another Markup Language") -based templates to identify vulnerabilities such as misconfigurations, outdated software, and known CVEs (Common Vulnerabilities and Exposures).

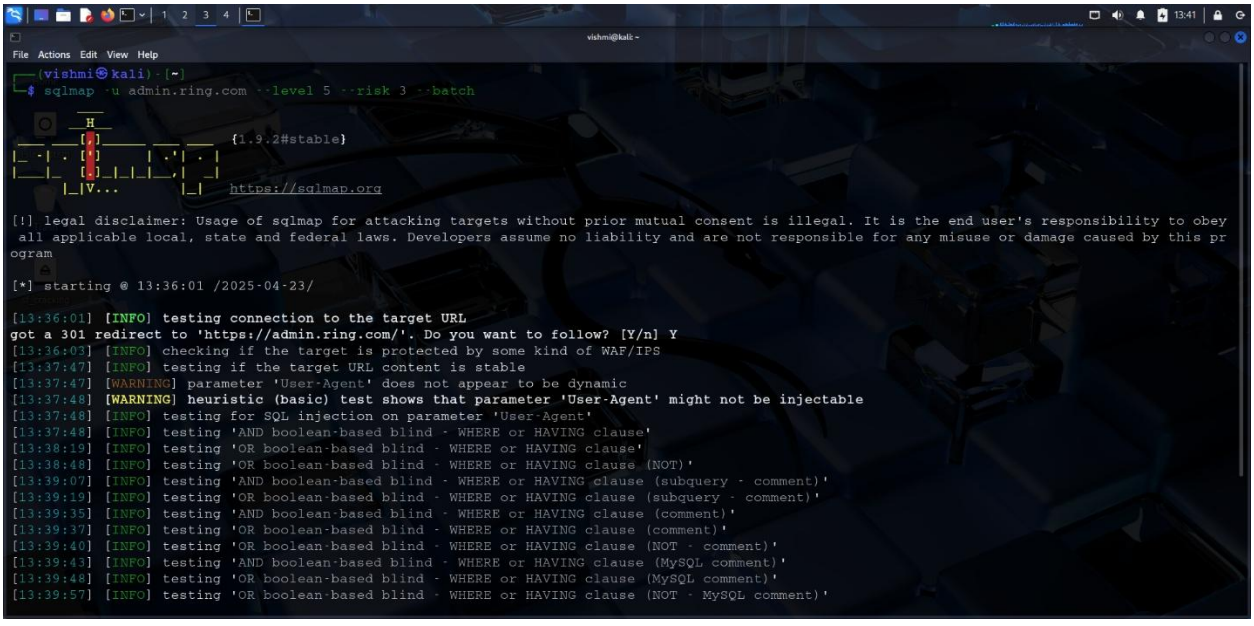


Here, the nuclei scan found no issue.

SQLmap

An open-source penetration testing tool called SQLmap makes it easier to find and take advantage of SQL injection flaws in web apps. If the database permits, it can even access the underlying file system or run commands on the server in addition to identifying the type of database and extracting data. Security experts frequently use it to evaluate and protect web apps from SQL injection attacks.





Option	Meaning
-u	For basic testing, the target URL is required.
--level5	Increases the number of payloads and tests that are done (maximum is 5).
--risk3	Increase the danger level of the payloads used (maximum is 3)
--batch	Executes SQLMap in a non-interactive mode, selecting default responses automatically.

Detected Information

[WARNING] heuristic (basic) test shows that parameter 'User-Agent' might be injectable

[This is a *potential* vulnerability, but not confirmed.]

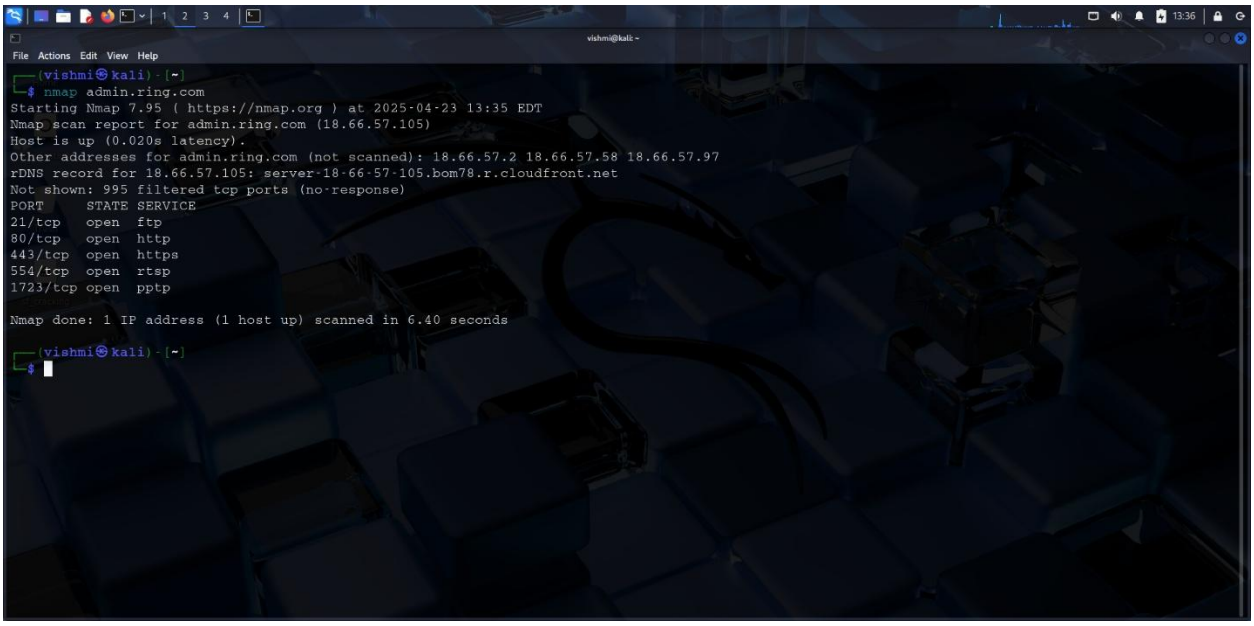
* ***[INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'***

[SQLmap is still in the process of testing for SQL injection using Boolean-based techniques.]

Searching for vulnerabilities

Nmap

Nmap (Network Mapper) is a strong, open-source network scanning program that uses packet transmission and response analysis to find hosts and services on a computer network. To find open ports, running services, operating systems, and active devices on a network, network managers and security experts utilize Nmap. Network inventory, vulnerability assessment, security auditing, and penetration testing are among its many uses.



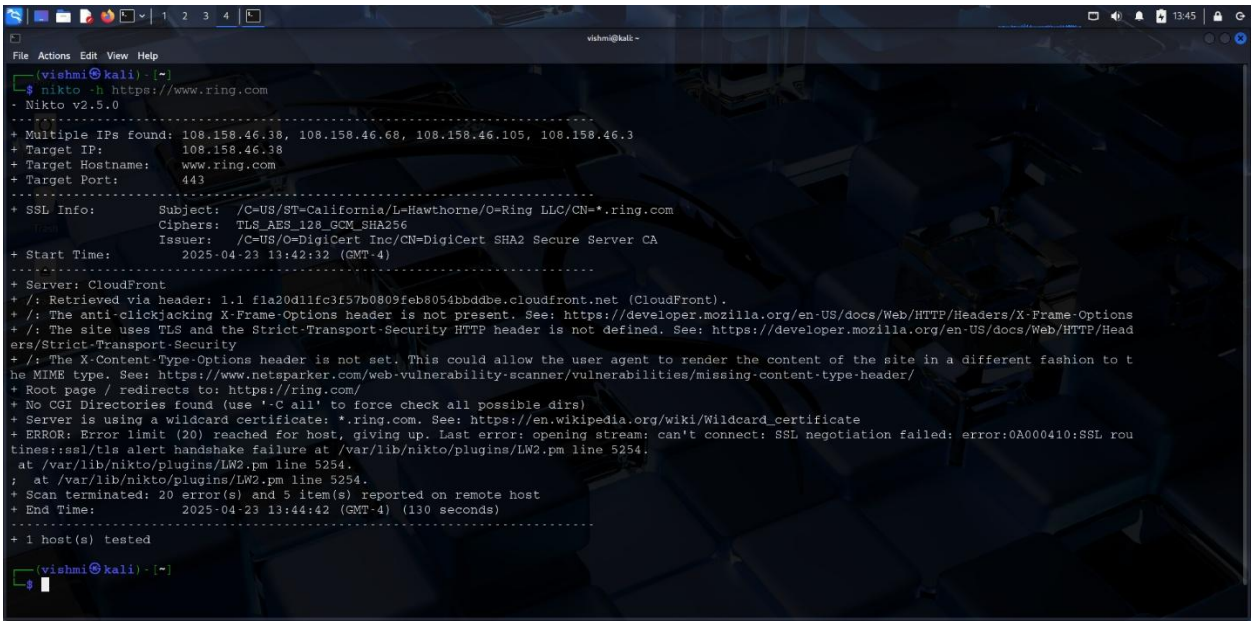
I discovered these details by using Nmap to search *admin.ring.com.*

PORT	STATE	SERVICE
21/tcp	open	ftp
80/tcp	open	http
443/tcp	open	https
554/tcp	open	rtsp
1723/tcp	open	pptp

PORT	SERVICE	Vulnerabilities
21/tcp	ftp	Unencrypted credentials are accepted.
80/tcp	http	Transmits plain text data.
443/tcp	https	Deprecated TLS versions are supported.
554/tcp	Rtsp	Usually doesn't have authenticity.
1723/tcp	pptp	Makes use of a weak encryption

Nikto

An open-source program called Nikto scans web servers for common vulnerabilities, malicious files, outdated software, and improperly configured settings, among other potential security issues. It is widely used for penetration testing and assessments, but it functions best when combined with other tools.



Security issues found on ***https://www.ring.com"s*** by Nikto Scan

* The anti-clickjacking x-frame-options header is not present.

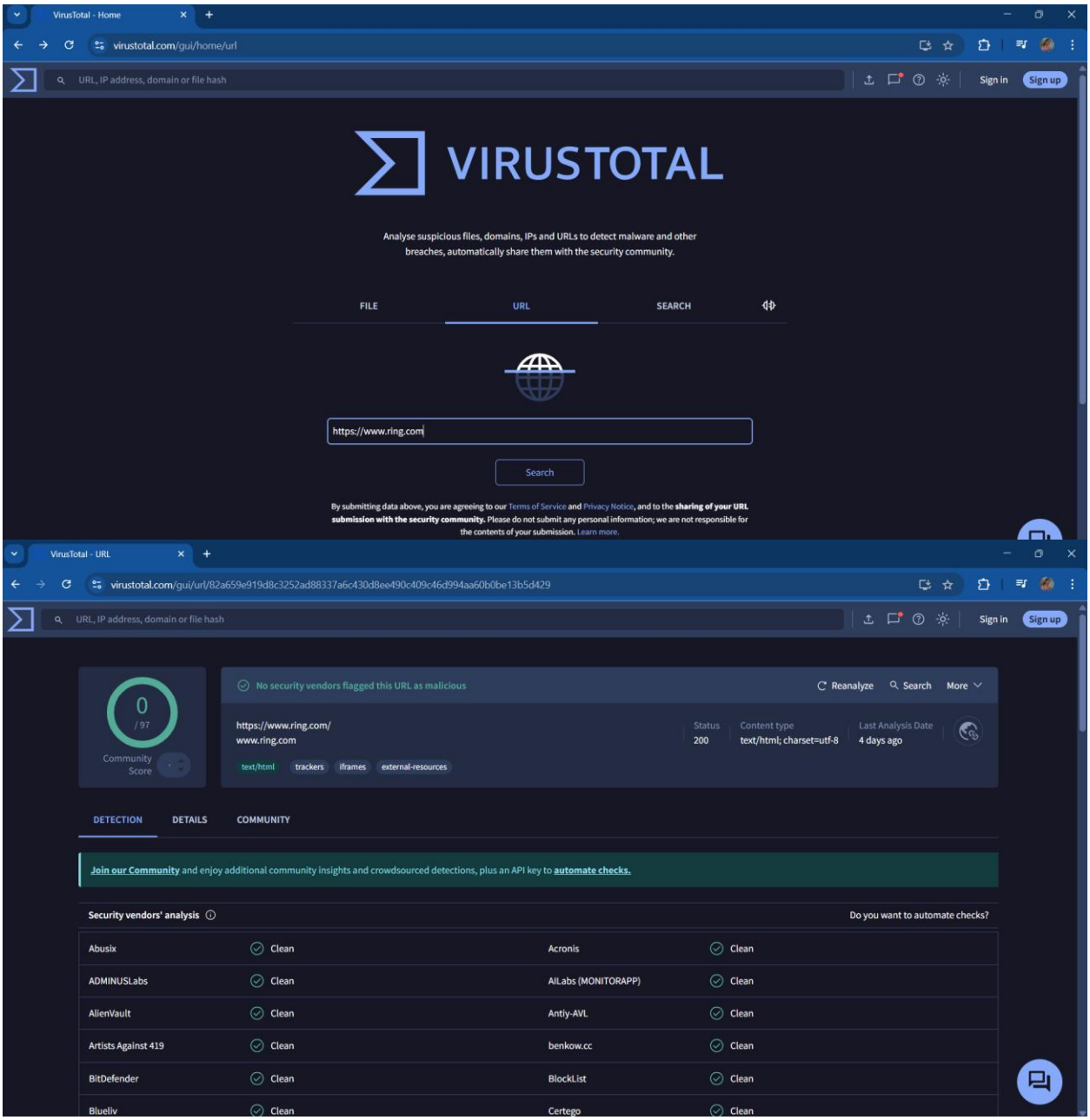
*The x-content-type-options header is not set.

*The site uses TLS and the Strict-Transport-Security HTTP header is not defined.

Virustotal

Virustotal is a free web service called VirusTotal employs 70 antivirus engines and URL blocklisting services to scan files and URLs for malware, adware, and other malicious content.

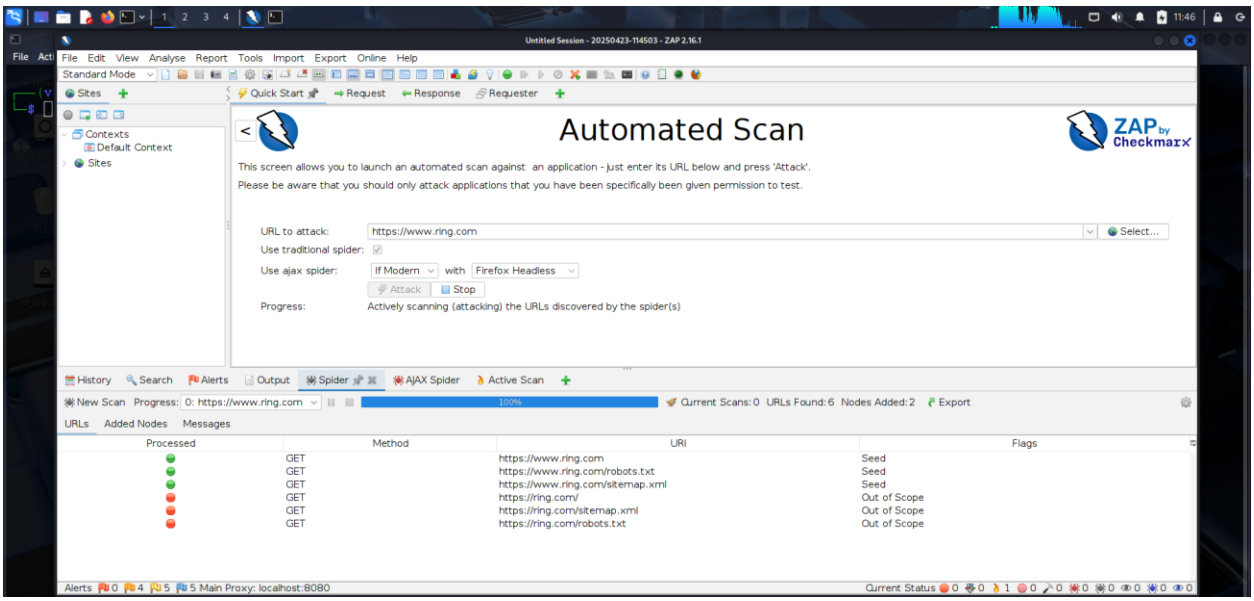
I entered https://www.ring.com in URL section.



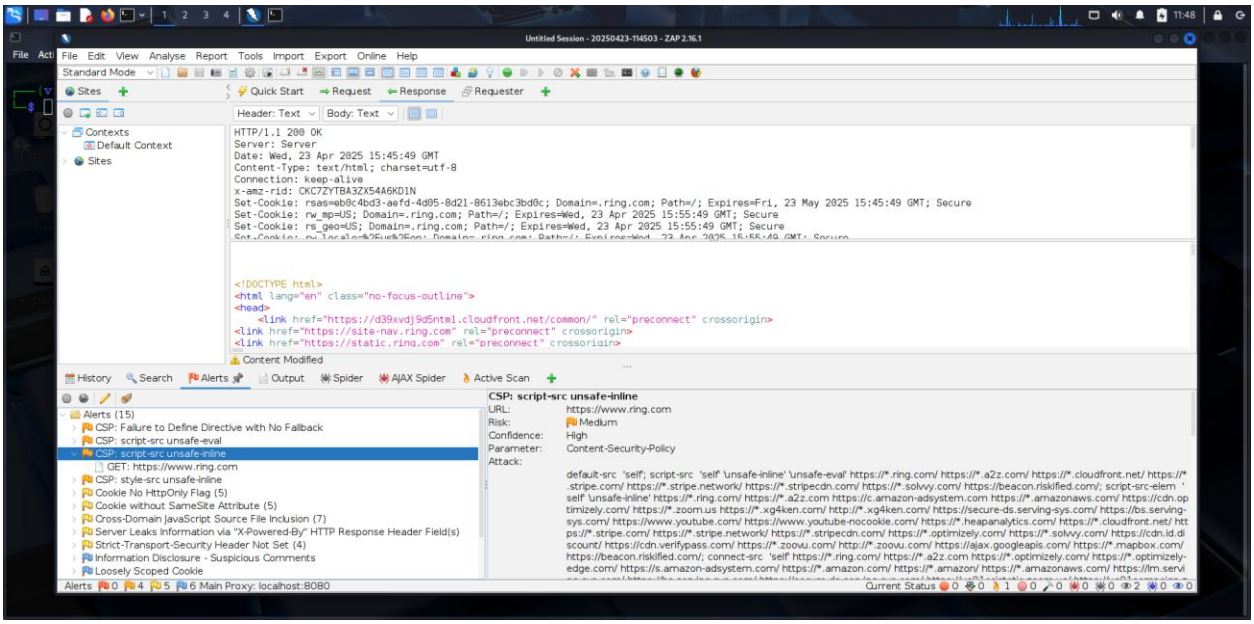
OWASP ZAP

A free and open-source security tool called ***OWASP ZAP (Zed Attack Proxy)*** simulates attacks and examines how an application behaves when it is running to help in discovering and fixing vulnerabilities in web applications.

In here, I entered the target URL [***https://www.ring.com***] designated textbox, simply select "Attack" to initiate the scanning process.



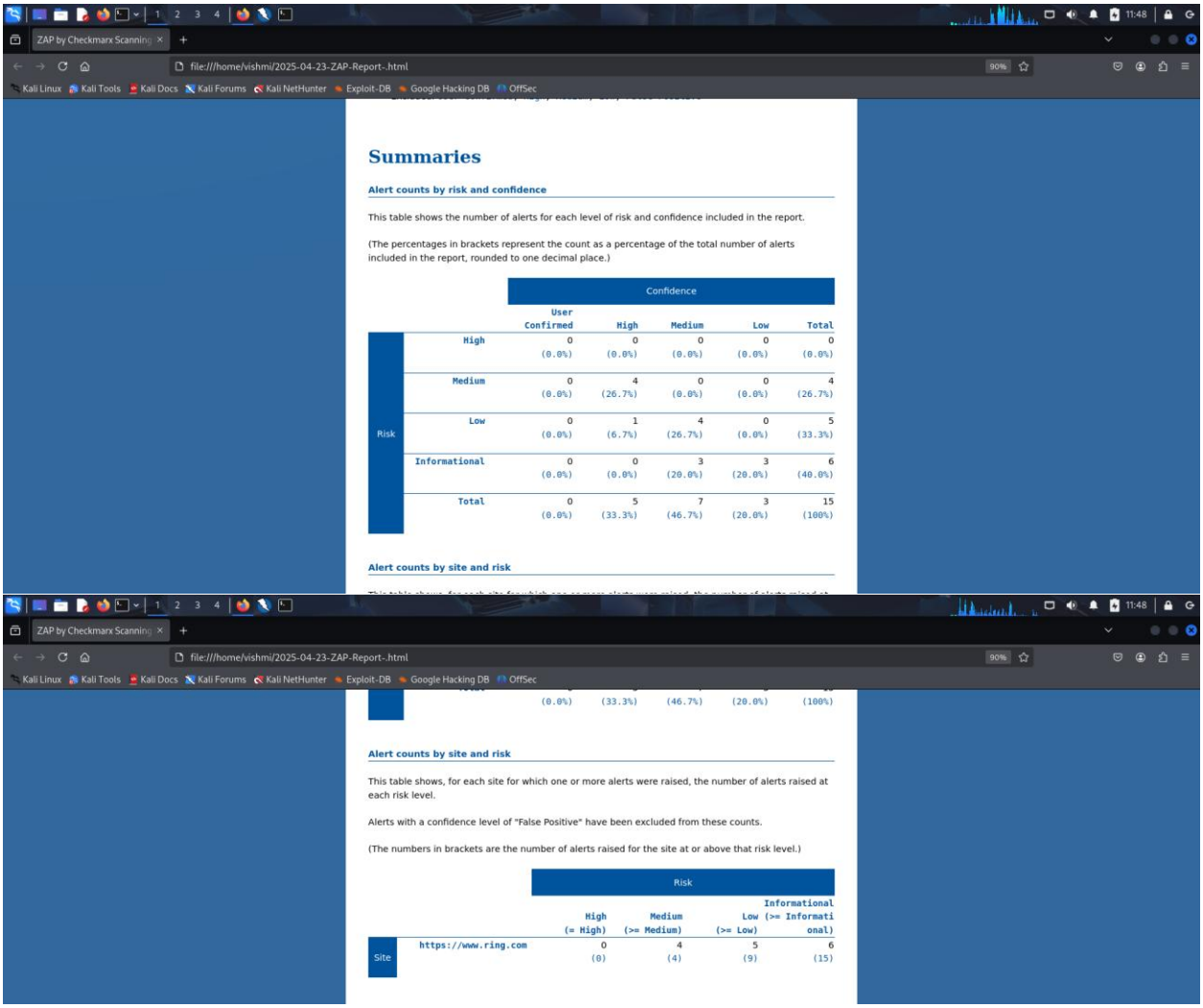
As next step, I entered to the Alerts tab. Here it's detected a vulnerability.



After finishing, it is possible to obtain a thorough report of the results by choosing "Report." The results of scanning many domains are displayed in the screenshots below.

Report = file:///home/vishmi/2025-04-23-ZAP-Report-.html

Please take note that these vulnerabilities have been rated using the OWASP risk rating methodology, which is available at this link.[*OWASP Risk Rating Methodology*]



Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	4 (26.7%)	0 (0.0%)	0 (0.0%)	4 (26.7%)
	Low	0 (0.0%)	1 (6.7%)	4 (26.7%)	0 (0.0%)	5 (33.3%)
	Informational	0 (0.0%)	0 (0.0%)	3 (20.0%)	3 (20.0%)	6 (40.0%)
	Total	0 (0.0%)	5 (33.3%)	7 (46.7%)	3 (20.0%)	15 (100%)

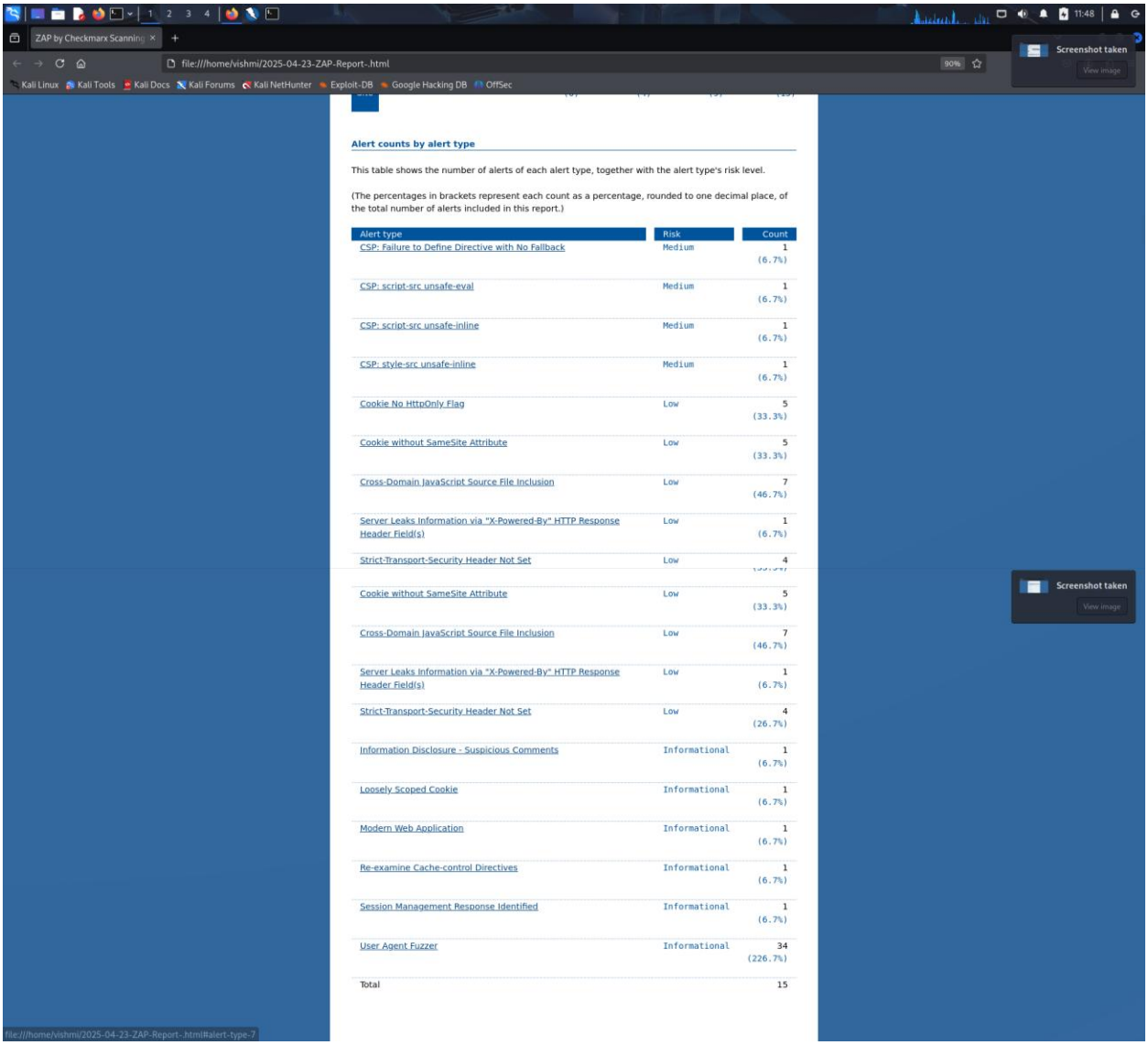
Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://www.ring.com	0 (0)	4 (4)	5 (9)	6 (15)


ZAP by Checkmarx Scanning
file:///home/vishmi/2025-04-23-ZAP-Report-.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Screenshot taken
View image
Alert counts by alert type
This table shows the number of alerts of each alert type, together with the alert type's risk level.
(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)
Alert type
Risk
Count
CSP: Failure to Define Directive with No Fallback
Medium
1 (6.7%)
CSP: script-src unsafe-eval
Medium
1 (6.7%)
CSP: script-src unsafe-inline
Medium
1 (6.7%)
CSP: style-src unsafe-inline
Medium
1 (6.7%)
Cookie No HttpOnly Flag
Low
5 (33.3%)
Cookie without SameSite Attribute
Low
5 (33.3%)
Cross-Domain JavaScript Source File Inclusion
Low
7 (46.7%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Low
1 (6.7%)
Strict-Transport-Security Header Not Set
Low
4 (26.7%)
Cookie without SameSite Attribute
Low
5 (33.3%)
Cross-Domain JavaScript Source File Inclusion
Low
7 (46.7%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Low
1 (6.7%)
Strict-Transport-Security Header Not Set
Low
4 (26.7%)
Information Disclosure - Suspicious Comments
Informational
1 (6.7%)
Loosely Scoped Cookie
Informational
1 (6.7%)
Modern Web Application
Informational
1 (6.7%)
Re-examine Cache-control Directives
Informational
1 (6.7%)
Session Management Response Identified
Informational
1 (6.7%)
User Agent Fuzzer
Informational
34 (226.7%)
Total
15
Screenshot taken
View image
file:///home/vishmi/2025-04-23-ZAP-Report-.html#alert-type-7

Vulnerabilities

a.Vulnerability Title	**CSP:script-src unsafe-inline**
b.Vulnerability Description	The directive `script-src 'unsafe-inline'` in the target website's Content Security Policy (CSP) allows inline scripts to run, making the website vulnerable to cross-site scripting attacks.
c.Affected Components	HTTP response headers containing the CSP configuration.
d.Impact Assessment	This vulnerability allows attackers to insert and run malicious code. Data theft, session hijacking, or unauthorized activities taken on the user's behalf are examples of possible outcomes.
e.Steps to Reproduce	1.Use OWASP ZAP or browser developer tools to examine the target website's HTTP response headers. 2.Find the CSP directive and make sure script-src 'unsafe-inline' is present. 3.Inject a simple inline script html=<script>alert('XSS Vulnerability');</script>
f.Proof of Concept (if applicable)	Provide a screenshot showing the effective execution of an inline script and the CSP directive in the HTTP response headers.
g.Proposed Mitigation or Fix	1.Use http; *[Content-Security-Policy: script-src 'self' 'nonce-<random-value>';]* 2.Avoid using *unsafe-inline* entirely to ensure robust protection against XSS.

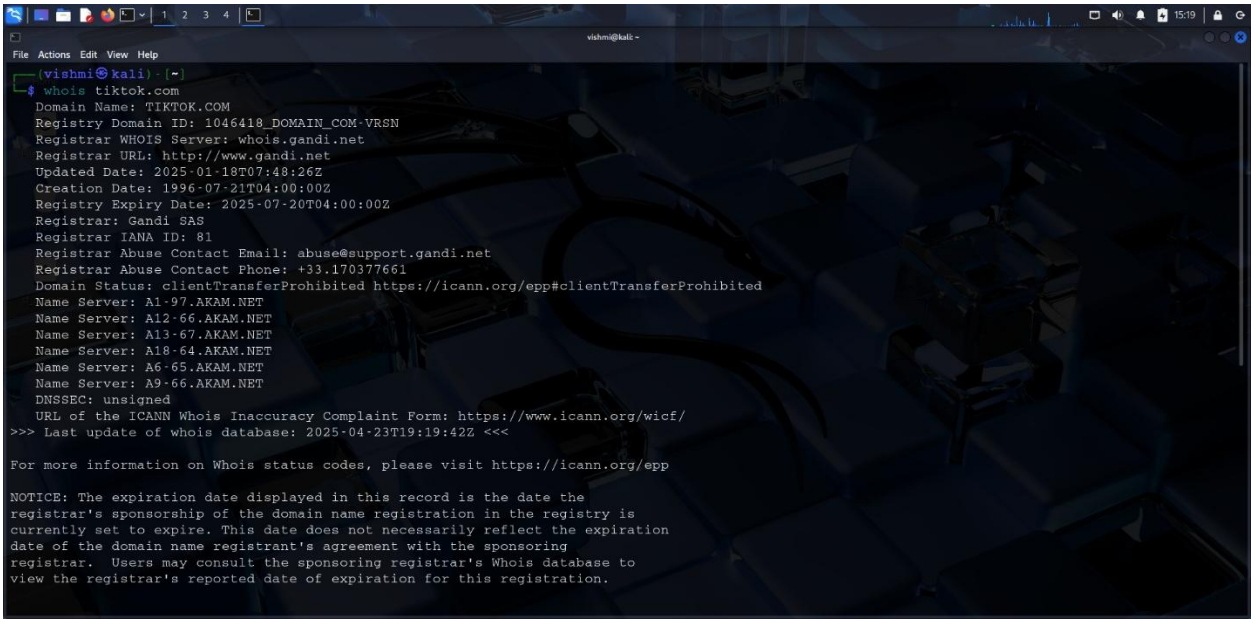
Report-06

Web Audit
tiktok.com

Domain = *tiktok.com*
Sub-domain = *in.tiktok.com*
URL = *https://www.tiktok.com*

Target Reconnaissance

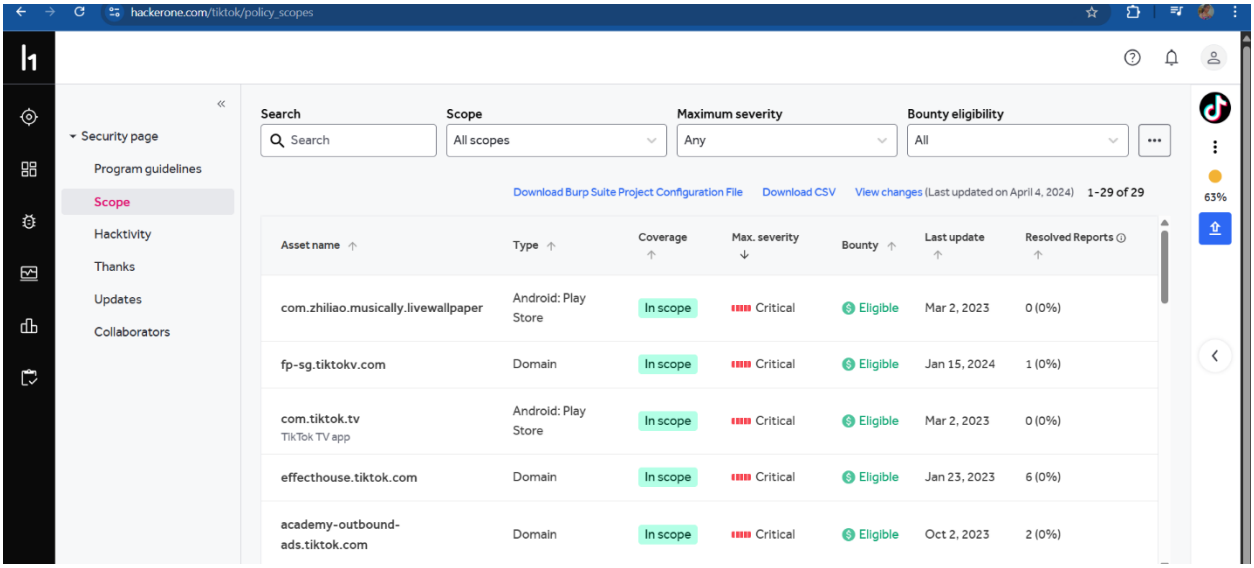
Introduction to Tiktok and Audit Scope

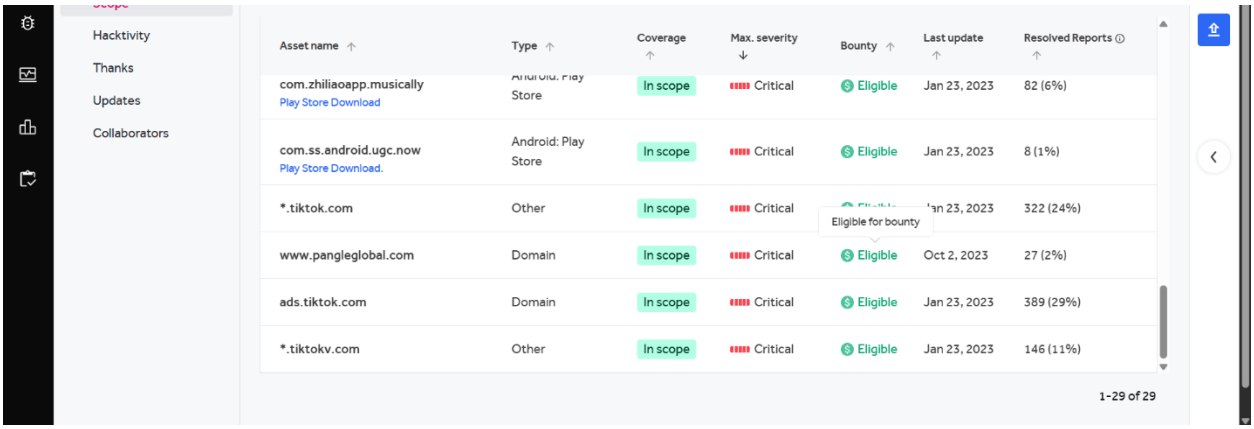


TikTok is a well-known platform for short videos that lets users make, share, and find interesting material with sound effects, music, and visuals. TikTok has grown to be a global center for entertainment, self-expression, and even education because to its viral trends, challenges, and creative community. Anyone can become a content creator there and quickly reach millions of people with everything from comedy skits and dance routines to do-it-yourself advice and life hacks.

These subdomains (and all included) have been approved as legitimate subdomains for testing in the **Hackerone** Bug Bounty program.

Eligible in-scope subdomains for bug bounty program are mentioned below.





Information gathering phase.

The information-gathering phase, often known as reconnaissance or recon, is essential to both assessments of security and cyberattacks. In order to map out the target's structure and determine how it functions, the target of this stage is to gather as much information as possible about it. Because it helps auditors or attackers identify vulnerabilities that could be exploited later on, this fundamental understanding is essential.

There are two main approaches to information gathering

1.Active Scanning :

Involves direct interaction with the target, which can generate noticeable activity and typically uncovers a wealth of details about the system.

2.Passive Scanning :

Seeks to observe the target without direct engagement, resulting in less detectable activity but often providing more limited information

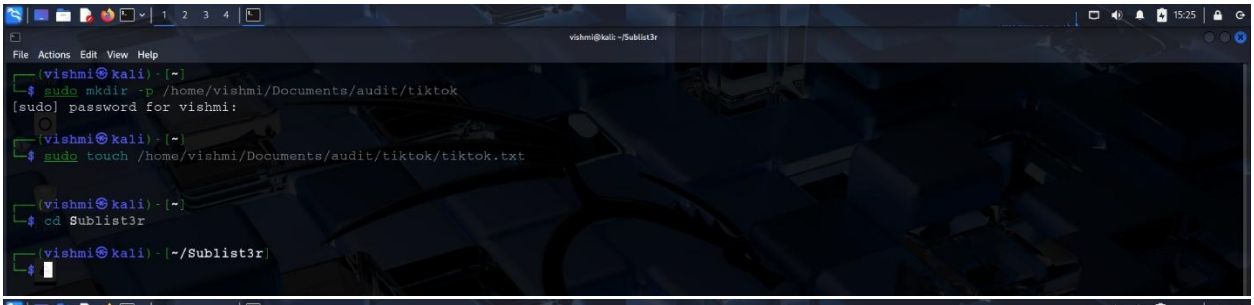
Finding active subdomains and their states

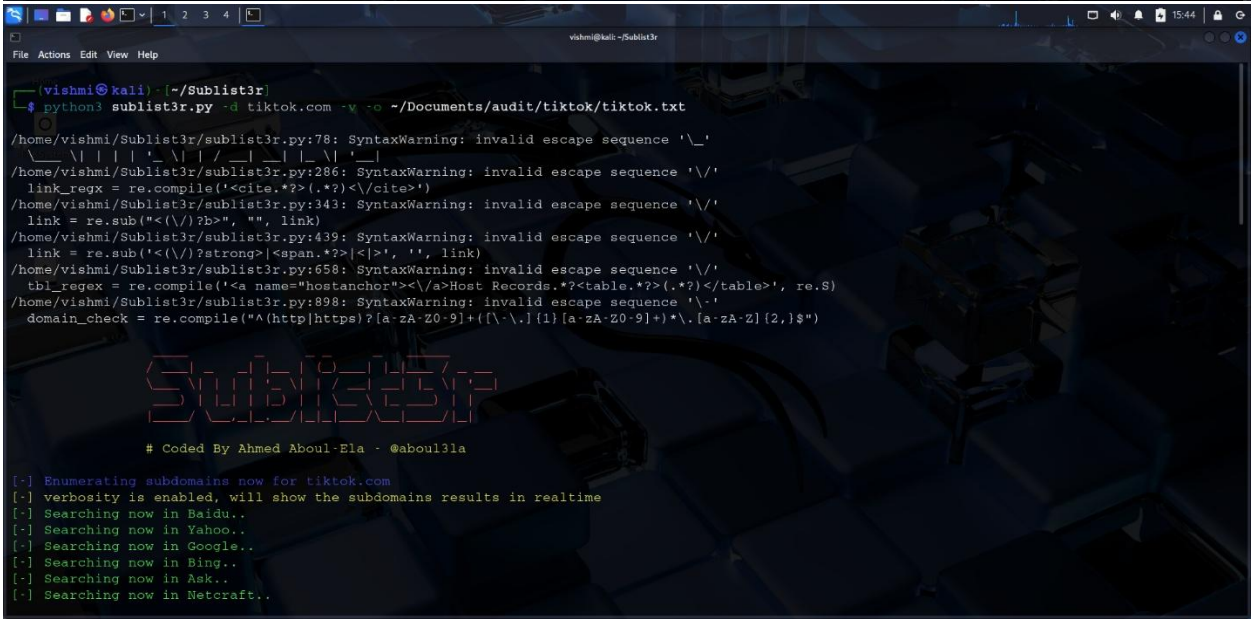
Sublist3r

Sublist3r is an open-source Python application that uses OSINT (Open Source Intelligence) techniques to quickly and effectively scan subdomains. Subdomains linked to a target domain can be found by penetration testers, security researchers, and bug bounty hunters using a variety of search engine queries (including Google, Yahoo, Bing, Baidu, and Ask). Additionally, Sublist3r includes a brute-force module (subbrute) to employ a stronger wordlist to improve the probability of discovering more subdomains.

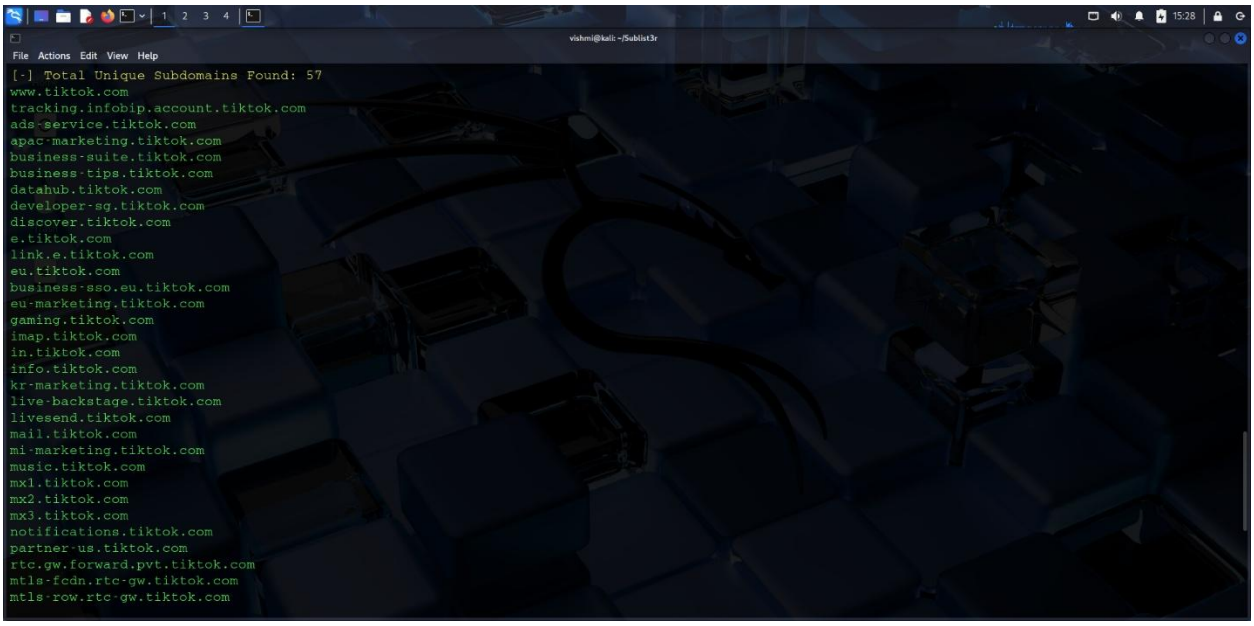
I created a .txt file to store the subdomain headers that were initiated via sublist3r.

Path to .txt file = ***home/vishmi/Documents/audit/tiktok/ tiktok.txt***





I got, these subdomains according to the ***tiktok.com*** domain.

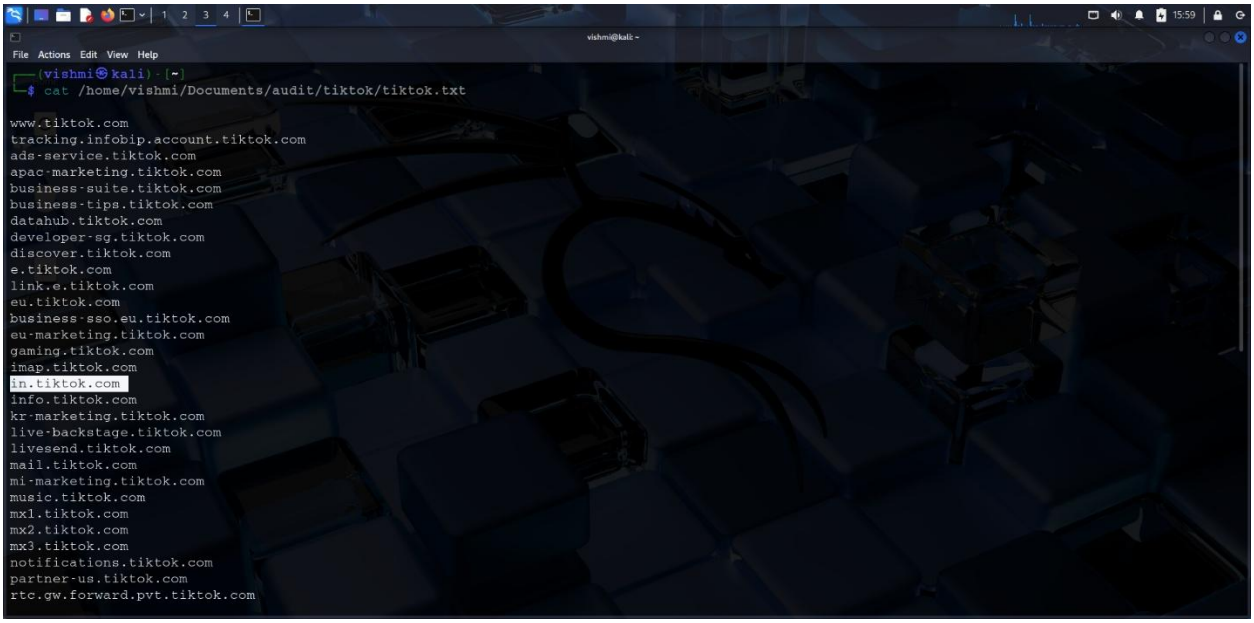


HTTProbe

HTTProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing on achievable goals by providing you with the URLs of active domains.

I am using the text file generated before by the sublist3r and stored the active subdomains to another new .txt file.

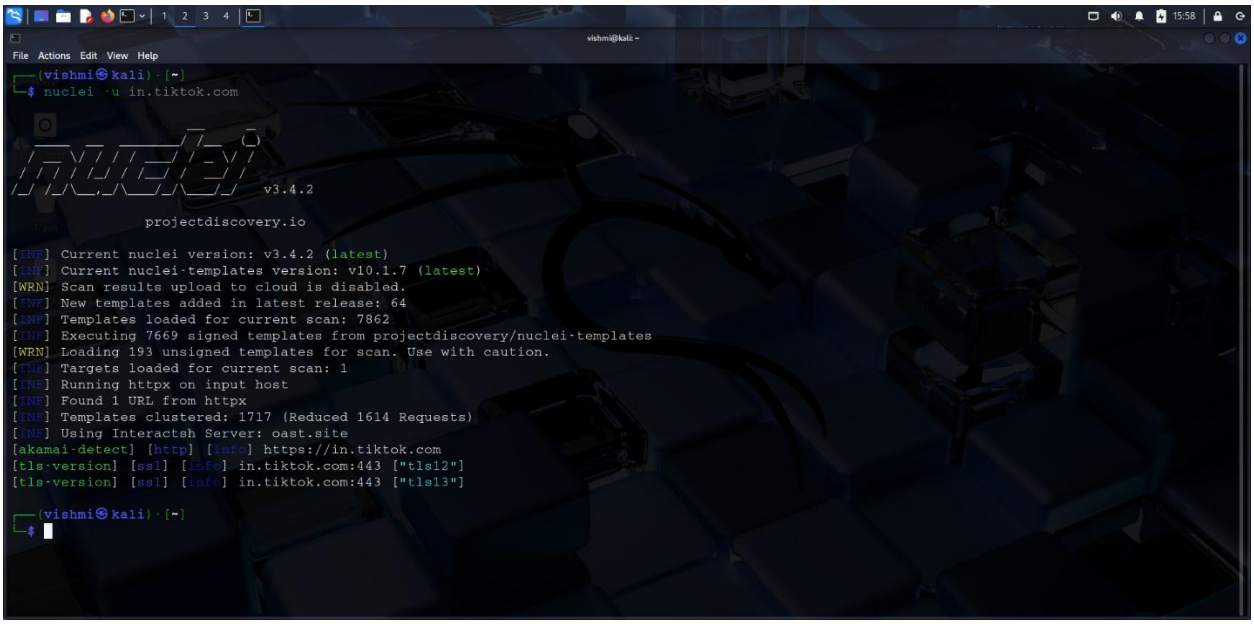
Below, we can see the active subdomains related to the ***tiktok.com*** domain.



To move forward, I chose the active subdomain as **“in.tiktok.com”.**

Nuclei

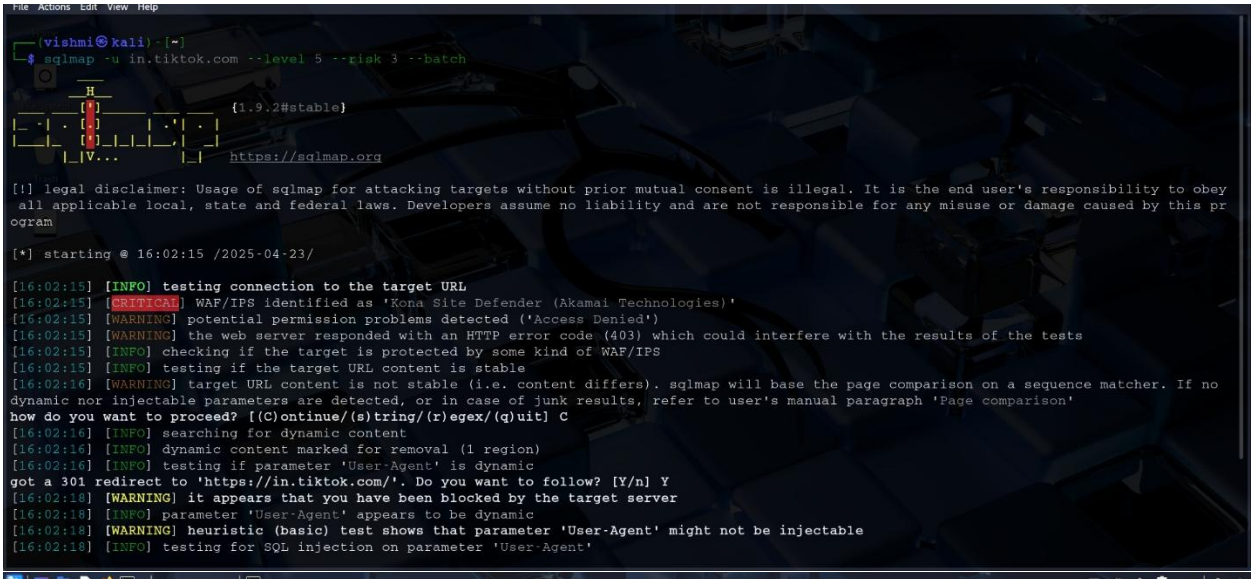
Nuclei is an open-source vulnerability scanner developed by ProjectDiscovery for security professionals, penetration testers, and bug bounty hunters. It uses customizable YAML("Yet Another Markup Language") -based templates to identify vulnerabilities such as misconfigurations, outdated software, and known CVEs (Common Vulnerabilities and Exposures).

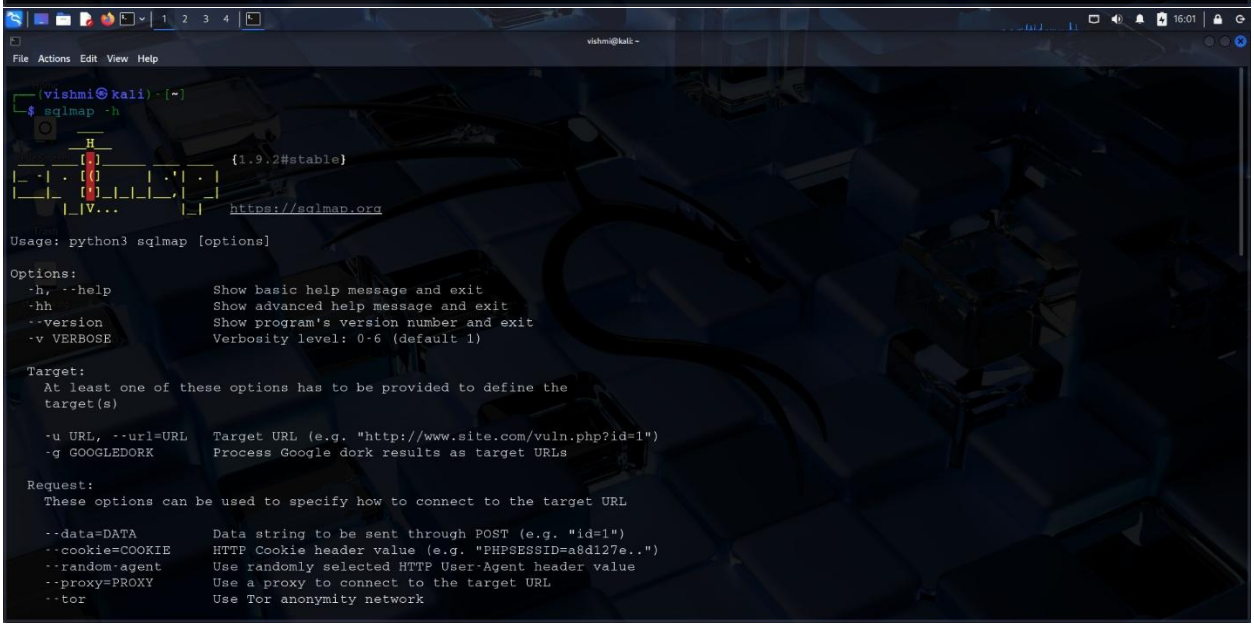


Vulnerability Type	Description	Risk
akamai-detect	Just verifies that the destination website has Akamai protection.	Not a vulnerability; [Information detect]
SSL/TLS Exposure	The scanner successfully initiated connections to tiktok.com over HTTPS port 443, potentially revealing SSL/TLS configuration details.	Low

SQLmap

An open-source penetration testing tool called SQLmap makes it easier to find and take advantage of SQL injection flaws in web apps. If the database permits, it can even access the underlying file system or run commands on the server in addition to identifying the type of database and extracting data. Security experts frequently use it to evaluate and protect web apps from SQL injection attacks.





Option	Meaning
-u	For basic testing, the target URL is required.
--level5	Increases the number of payloads and tests that are done (maximum is 5).
--risk3	Increase the danger level of the payloads used (maximum is 3)
--batch	Executes SQLMap in a non-interactive mode, selecting default responses automatically.

Detected Information

* ***[WARNING] heuristic (basic) test shows that parameter 'User-Agent' might be injectable***

[This is a *potential* vulnerability, but not confirmed.]

* ***[INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'***

[SQLmap is still in the process of testing for SQL injection using Boolean-based techniques.]

**** [CRITICAL] WAF/IPS identified as 'Kona Site Defender (Akamai Technologies)***

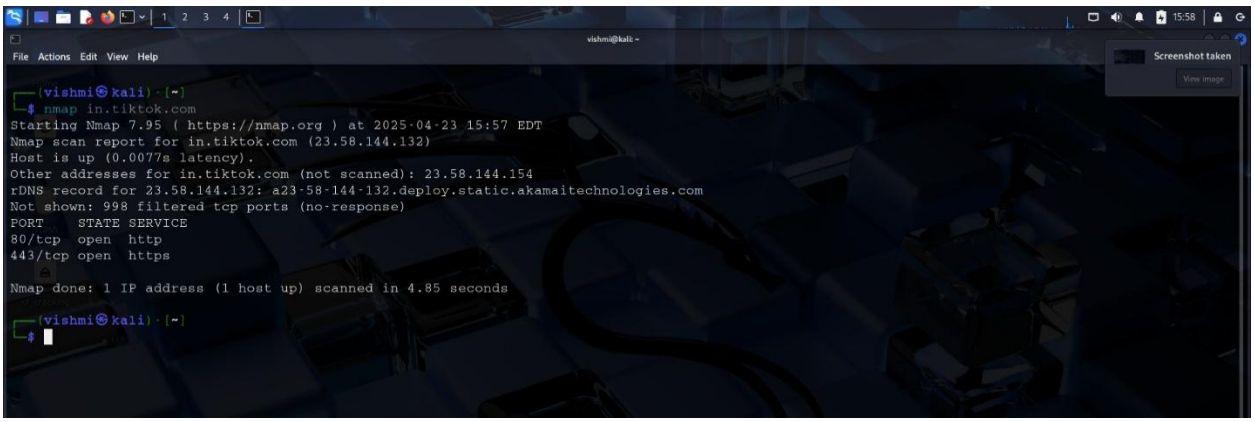
**** [WARNING] potential permission problems detected***

**** [WARNING] target URL content is not stable***

Searching for vulnerabilities

Nmap

Nmap (Network Mapper) is a strong, open-source network scanning program that uses packet transmission and response analysis to find hosts and services on a computer network. To find open ports, running services, operating systems, and active devices on a network, network managers and security experts utilize Nmap. Network inventory, vulnerability assessment, security auditing, and penetration testing are among its many uses.



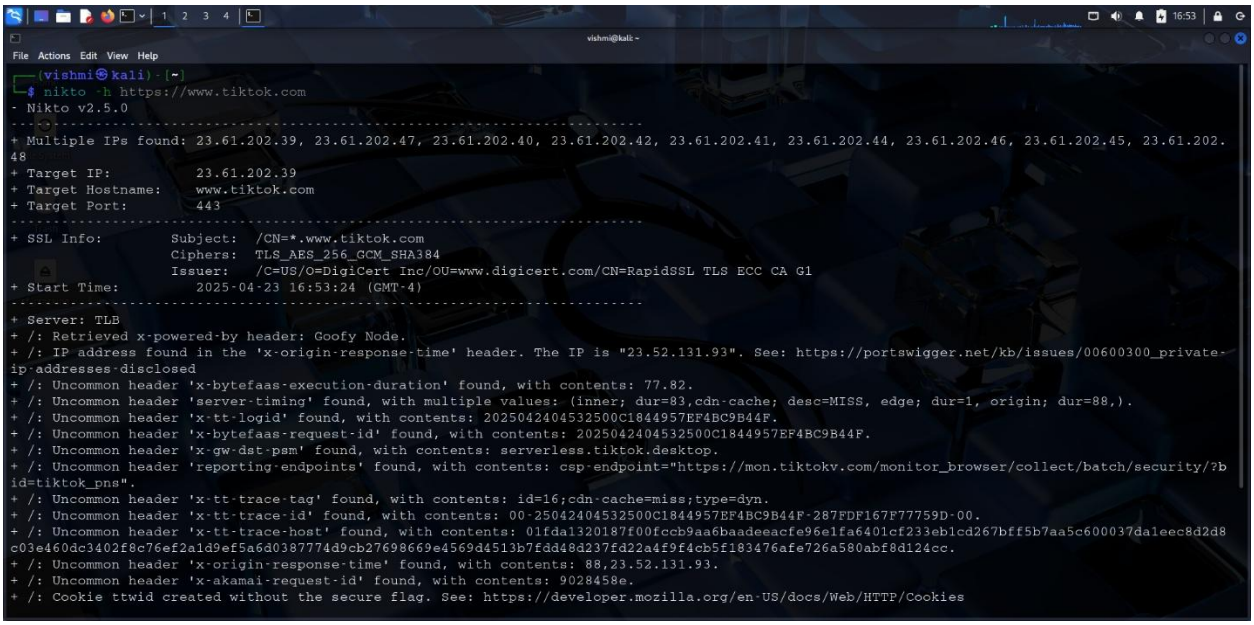
I discovered these details by using Nmap to search *in.tiktok.com.*

PORT	**STATE**	**SERVICE**
80/tcp	open	http
443/tcp	open	https

PORT	**SERVICE**	**VULNERABILITY**
80/tcp	http	Transmits plain text data.
443/tcp	https	Deprecated TLS versions are supported.

Nikto

An open-source program called Nikto scans web servers for common vulnerabilities, malicious files, outdated software, and improperly configured settings, among other potential security issues. It is widely used for penetration testing and assessments, but it functions best when combined with other tools.



Security issues found on ***https://www.tiktok.com's*** by Nikto Scan.

*Uncommon header 'x-bytefaas-execution-duration' found.

*Uncommon header 'x-tt-logid' found, with contents.

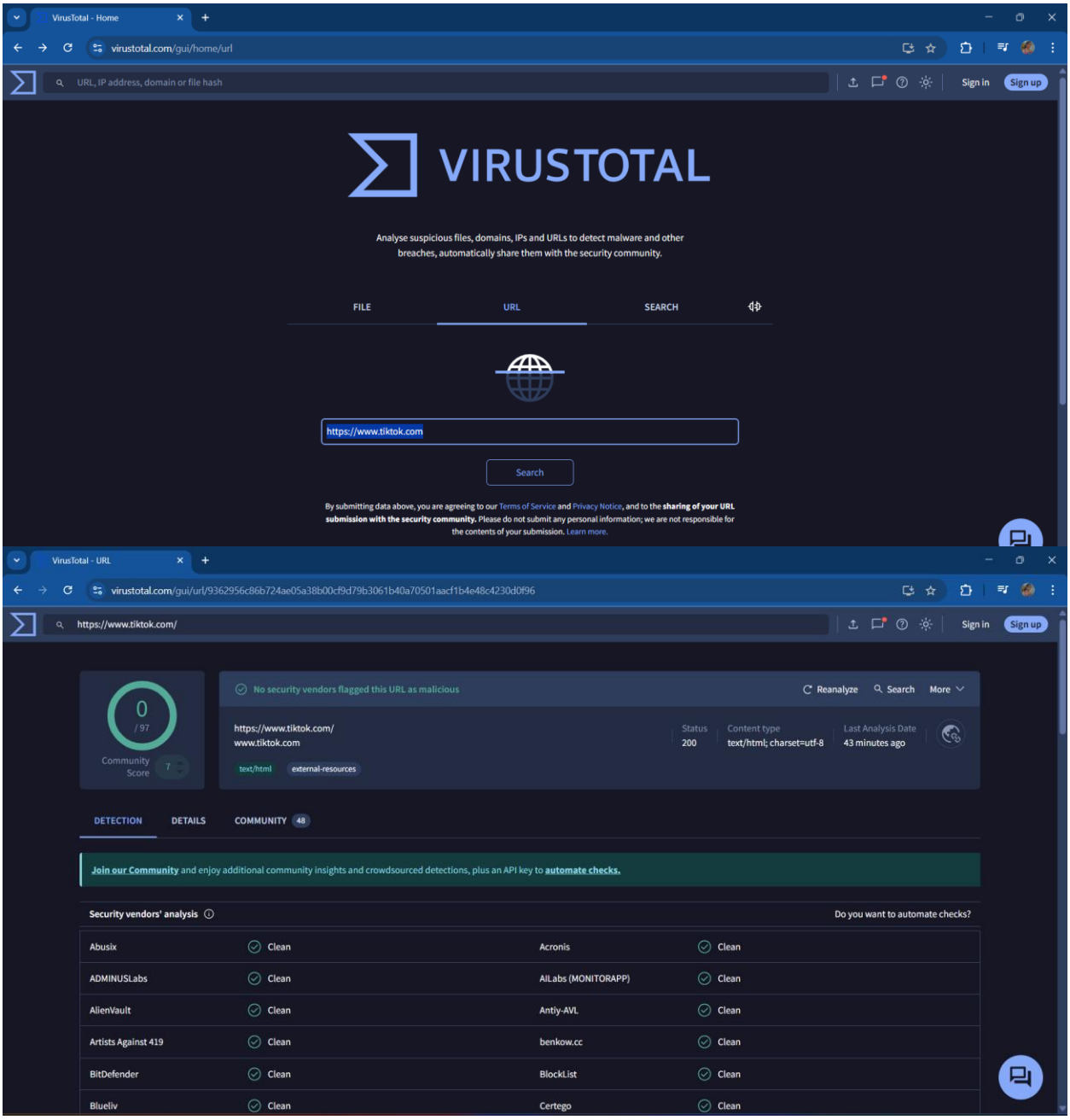
*Uncommon header 'x-bytefaas-request-id' found, with contents.

*Uncommon header 'x-origin-response-time' found

*Uncommon header 'x-akamai-request-id' found,

Virustotal

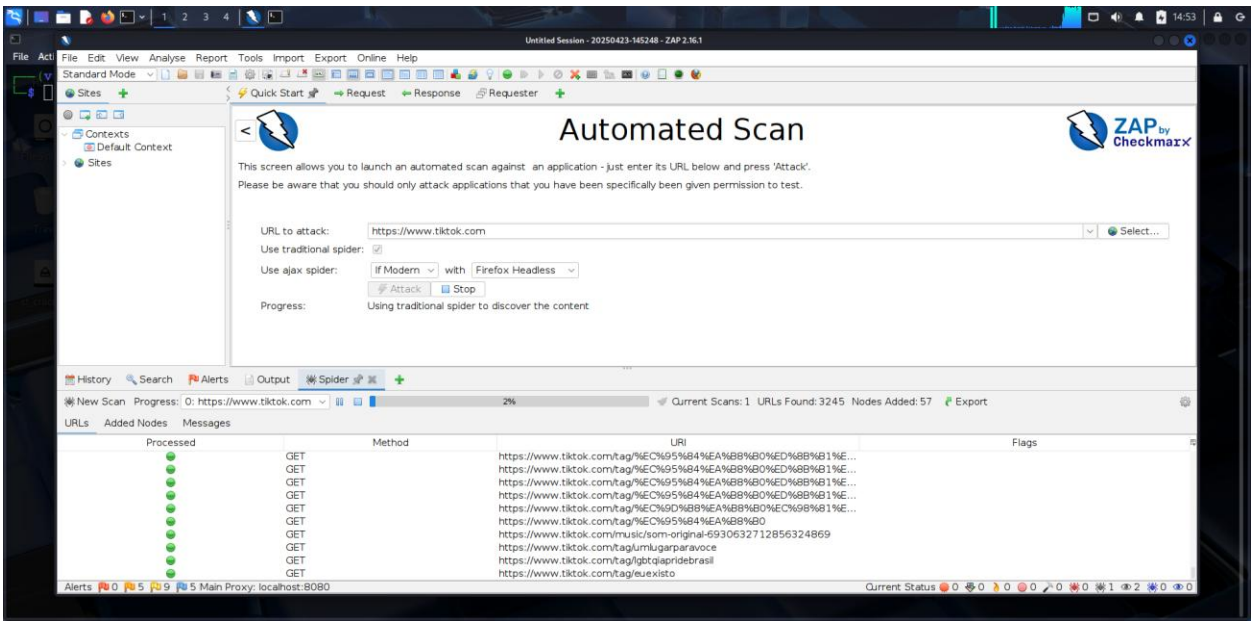
Virustotal is a free web service called VirusTotal employs 70 antivirus engines and URL blocklisting services to scan files and URLs for malware, adware, and other malicious content.
I entered https://www.tiktok.com in URL section .



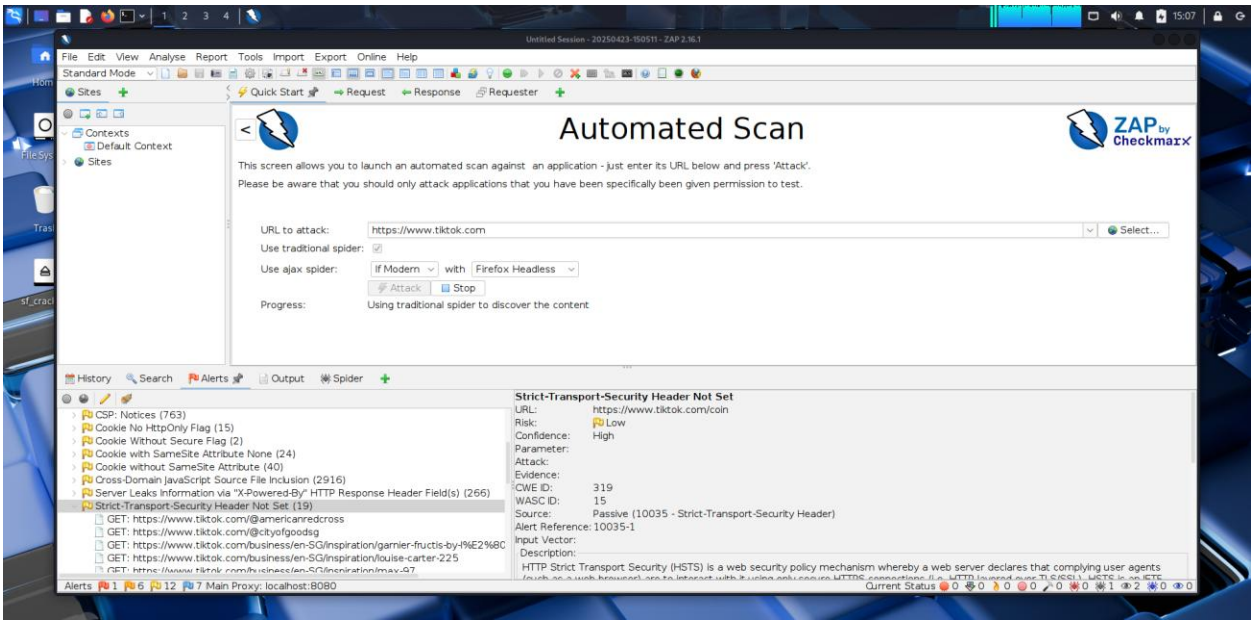
OWASP ZAP

A free and open-source security tool called ***OWASP ZAP (Zed Attack Proxy)*** simulates attacks and examines how an application behaves when it is running to help in discovering and fixing vulnerabilities in web applications.

In here, I entered the target URL [***https://www. tiktok.com***] designated textbox, simply select "Attack" to initiate the scanning process.



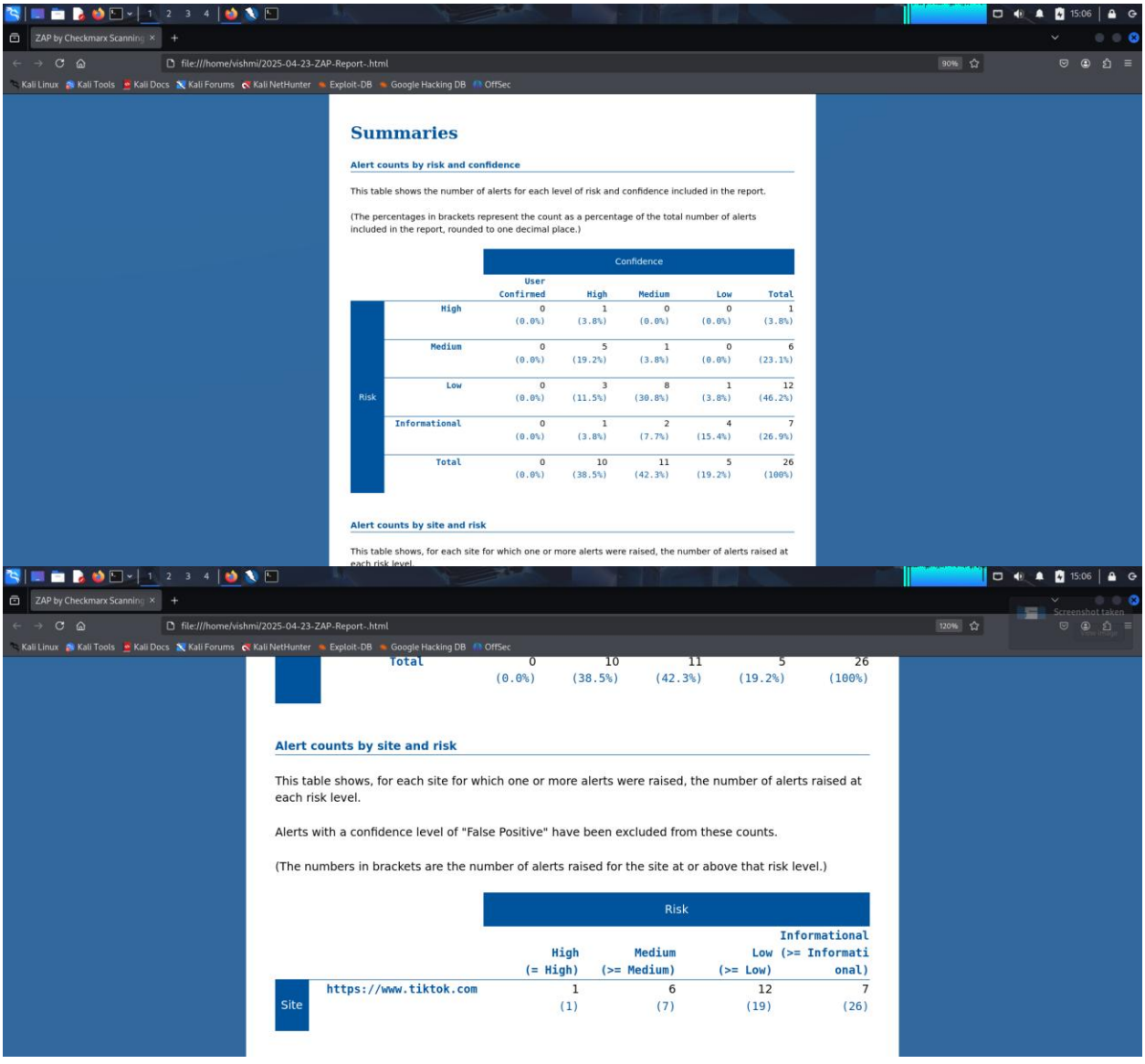
As next step, I entered to the Alerts tab. Here it's detected a vulnerability.



After finishing, it is possible to obtain a thorough report of the results by choosing "Report." The results of scanning many domains are displayed in the screenshots below.

Report = file:///home/vishmi/2025-04-23-ZAP-Report-.html

Please take note that these vulnerabilities have been rated using the OWASP risk rating methodology, which is available at this link.[*OWASP Risk Rating Methodology*]



Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	1 (3.8%)	0 (0.0%)	0 (0.0%)	1 (3.8%)
	Medium	0 (0.0%)	5 (19.2%)	1 (3.8%)	0 (0.0%)	6 (23.1%)
	Low	0 (0.0%)	3 (11.5%)	8 (30.8%)	1 (3.8%)	12 (46.2%)
	Informational	0 (0.0%)	1 (3.8%)	2 (7.7%)	4 (15.4%)	7 (26.9%)
	Total	0 (0.0%)	10 (38.5%)	11 (42.3%)	5 (19.2%)	26 (100%)

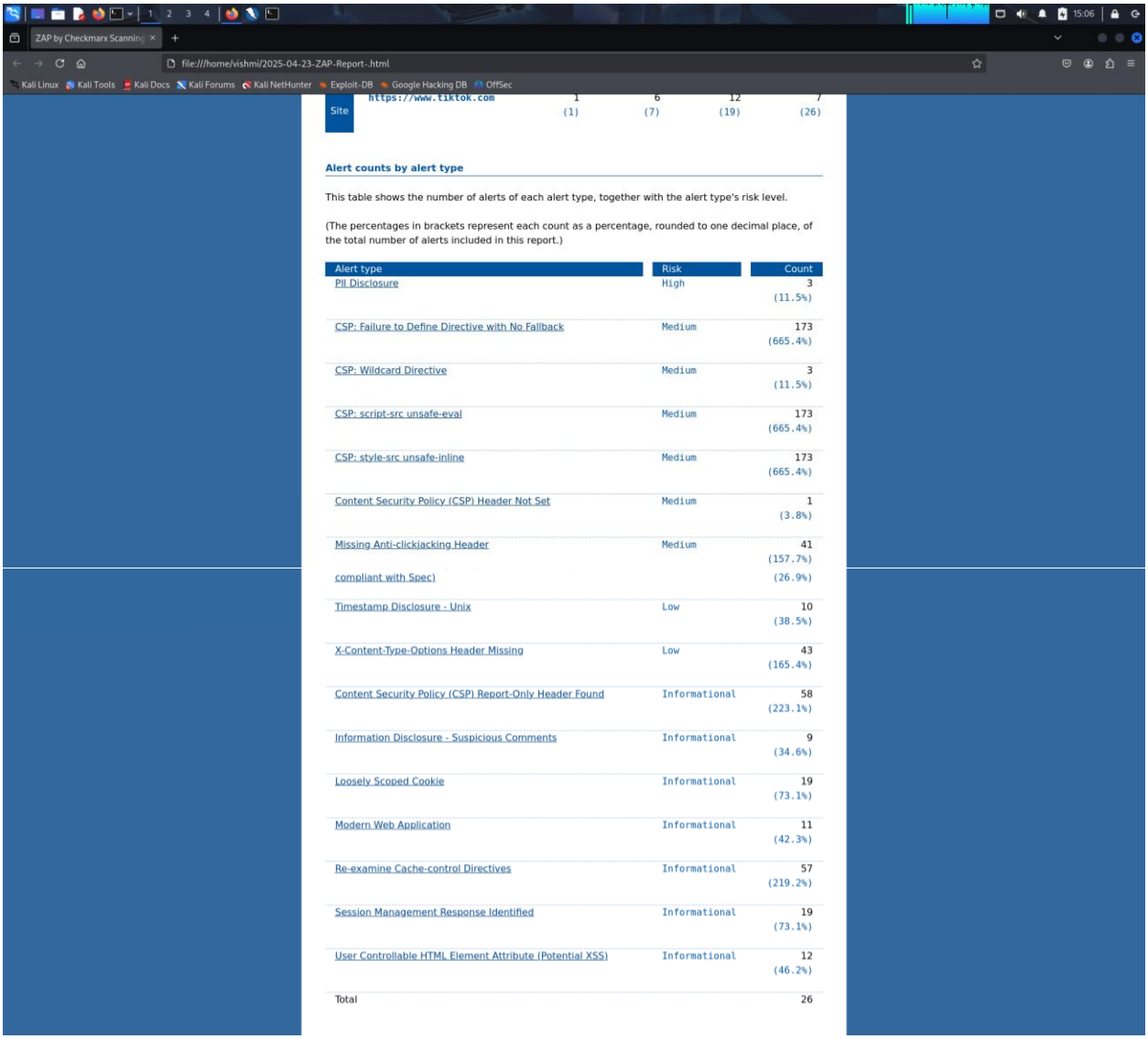
Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://www.tiktok.com	1 (1)	6 (7)	12 (19)	7 (26)


ZAP by Checkmarx Scanning
file:///home/vishmi/2025-04-23-ZAP-Report-.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Site
https://www.tiktok.com
1 (1)
6 (7)
12 (19)
7 (26)
Alert counts by alert type
This table shows the number of alerts of each alert type, together with the alert type's risk level.
(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)
Alert type
Risk
Count
PII Disclosure
High
3 (11.5%)
CSP: Failure to Define Directive with No Fallback
Medium
173 (665.4%)
CSP: Wildcard Directive
Medium
3 (11.5%)
CSP: script-src unsafe-eval
Medium
173 (665.4%)
CSP: style-src unsafe-inline
Medium
173 (665.4%)
Content Security Policy (CSP) Header Not Set
Medium
1 (3.8%)
Missing Anti-clickjacking Header
Medium
41 (157.7%)
compliant with Spec)
(26.9%)
Timestamp Disclosure - Unix
Low
10 (38.5%)
X-Content-Type-Options Header Missing
Low
43 (165.4%)
Content Security Policy (CSP) Report-Only Header Found
Informational
58 (223.1%)
Information Disclosure - Suspicious Comments
Informational
9 (34.6%)
Loosely Scoped Cookie
Informational
19 (73.1%)
Modern Web Application
Informational
11 (42.3%)
Re-examine Cache-control Directives
Informational
57 (219.2%)
Session Management Response Identified
Informational
19 (73.1%)
User Controllable HTML Element Attribute (Potential XSS)
Informational
12 (46.2%)
Total
26

Vulnerabilities

a.Vulnerability Title	**Strict-Transport-Security Header Not Set**
b.Vulnerability Description	The target server's HTTP response headers lack the Strict-Transport-Security (HSTS) header, exposing the website to Man-in-the-Middle (MITM) attacks due to unencrypted communication.
c.Affected Components	Web server configuration, specifically the HTTP response headers.
d.Impact Assessment	Users may unknowingly connect to a website via HTTP, potentially exposing sensitive data to interception.
e.Steps to Reproduce	1. Try connecting to the target website with http:// rather than https:// by opening a browser. 2. Note that HTTPS is not immediately updated for the connection. 3. Verify that the Strict-Transport-Security header is missing by looking at the HTTP response headers.
f.Proof of Concept (if applicable)	Use a network analysis tool to monitor traffic and establish an HTTP connection to the website, ensuring data transmission is not encrypted and susceptible to interceptions.
g.Proposed Mitigation or Fix	Add the Strict-Transport-Security header to the server to enable the HSTS policy.

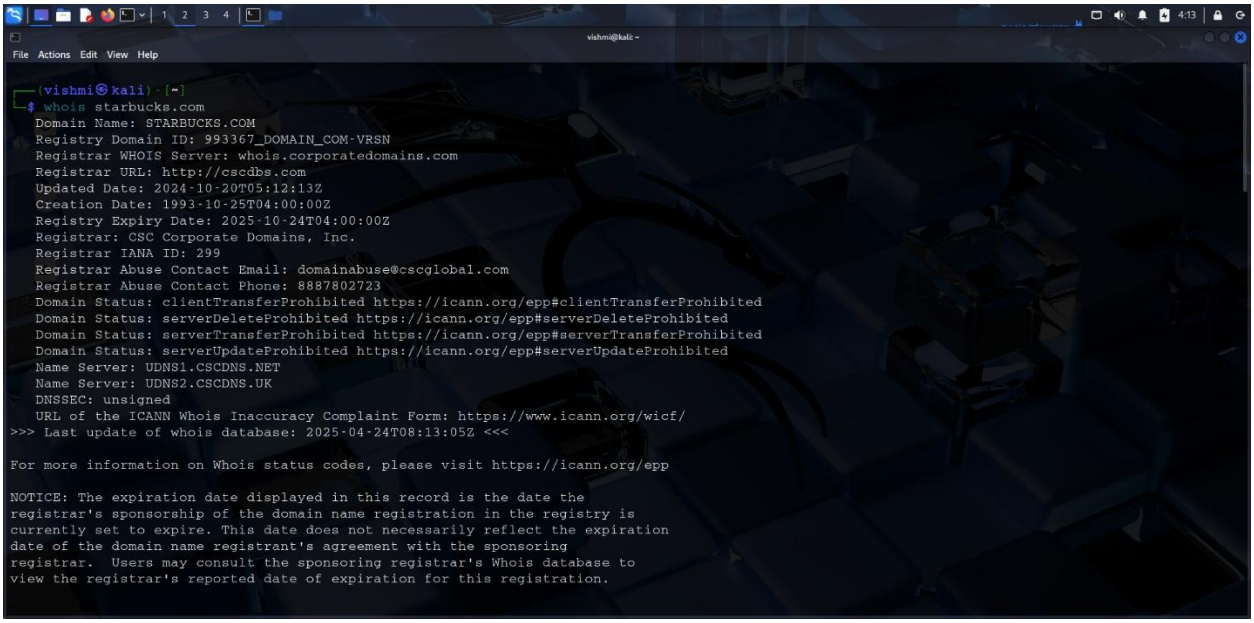
Report-07

Web Audit *starbucks.com*

Domain = *starbucks.com*
Sub-domain = *a.starbucks.com*
URL = *https://www.starbucks.com*

Target Reconnaissance

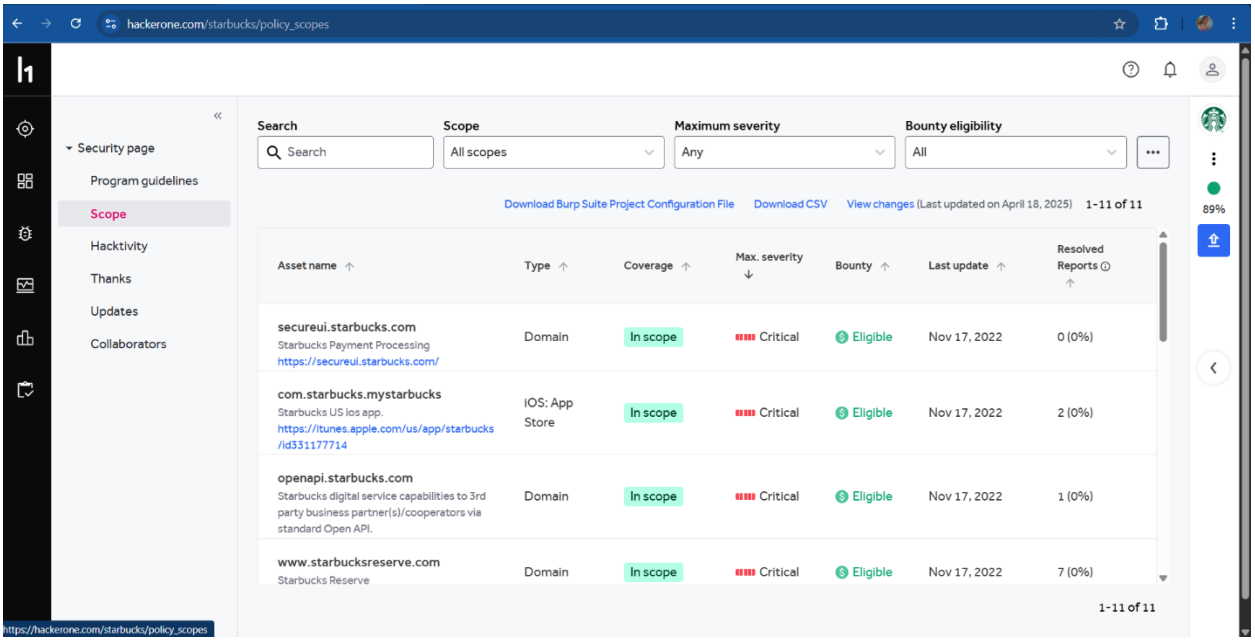
Introduction to Starbucks and Audit Scope

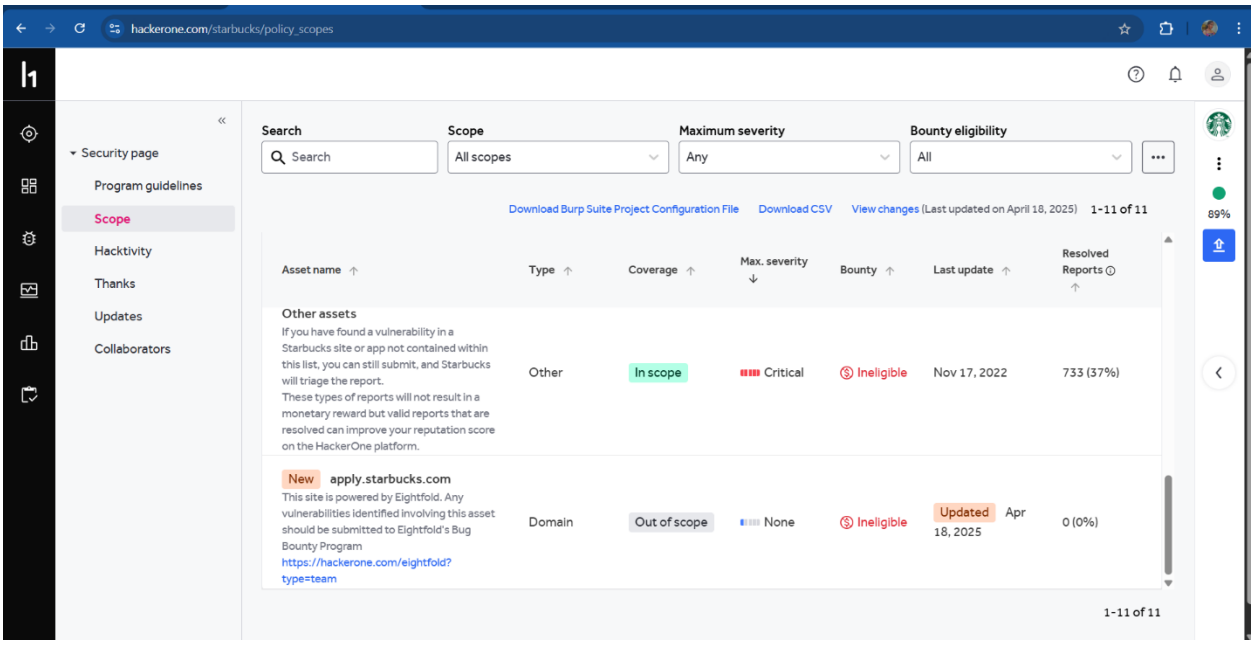


Starbucks is an international chain of coffee shops famous for its high-quality coffee, espresso drinks, and welcoming atmosphere. Since its founding in Seattle in 1971, it has developed into a global icon of coffee culture. Offering a range of drinks, pastries, and snacks, Starbucks has created a welcome area for individuals to rest, work, and interact.

These subdomains (and all included) have been approved as legitimate subdomains for testing in the **Hackerone** Bug Bounty program.

Eligible in-scope subdomains for bug bounty program are mentioned below





Information gathering phase.

The information-gathering phase, often known as reconnaissance or recon, is essential to both assessments of security and cyberattacks. In order to map out the target's structure and determine how it functions, the target of this stage is to gather as much information as possible about it. Because it helps auditors or attackers identify vulnerabilities that could be exploited later on, this fundamental understanding is essential.

There are two main approaches to information gathering

1.Active Scanning :

Involves direct interaction with the target, which can generate noticeable activity and typically uncovers a wealth of details about the system.

2.Passive Scanning :

Seeks to observe the target without direct engagement, resulting in less detectable activity but often providing more limited information

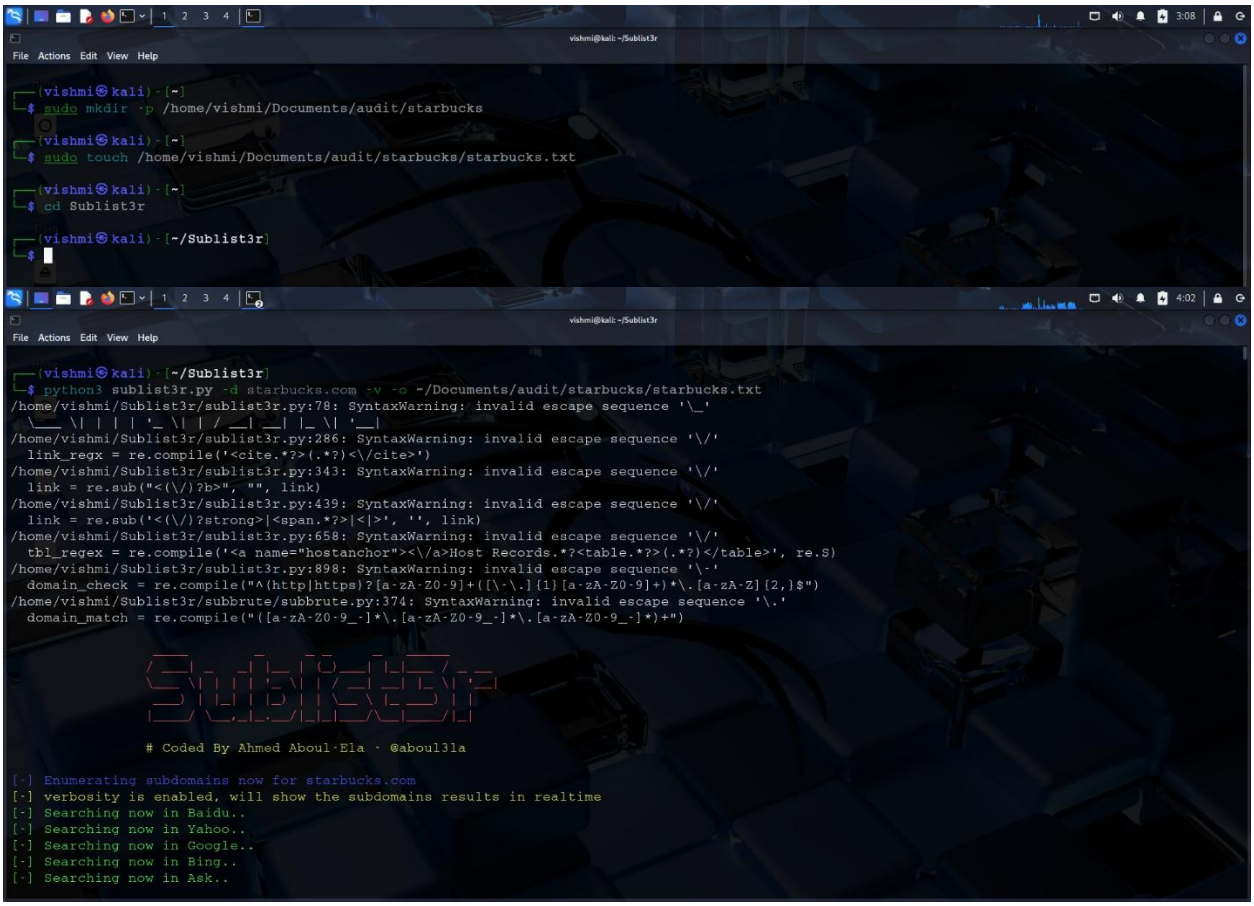
Finding active subdomains and their states

Sublist3r

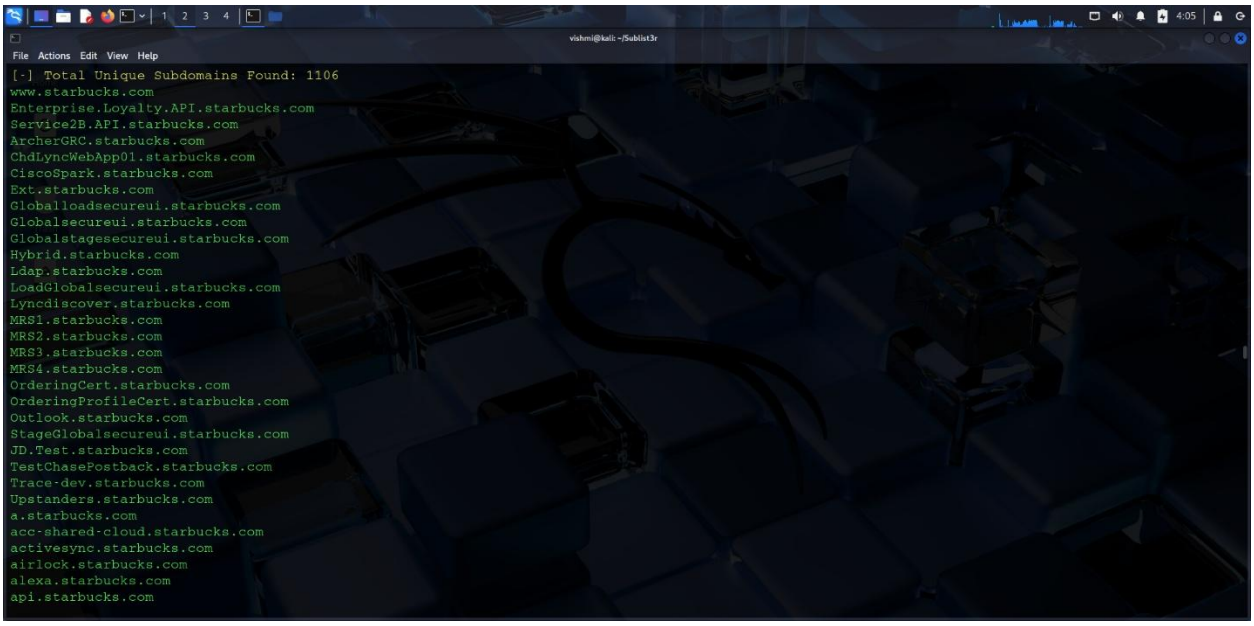
Sublist3r is an open-source Python application that uses OSINT (Open Source Intelligence) techniques to quickly and effectively scan subdomains. Subdomains linked to a target domain can be found by penetration testers, security researchers, and bug bounty hunters using a variety of search engine queries (including Google, Yahoo, Bing, Baidu, and Ask). Additionally, Sublist3r includes a brute-force module (subbrute) to employ a stronger wordlist to improve the probability of discovering more subdomains.

I created a .txt file to store the subdomain headers that were initiated via sublist3r.

Path to .txt file = ***home/vishmi/Documents/audit/starbucks/ starbucks.txt***



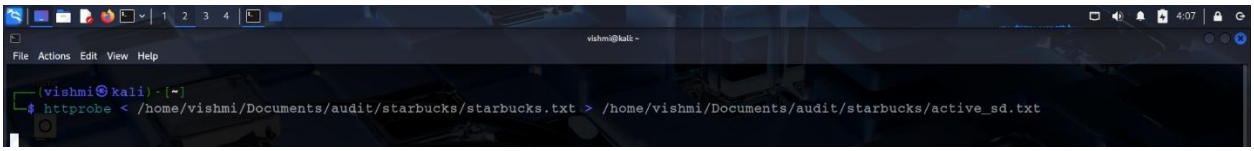
I got, these subdomains according to the ***starbucks.com*** domain.



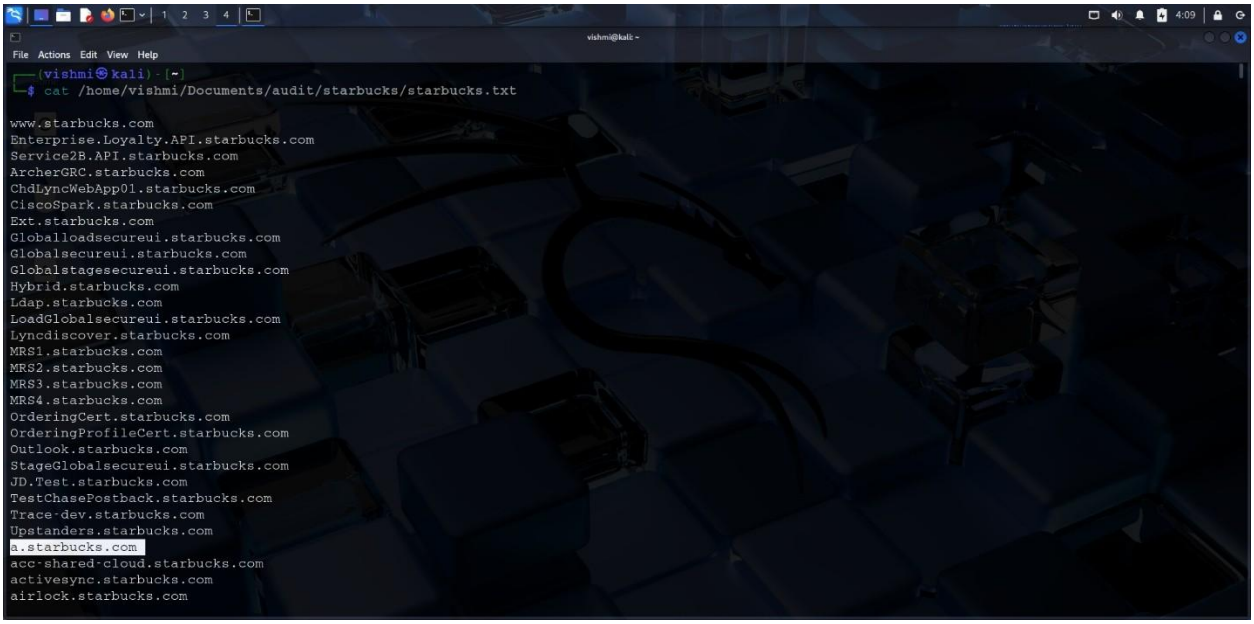
HTTProbe

HTTProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing on achievable goals by providing you with the URLs of active domains.

I am using the text file generated before by the sublist3r and stored the active subdomains to another new .txt file.



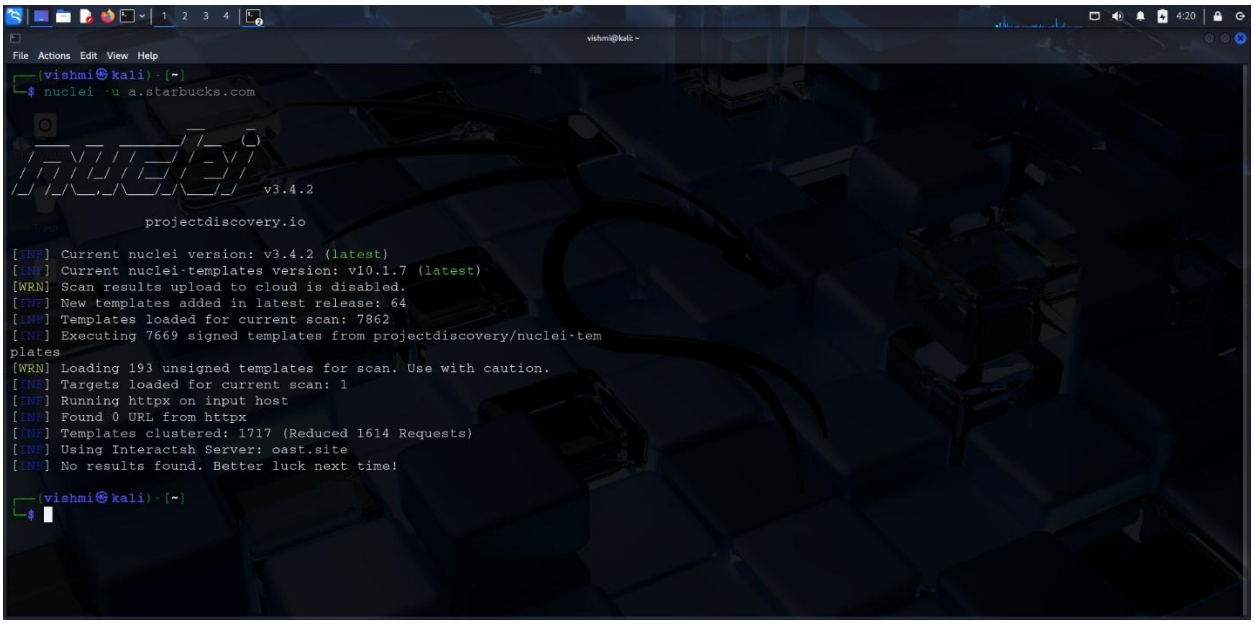
Below, we can see the active subdomains related to the ***starbucks.com*** domain.



To move forward, I chose the active subdomain as **“a.starbucks.com”.**

Nuclei

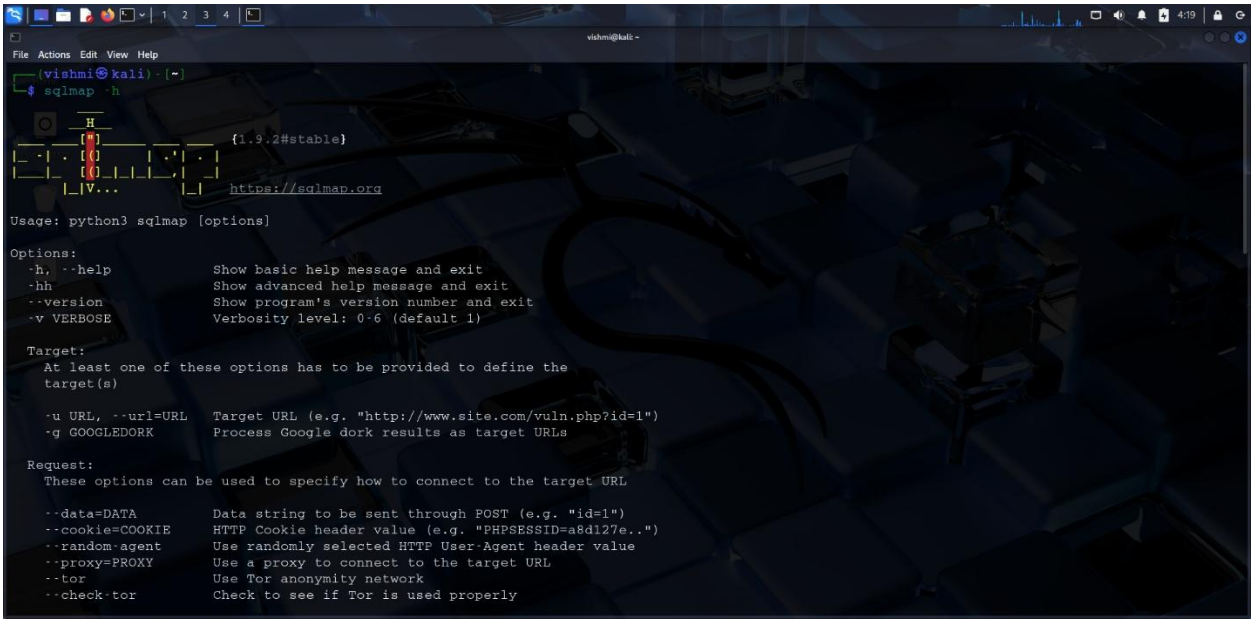
Nuclei is an open-source vulnerability scanner developed by ProjectDiscovery for security professionals, penetration testers, and bug bounty hunters. It uses customizable YAML("Yet Another Markup Language") -based templates to identify vulnerabilities such as misconfigurations, outdated software, and known CVEs (Common Vulnerabilities and Exposures).

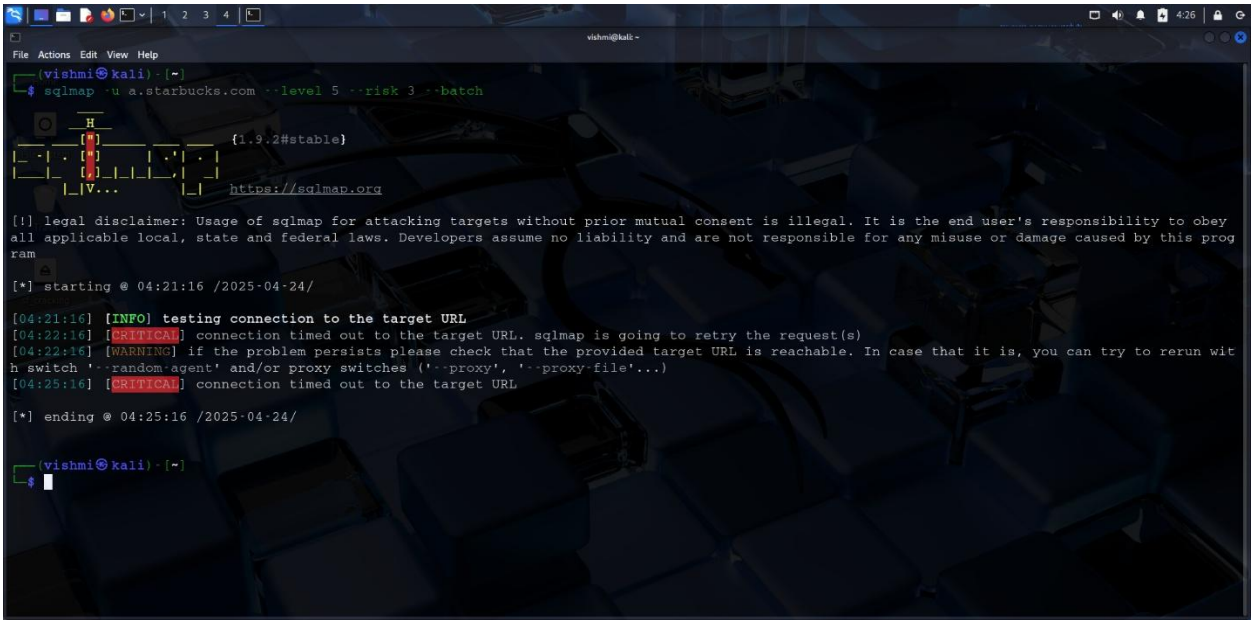


Here, the nuclei scan found no issue.

SQLmap

An open-source penetration testing tool called SQLmap makes it easier to find and take advantage of SQL injection flaws in web apps. If the database permits, it can even access the underlying file system or run commands on the server in addition to identifying the type of database and extracting data. Security experts frequently use it to evaluate and protect web apps from SQL injection attacks.





Option	Meaning
-u	For basic testing, the target URL is required.
--level5	Increases the number of payloads and tests that are done (maximum is 5).
--risk3	Increase the danger level of the payloads used (maximum is 3)
--batch	Executes SQLMap in a non-interactive mode, selecting default responses automatically.

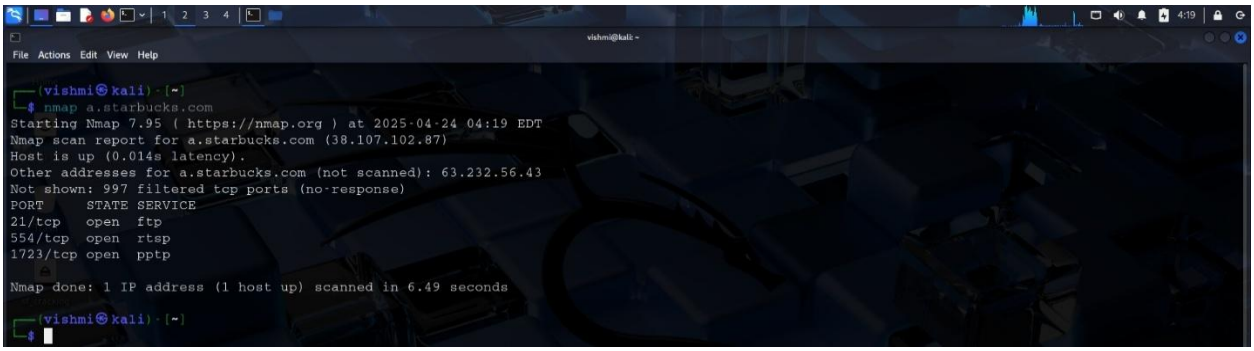
Detected Information

**** [CRITICAL] connection timed out to the target URL.*** – It's not a vulnerability.

Searching for vulnerabilities

Nmap

Nmap (Network Mapper) is a strong, open-source network scanning program that uses packet transmission and response analysis to find hosts and services on a computer network. To find open ports, running services, operating systems, and active devices on a network, network managers and security experts utilize Nmap. Network inventory, vulnerability assessment, security auditing, and penetration testing are among its many uses.



I discovered these details by using Nmap to search *a.starbucks.com.*

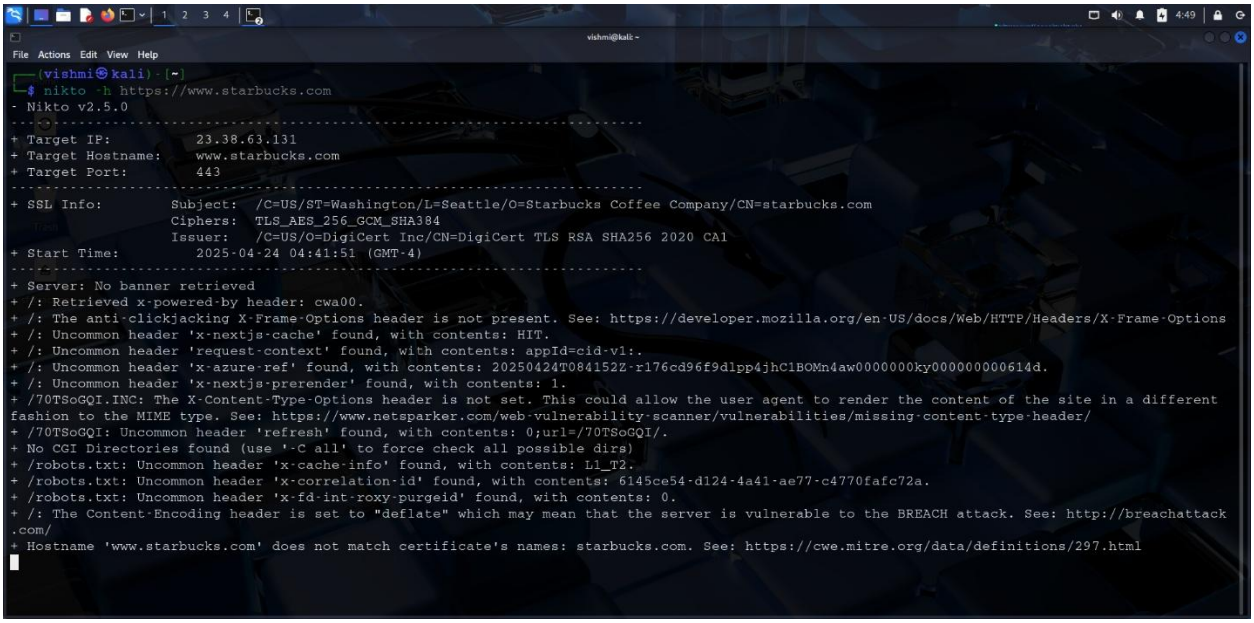
PORT	STATE	SERVICE
21/tcp	open	ftp
554/tcp	open	rtsp
1723/tcp	open	pptp

PORT	SERVICE	Vulnerabilities
21/tcp	ftp	Unencrypted credentials are accepted.
554/tcp	Rtsp	Usually doesn't have authenticity.
1723/tcp	pptp	Makes use of a weak encryption

Nikto

An open-source program called Nikto scans web servers for common vulnerabilities, malicious files, outdated software, and improperly configured settings, among other potential security issues. It is widely used for penetration testing and assessments, but it functions best when combined with other tools

.



Security issues found on ***https://www.starbucks.com's*** by Nikto Scan

* The anti-clickjacking X-Frame-Options header is not present.

* Uncommon header 'x-nextjs-cache' found, with contents.

* The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack.

* No CGI Directories found.

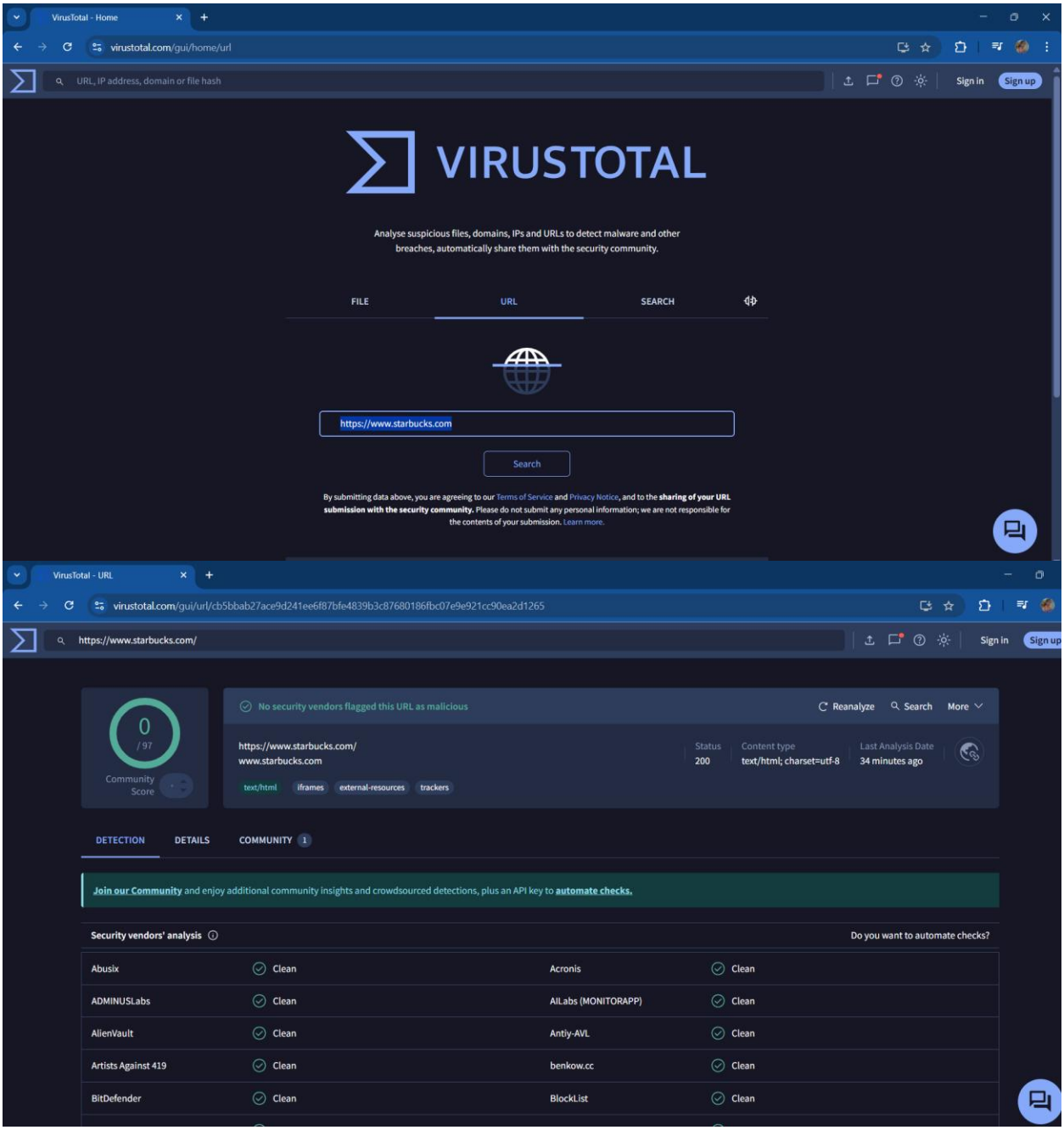
* X-Content-Type-Options header is not set.

*Uncommon header 'x-fd-int-roxy-purgeid' found, with contents: 0.

Virustotal

Virustotal is a free web service called VirusTotal employs 70 antivirus engines and URL blocklisting services to scan files and URLs for malware, adware, and other malicious content.

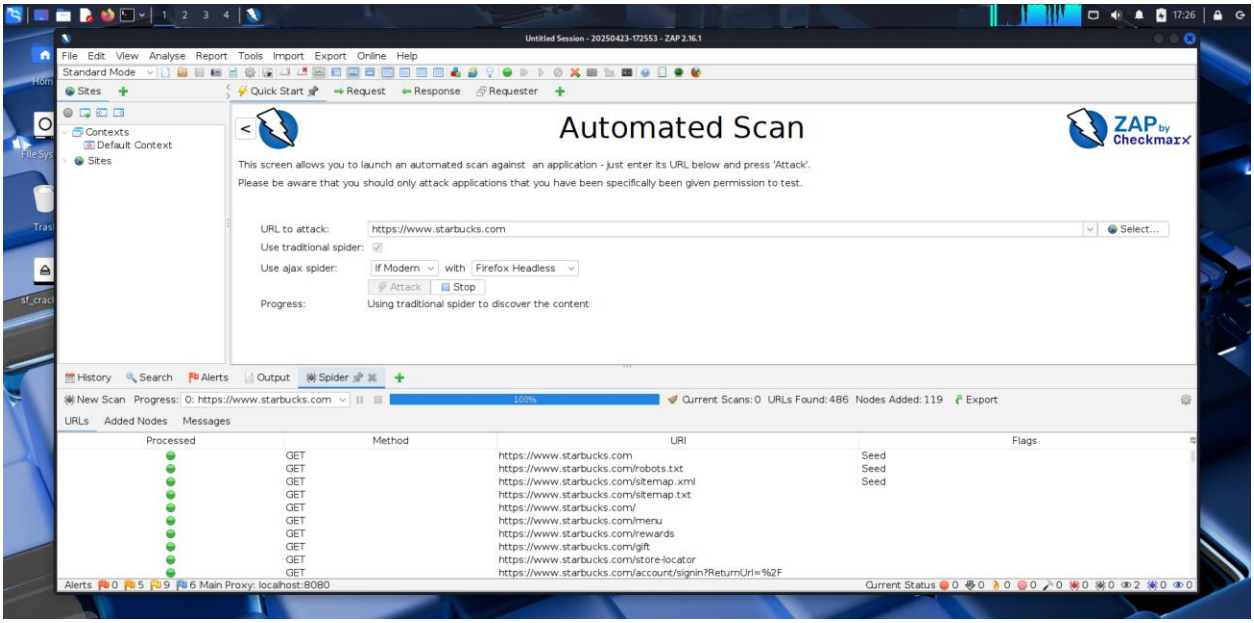
I entered https://www.starbucks.com in URL section .



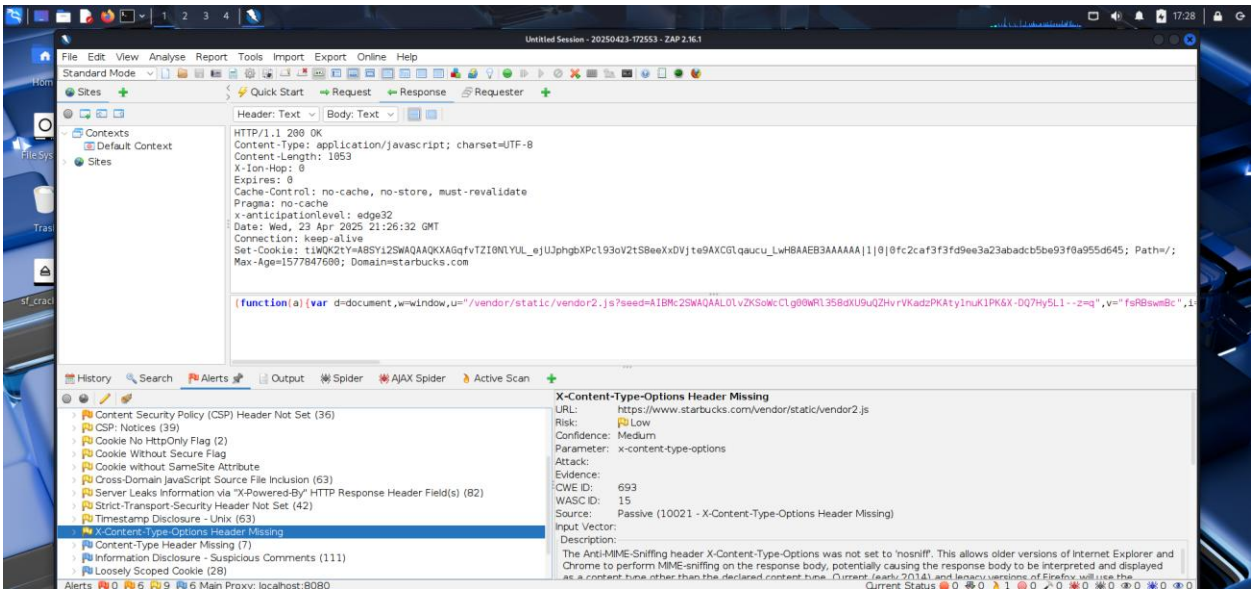
OWASP ZAP

A free and open-source security tool called ***OWASP ZAP (Zed Attack Proxy)*** simulates attacks and examines how an application behaves when it is running to help in discovering and fixing vulnerabilities in web applications.

In here, I entered the target URL [***https://www.starbucks.com***] designated textbox, simply select "Attack" to initiate the scanning process.



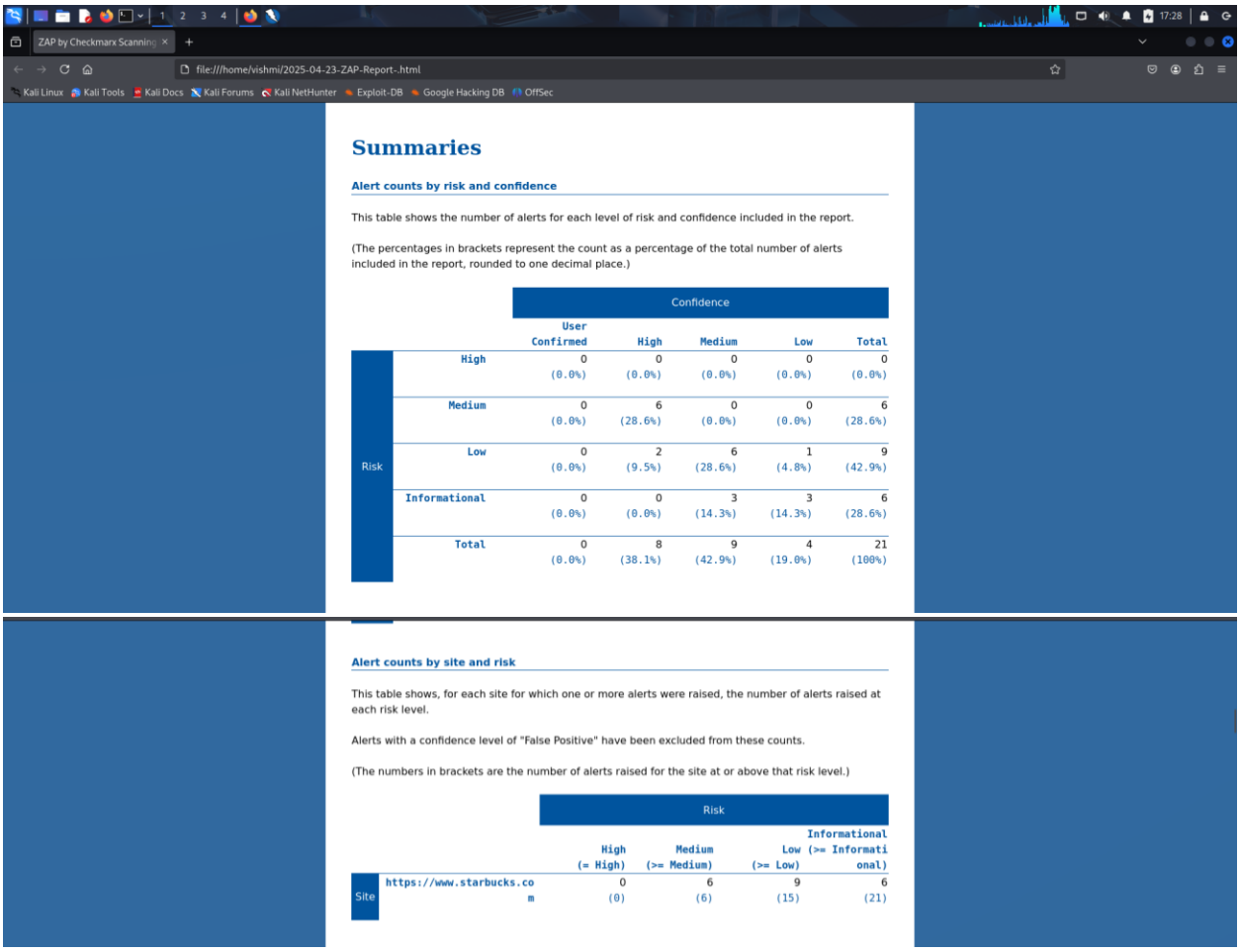
As next step, I entered to the Alerts tab. Here it's detected a vulnerability.



After finishing, it is possible to obtain a thorough report of the results by choosing "Report." The results of scanning many domains are displayed in the screenshots below.

Report = *file:///home/vishmi/2025-04-23-ZAP-Report-.html*

Please take note that these vulnerabilities have been rated using the OWASP risk rating methodology, which is available at this link.[*OWASP Risk Rating Methodology*]



Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	6 (28.6%)	0 (0.0%)	0 (0.0%)	6 (28.6%)
	Low	0 (0.0%)	2 (9.5%)	6 (28.6%)	1 (4.8%)	9 (42.9%)
	Informational	0 (0.0%)	0 (0.0%)	3 (14.3%)	3 (14.3%)	6 (28.6%)
	Total	0 (0.0%)	8 (38.1%)	9 (42.9%)	4 (19.0%)	21 (100%)

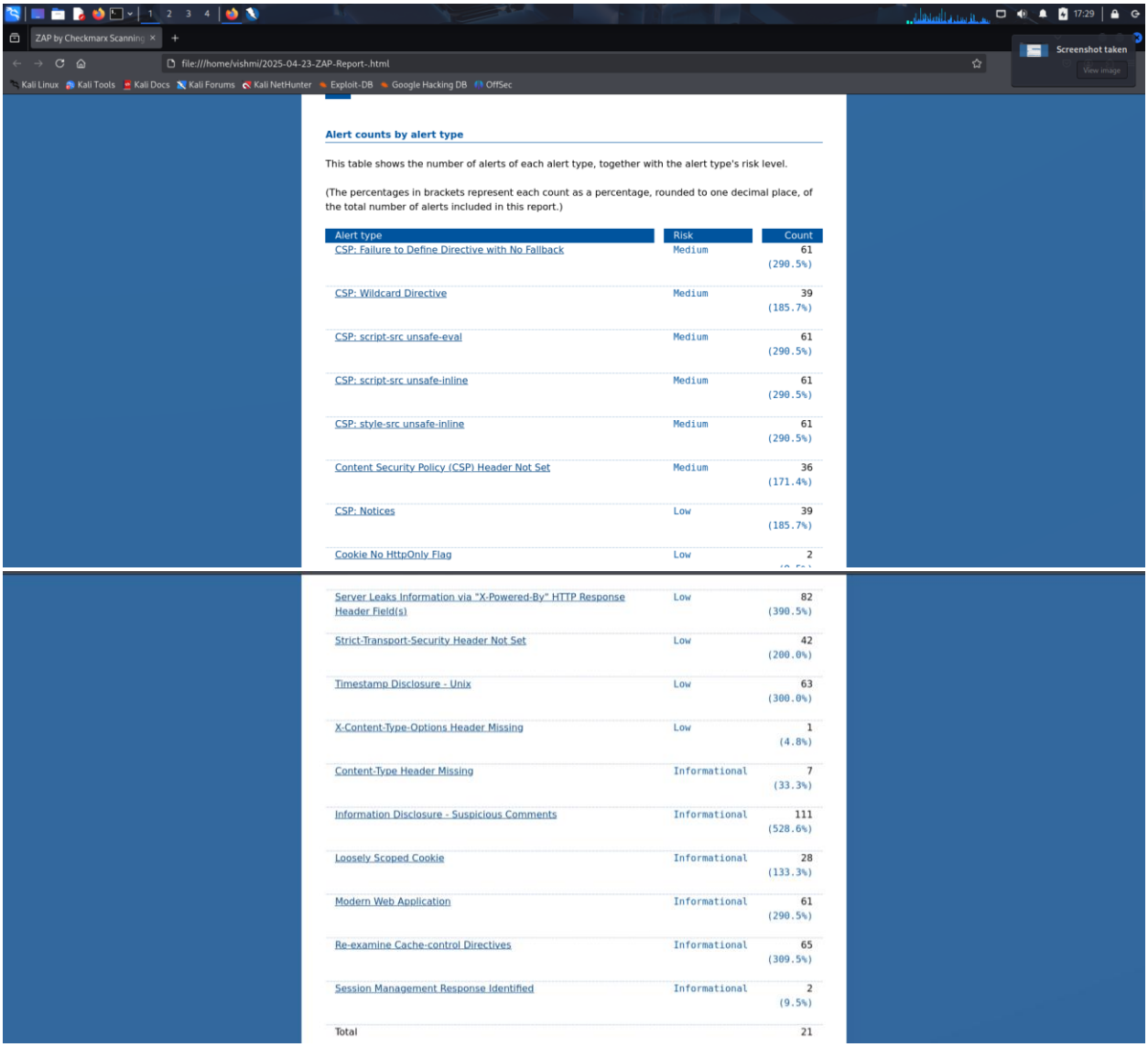
Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://www.starbucks.com	0 (0)	6 (6)	9 (15)	6 (21)


ZAP by Checkmarx Scanning
file:///home/vishmi/2025-04-23-ZAP-Report-.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Screenshot taken
Alert counts by alert type
This table shows the number of alerts of each alert type, together with the alert type's risk level.
(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)
Alert type
Risk
Count
CSP: Failure to Define Directive with No Fallback
Medium
61 (290.5%)
CSP: Wildcard Directive
Medium
39 (185.7%)
CSP: script-src unsafe-eval
Medium
61 (290.5%)
CSP: script-src unsafe-inline
Medium
61 (290.5%)
CSP: style-src unsafe-inline
Medium
61 (290.5%)
Content Security Policy (CSP) Header Not Set
Medium
36 (171.4%)
CSP: Notices
Low
39 (185.7%)
Cookie No HttpOnly Flag
Low
2
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Low
82 (390.5%)
Strict-Transport-Security Header Not Set
Low
42 (200.0%)
Timestamp Disclosure - Unix
Low
63 (300.0%)
X-Content-Type-Options Header Missing
Low
1 (4.8%)
Content-Type Header Missing
Informational
7 (33.3%)
Information Disclosure - Suspicious Comments
Informational
111 (528.6%)
Loosely Scoped Cookie
Informational
28 (133.3%)
Modern Web Application
Informational
61 (290.5%)
Re-examine Cache-control Directives
Informational
65 (309.5%)
Session Management Response Identified
Informational
2 (9.5%)
Total
21

Vulnerabilities

a.Vulnerability Title	**X-Content-Type Header Missing**
b.Vulnerability Description	There is no X-Content-Type header in the HTTP response. The prevention of browsers sniffing MIME types, which can result in vulnerabilities like cross-site scripting (XSS) attacks, depends on this header. In the lack of this header, browsers may incorrectly read files with different MIME types, opening the door for possible attacks.
c.Affected Components	HTTP response headers, Web server configuration
d.Impact Assessment	The absence of the X-Content-Type header increases the risk of MIME-sniffing attacks, which alter browser handling of content, potentially leading to XSS vulnerabilities.
e.Steps to Reproduce	1.Send an HTTP request to the web server. 2.Use tools such as network scanners or browser developer tools to examine the HTTP response headers. 3.Make that the response does not contain the X-Content-Type header.
f.Proof of Concept (if applicable)	The vulnerability is not directly exploitable, but a simple examination reveals the absence of the header in HTTP responses, verifying the vulnerability.
g.Proposed Mitigation or Fix	Add the X-Content-Type-Options header with the value nosniff to configure the web server, reducing MIME-based attacks by ensuring browsers adhere to disclosed resource types.

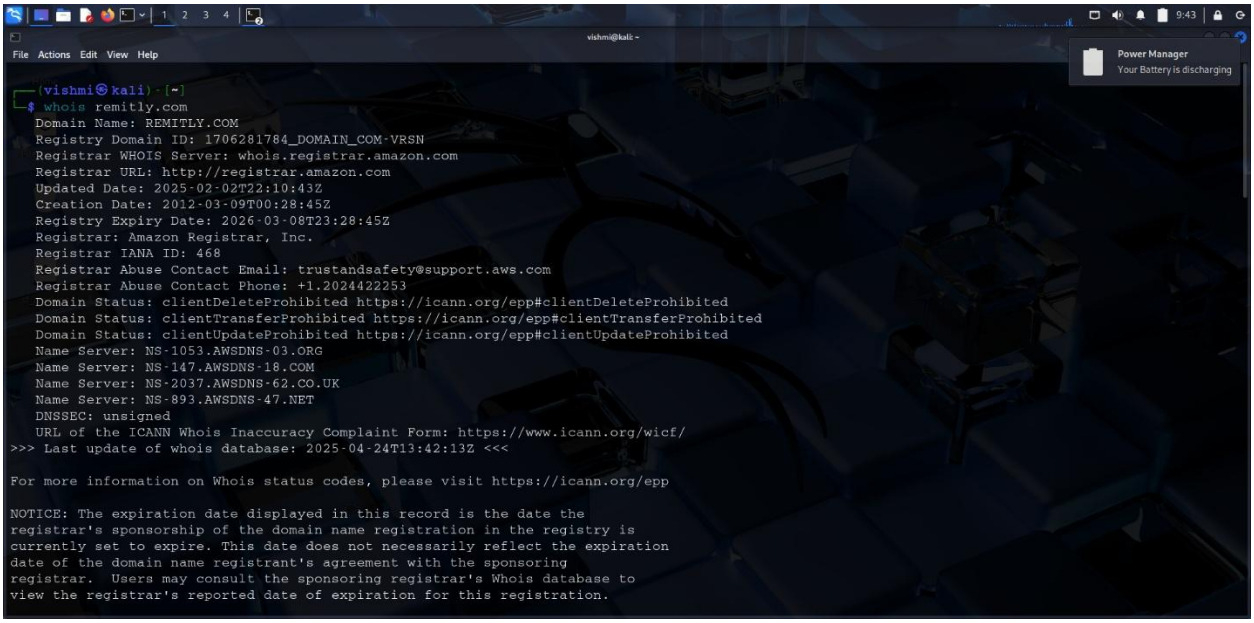
Report-08

Web Audit
remitly.com

Domain = *remitly.com*
Sub-domain = *www.remitly.com*
URL = *https://www.remitly.com*

Target Reconnaissance

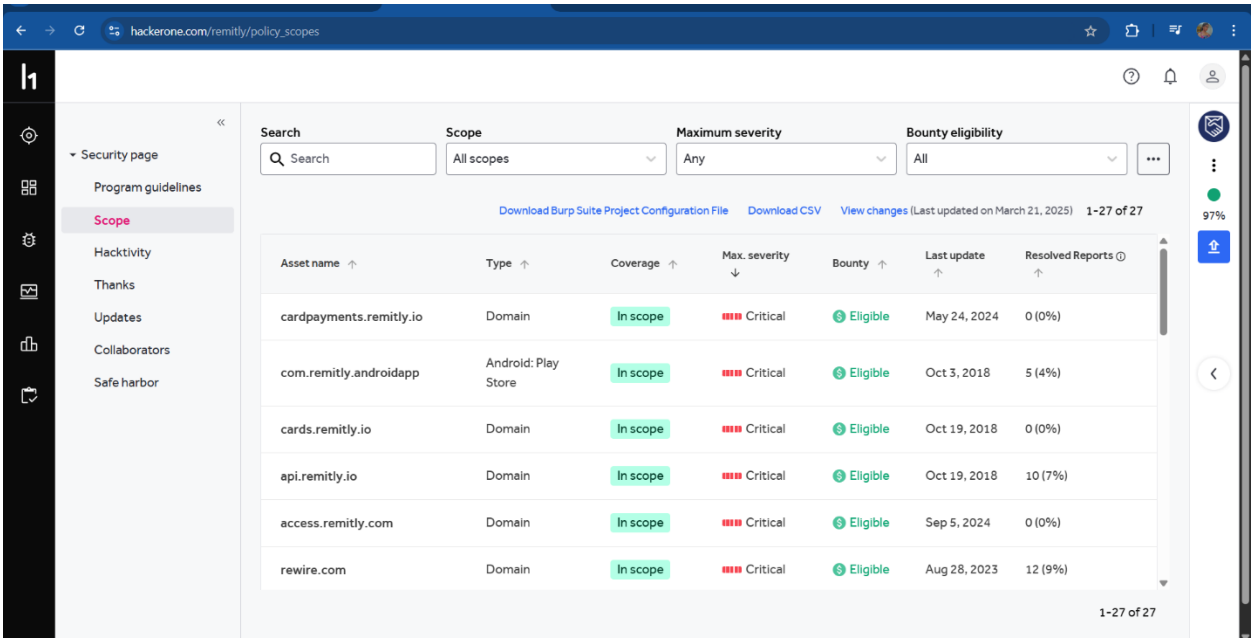
Introduction to Remitly and Audit Scope.

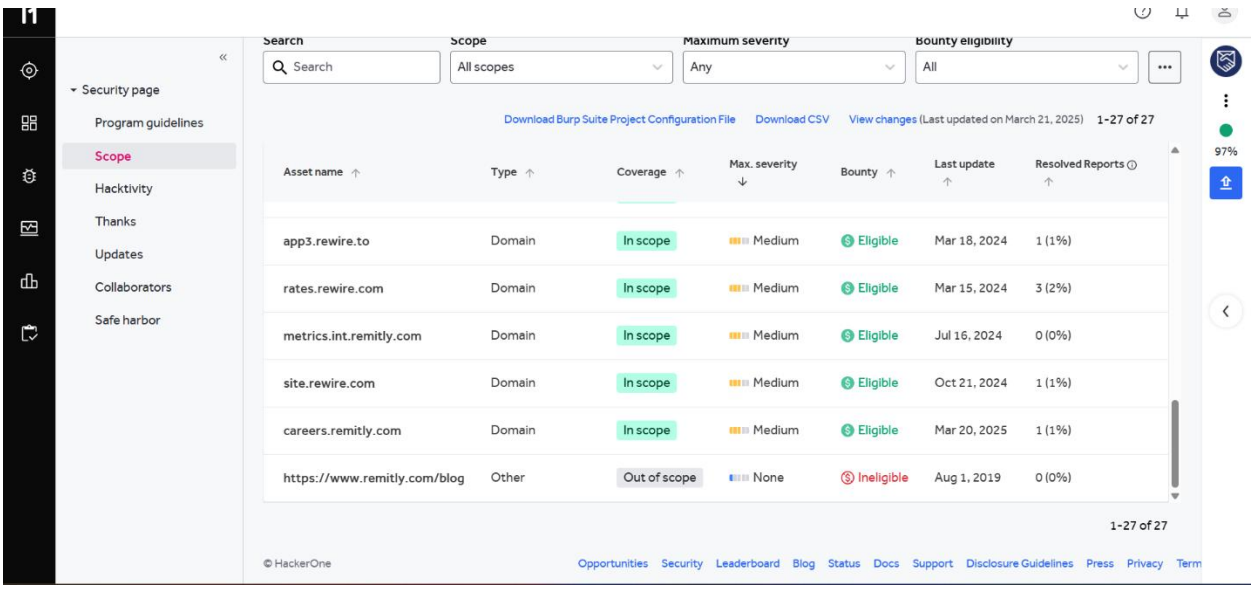


Remitly is a digital remittance company established in the United States that allows consumers to send money to more than 170 countries via the internet. Through its website and mobile app, this 2011-founded company provides quick, safe, and reasonably priced international transfers. Consumers have the choice of home delivery, mobile wallets, cash pickups, or bank deposits. Remitly's clear costs and real-time tracking make it particularly popular among immigrants helping families overseas. In 2021, the business went public, and it is still growing internationally.

These subdomains (and all included) have been approved as legitimate subdomains for testing in the **Hackerone** Bug Bounty program.

Eligible in-scope subdomains for bug bounty program are mentioned below.





Information gathering phase.

The information-gathering phase, often known as reconnaissance or recon, is essential to both assessments of security and cyberattacks. In order to map out the target's structure and determine how it functions, the target of this stage is to gather as much information as possible about it. Because it helps auditors or attackers identify vulnerabilities that could be exploited later on, this fundamental understanding is essential.

There are two main approaches to information gathering

1.Active Scanning :

Involves direct interaction with the target, which can generate noticeable activity and typically uncovers a wealth of details about the system.

2Passive Scanning :

Seeks to observe the target without direct engagement, resulting in less detectable activity but often providing more limited information

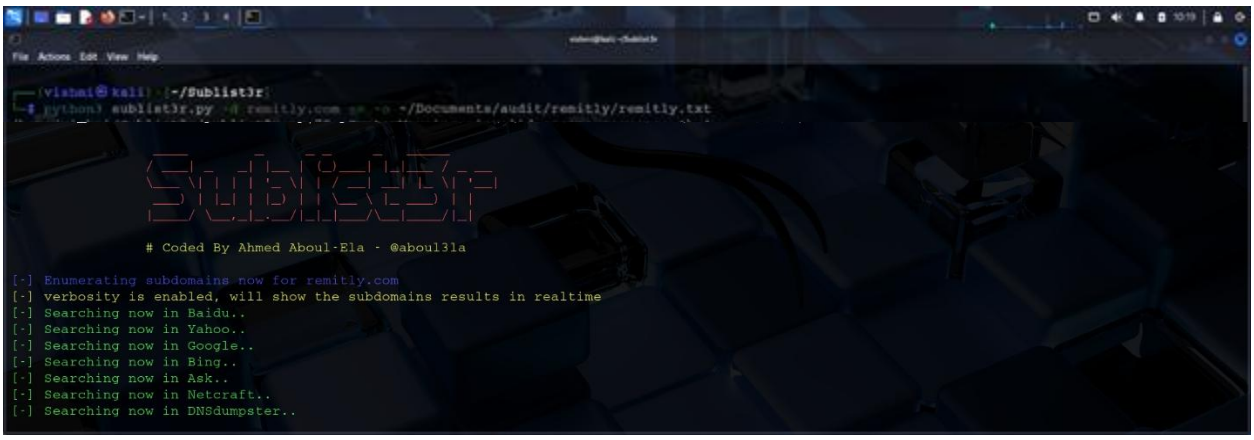
Finding active subdomains and their states

Sublist3r

Sublist3r is an open-source Python application that uses OSINT (Open Source Intelligence) techniques to quickly and effectively scan subdomains. Subdomains linked to a target domain can be found by penetration testers, security researchers, and bug bounty hunters using a variety of search engine queries (including Google, Yahoo, Bing, Baidu, and Ask). Additionally, Sublist3r includes a brute-force module (subbrute) to employ a stronger wordlist to improve the probability of discovering more subdomains.

I created a .txt file to store the subdomain headers that were initiated via sublist3r.

Path to .txt file = ***home/vishmi/Documents/audit/remitly/remitly.txt***

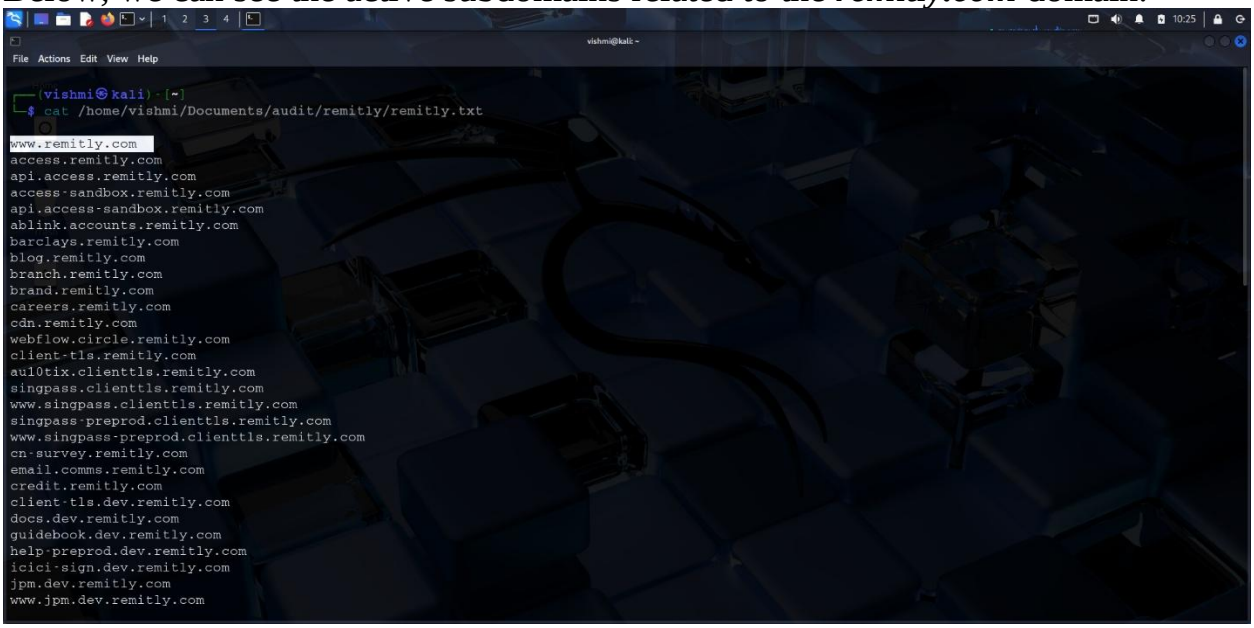


I got, these subdomains according to the ***remitly.com*** domain.

HTTProbe

HTTProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing on achievable goals by providing you with the URLs of active domains.
I am using the text file generated before by the sublist3r and stored the active subdomains to another new .txt file.

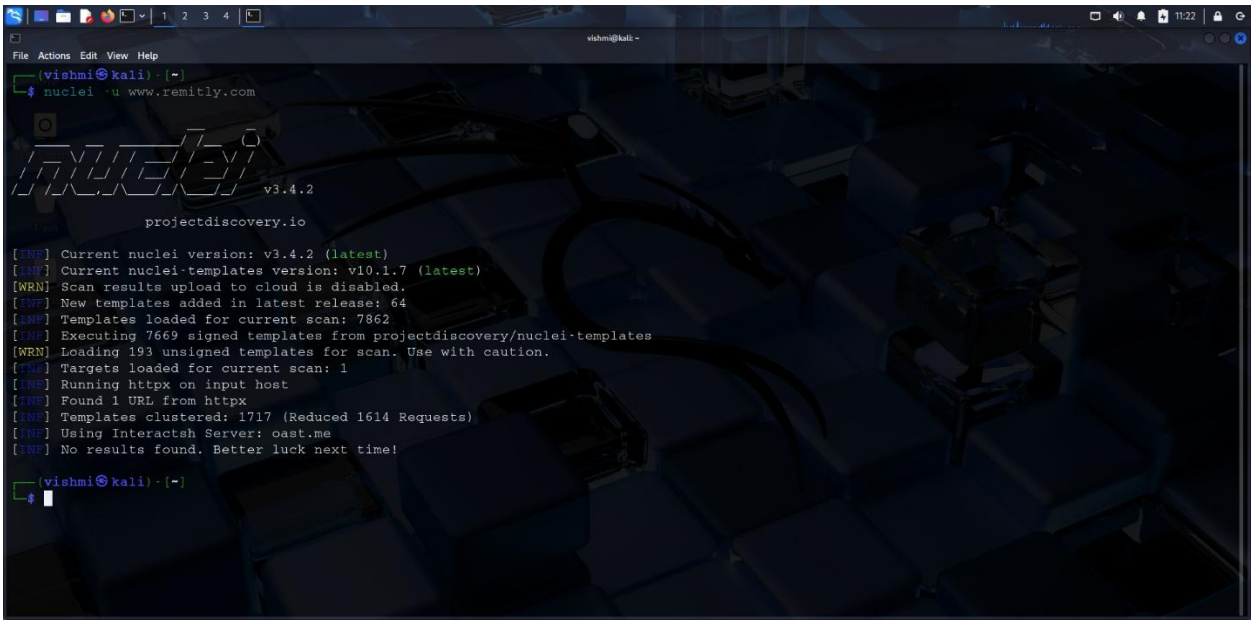
Below, we can see the active subdomains related to the ***remitly.com*** domain.



To move forward, I chose the active subdomain as **“www.remitly.com”.**

Nuclei

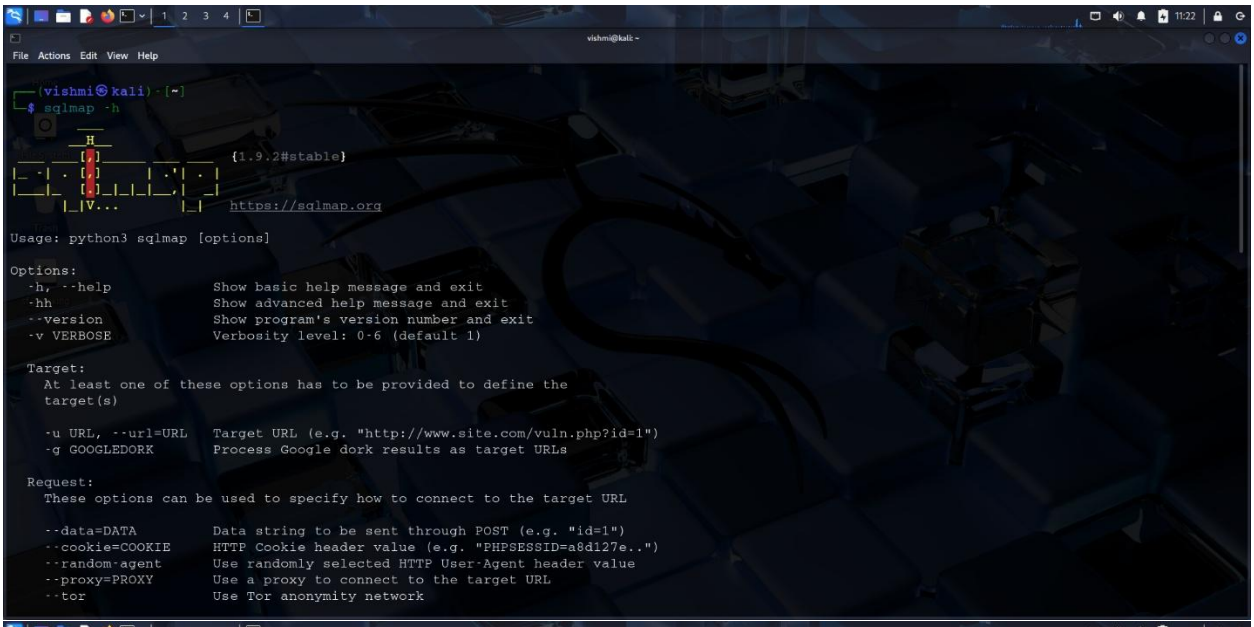
Nuclei is an open-source vulnerability scanner developed by ProjectDiscovery for security professionals, penetration testers, and bug bounty hunters. It uses customizable YAML("Yet Another Markup Language") -based templates to identify vulnerabilities such as misconfigurations, outdated software, and known CVEs (Common Vulnerabilities and Exposures).

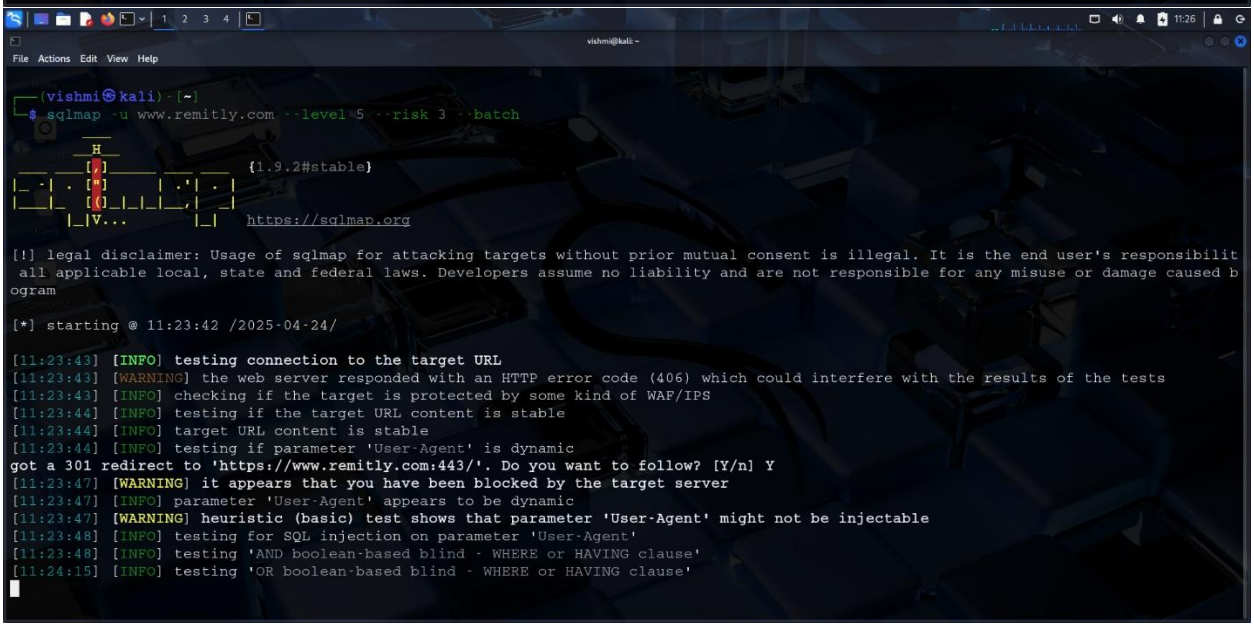


Here, the nuclei scan found no issue.

SQLmap

An open-source penetration testing tool called SQLmap makes it easier to find and take advantage of SQL injection flaws in web apps. If the database permits, it can even access the underlying file system or run commands on the server in addition to identifying the type of database and extracting data. Security experts frequently use it to evaluate and protect web apps from SQL injection attacks.





Option	Meaning
-u	For basic testing, the target URL is required.
--level5	Increases the number of payloads and tests that are done (maximum is 5).
--risk3	Increase the danger level of the payloads used (maximum is 3)
--batch	Executes SQLMap in a non-interactive mode, selecting default responses automatically.

Detected Information

* ***[WARNING] the web server responded with an HTTP error code.***

* ***[WARNING] heuristic (basic) test shows that parameter 'User-Agent' might be injectable***

[This is a *potential* vulnerability, but not confirmed.]

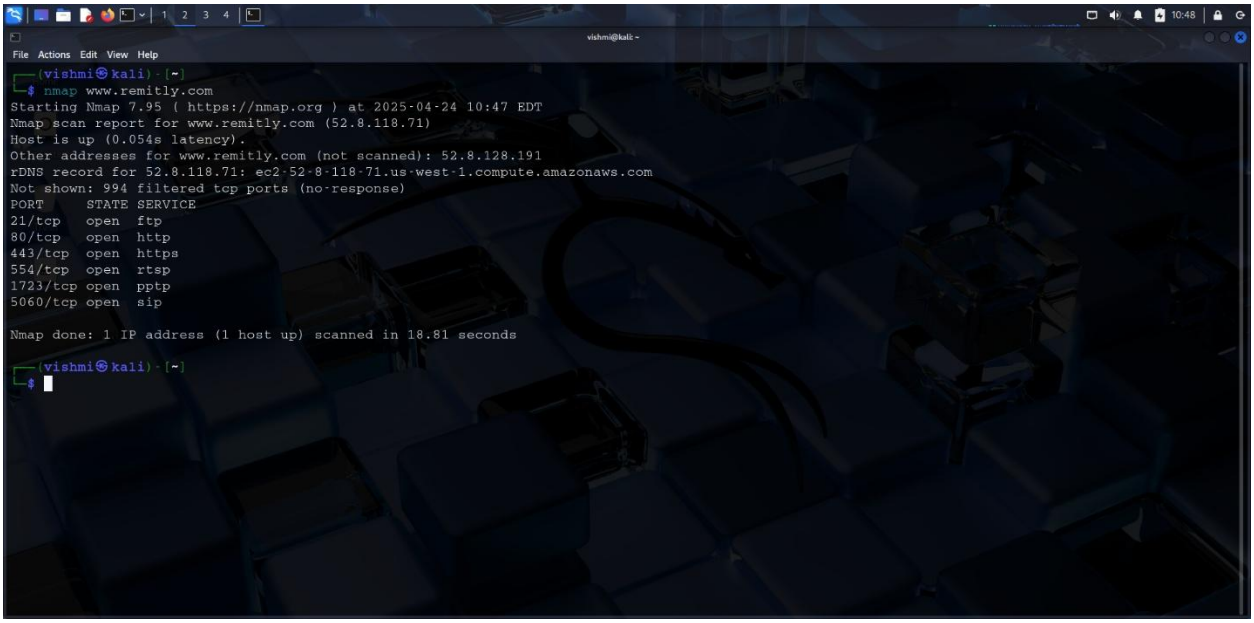
* ***[INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'***

[SQLmap is still in the process of testing for SQL injection using Boolean-based techniques.]

Searching for vulnerabilities

Nmap

Nmap (Network Mapper) is a strong, open-source network scanning program that uses packet transmission and response analysis to find hosts and services on a computer network. To find open ports, running services, operating systems, and active devices on a network, network managers and security experts utilize Nmap. Network inventory, vulnerability assessment, security auditing, and penetration testing are among its many uses.



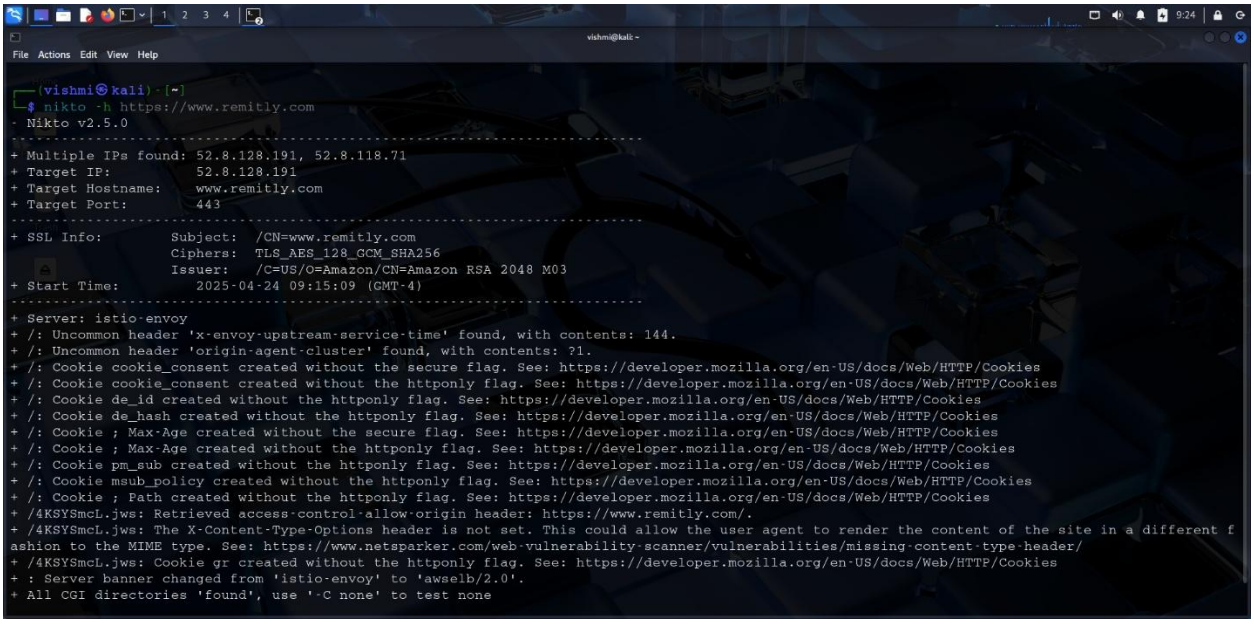
I discovered these details by using Nmap to search *www.remitly.com.*

PORT	STATE	SERVICE
21/tcp	open	ftp
80/tcp	open	http
443/tcp	open	https
554/tcp	open	rtsp
1723/tcp	open	pptp
5060/tcp	open	sip

PORT	SERVICE	Vulnerabilities
21/tcp	ftp	Unencrypted credentials are accepted.
80/tcp	http	Transmits plain text data.
443/tcp	https	Deprecated TLS versions are supported.
554/tcp	Rtsp	Usually doesn't have authenticity.
1723/tcp	pptp	Makes use of a weak encryption
5060/tcp	sip	Susceptible to spoofing and DoS due to lack of encryption.

Nikto

An open-source program called Nikto scans web servers for common vulnerabilities, malicious files, outdated software, and improperly configured settings, among other potential security issues. It is widely used for penetration testing and assessments, but it functions best when combined with other tools.



Security issues found on ***https://www.remitly.com's*** by Nikto Scan

*Uncommon header 'x-envoy-upstream-service-time' found.

*Uncommon header 'origin-agent-cluster' found.

*The X-Content-Type-Options header is not set.

*Retrieved access-control-allow-origin header.

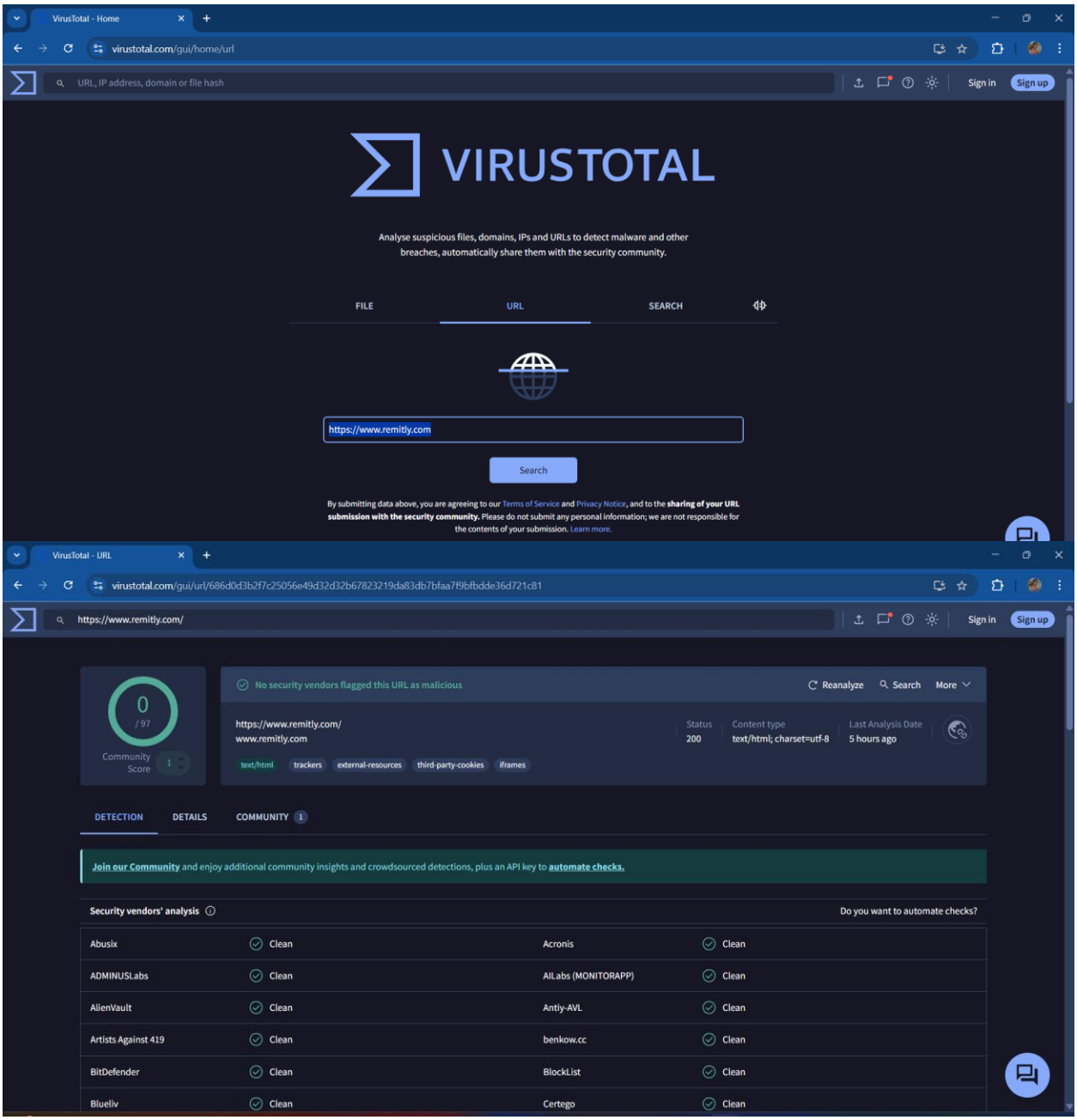
*Path created without the httponly flag.

*cookie_consent created without the httponly flag .

Virustotal

Virustotal is a free web service called VirusTotal employs 70 antivirus engines and URL blocklisting services to scan files and URLs for malware, adware, and other malicious content.

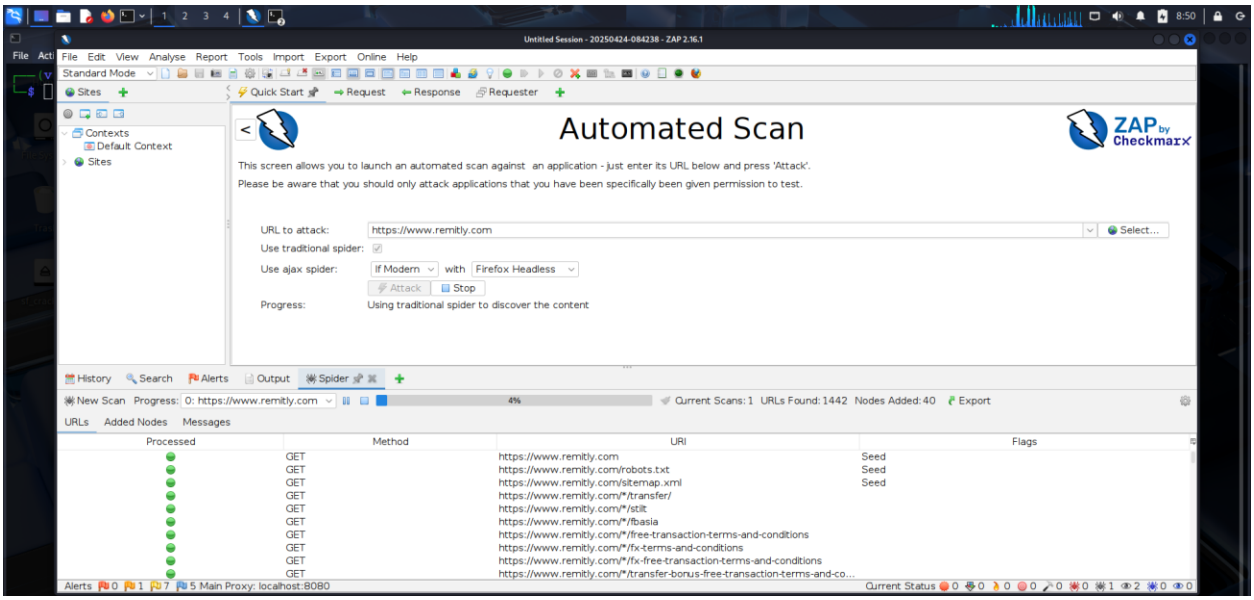
I entered https://www.remitly.com in URL section .



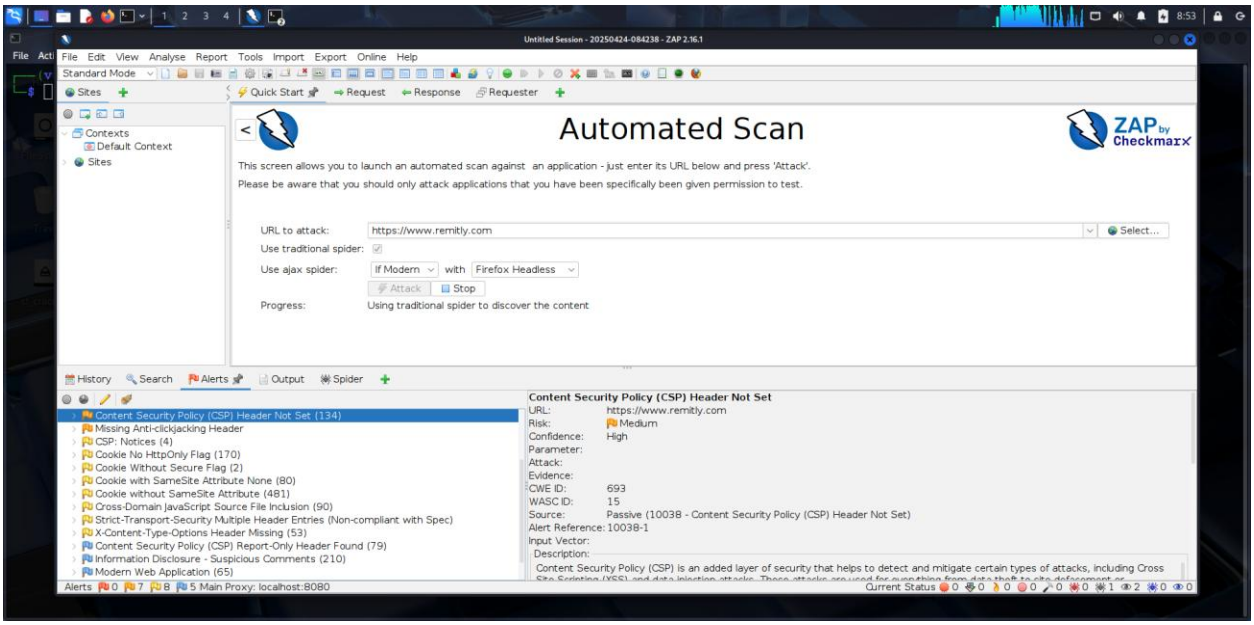
OWASP ZAP

A free and open-source security tool called ***OWASP ZAP (Zed Attack Proxy)*** simulates attacks and examines how an application behaves when it is running to help in discovering and fixing vulnerabilities in web applications.

In here, I entered the target URL [***https://www.remitly.com***] designated textbox, simply select "Attack" to initiate the scanning process.



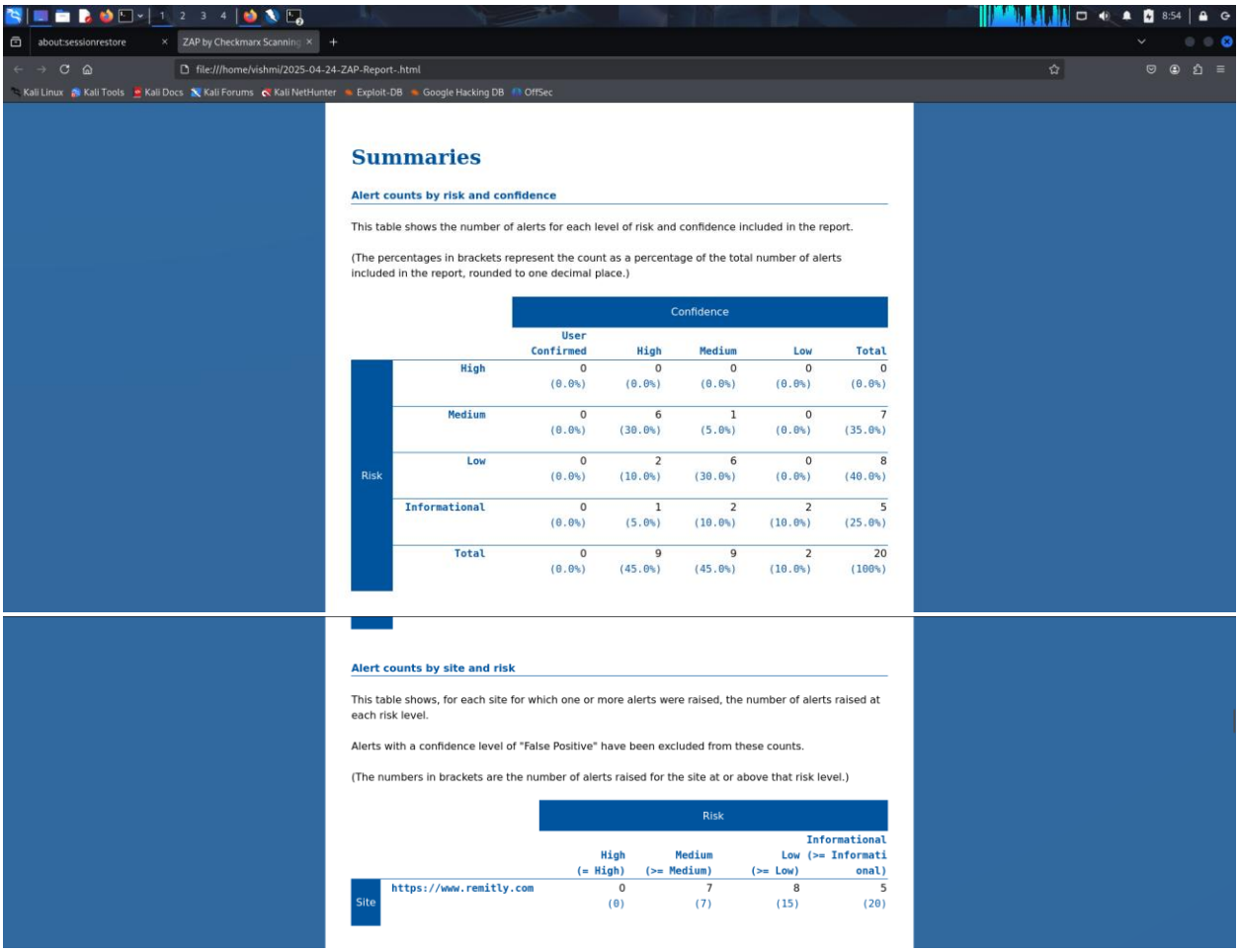
As next step, I entered to the Alerts tab. Here it's detected a vulnerability.



After finishing, it is possible to obtain a thorough report of the results by choosing "Report." The results of scanning many domains are displayed in the screenshots below.

Report = file:///home/vishmi/2025-04-24-ZAP-Report-.html

Please take note that these vulnerabilities have been rated using the OWASP risk rating methodology, which is available at this link.[*OWASP Risk Rating Methodology*]



Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	6 (30.0%)	1 (5.0%)	0 (0.0%)	7 (35.0%)
	Low	0 (0.0%)	2 (10.0%)	6 (30.0%)	0 (0.0%)	8 (40.0%)
	Informational	0 (0.0%)	1 (5.0%)	2 (10.0%)	2 (10.0%)	5 (25.0%)
	Total	0 (0.0%)	9 (45.0%)	9 (45.0%)	2 (10.0%)	20 (100%)

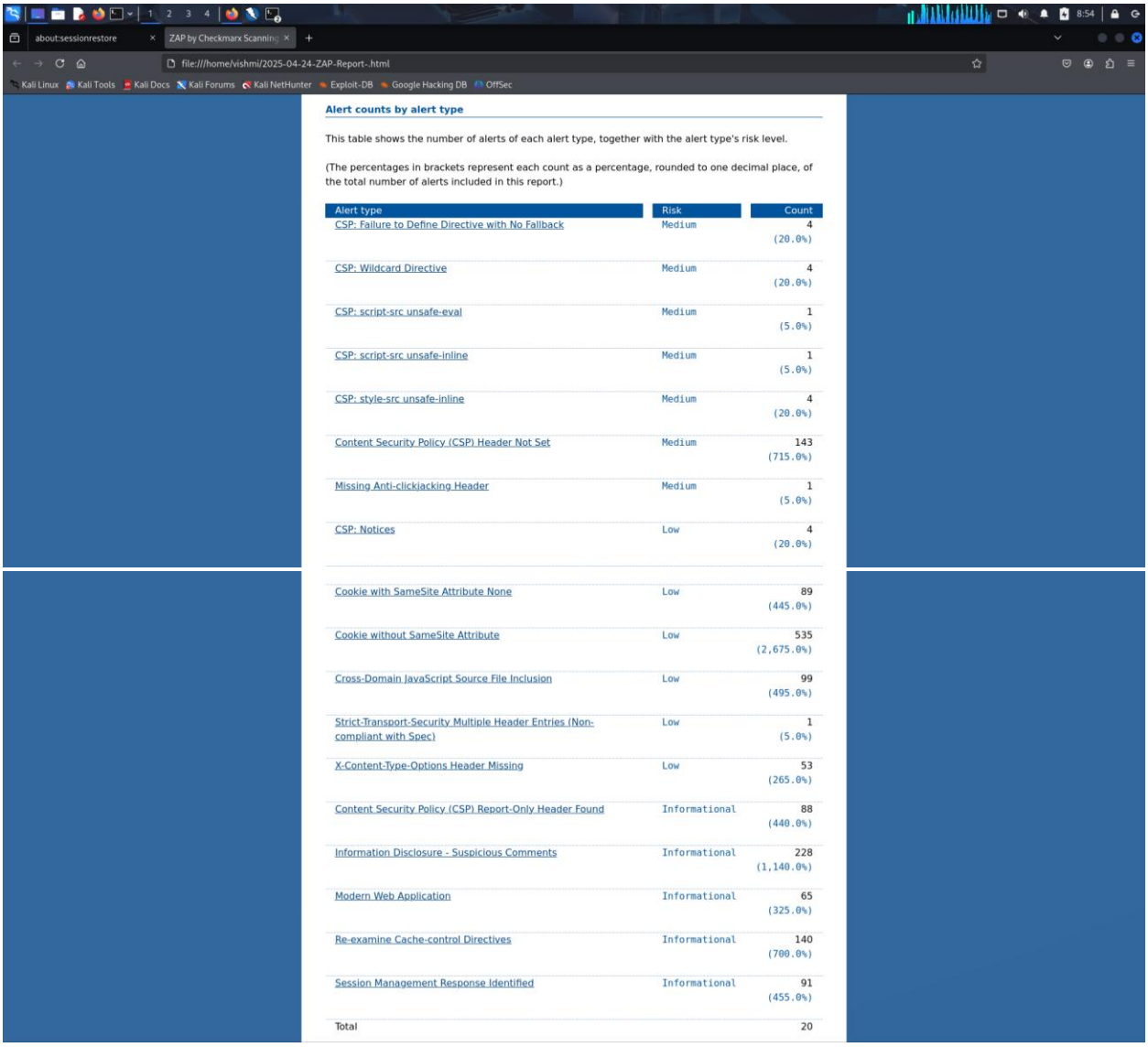
Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://www.remitly.com	0 (0)	7 (7)	8 (15)	5 (20)



Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
CSP: Failure to Define Directive with No Fallback	Medium	4 (20.0%)
CSP: Wildcard Directive	Medium	4 (20.0%)
CSP: script-src unsafe-eval	Medium	1 (5.0%)
CSP: script-src unsafe-inline	Medium	1 (5.0%)
CSP: style-src unsafe-inline	Medium	4 (20.0%)
Content Security Policy (CSP) Header Not Set	Medium	143 (715.0%)
Missing Anti-clickjacking Header	Medium	1 (5.0%)
CSP: Notices	Low	4 (20.0%)
Cookie with SameSite Attribute None	Low	89 (445.0%)
Cookie without SameSite Attribute	Low	535 (2,675.0%)
Cross-Domain JavaScript Source File Inclusion	Low	99 (495.0%)
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	1 (5.0%)
X-Content-Type-Options Header Missing	Low	53 (265.0%)
Content Security Policy (CSP) Report-Only Header Found	Informational	88 (440.0%)
Information Disclosure - Suspicious Comments	Informational	228 (1,140.0%)
Modern Web Application	Informational	65 (325.0%)
Re-examine Cache-control Directives	Informational	140 (700.0%)
Session Management Response Identified	Informational	91 (455.0%)
Total		20

Vulnerabilities

a.Vulnerability Title	**Content-Security-Policy(CSP) Header Not Set**
b.Vulnerability Description	The application is vulnerable to a number of security threats, including as injection attacks, clickjacking, data theft, and Cross-Site Scripting (XSS), since the HTTP response lacks the Content-Security-Policy (CSP) header. In order to lessen the impact of malicious information, CSP is an essential security mechanism that limits the kinds of resources that a web application can load and run.
c.Affected Components	Web server configuration, HTTP response headers of the web application.
d.Impact Assessment	When the Content-protection-Policy (CSP) header is missing, there is a greater chance of malicious script execution, data theft, clickjacking, Cross-Site Scripting (XSS), and other threats that risk user and sensitive data protection.
e.Steps to Reproduce	1.Open a browser and navigate to the impacted website. 2.Use the browser developer tools (F12 → Network → Headers tab) to examine the HTTP response headers. 3.Verify that the answer does not contain the Content-Security-Policy header.
f.Proof of Concept (if applicable)	1. Open the website (e.g.,youtube. google.com) in a web browser. 2.Use browser Developer Tools (F12), navigate to the "Network" tab, and inspect the HTTP response headers. 3.Verify that there is no *Content-Security-Policy* header listed among the response headers.
g.Proposed Mitigation or Fix	Implement a strict Content-Security-Policy (CSP) in the server configuration.

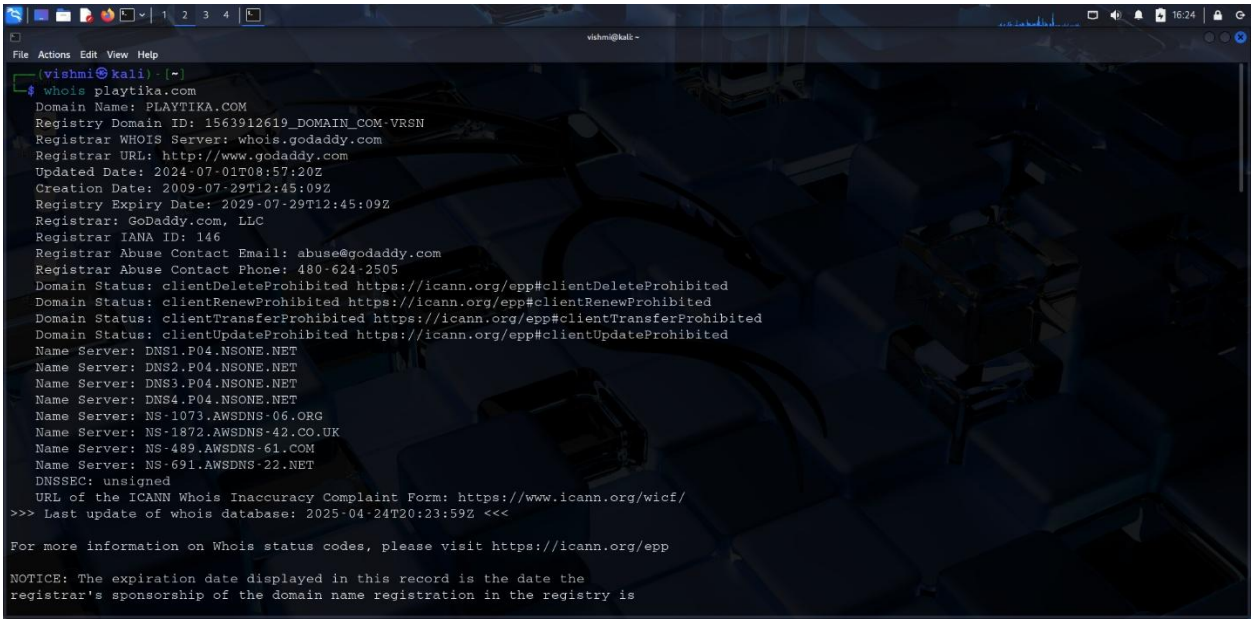
Report-09

Web Audit playtika.com

Domain = *playtika.com*
Sub-domain = *www.playtika.com*
URL = *https://www.playtika.com*

Target Reconnaissance

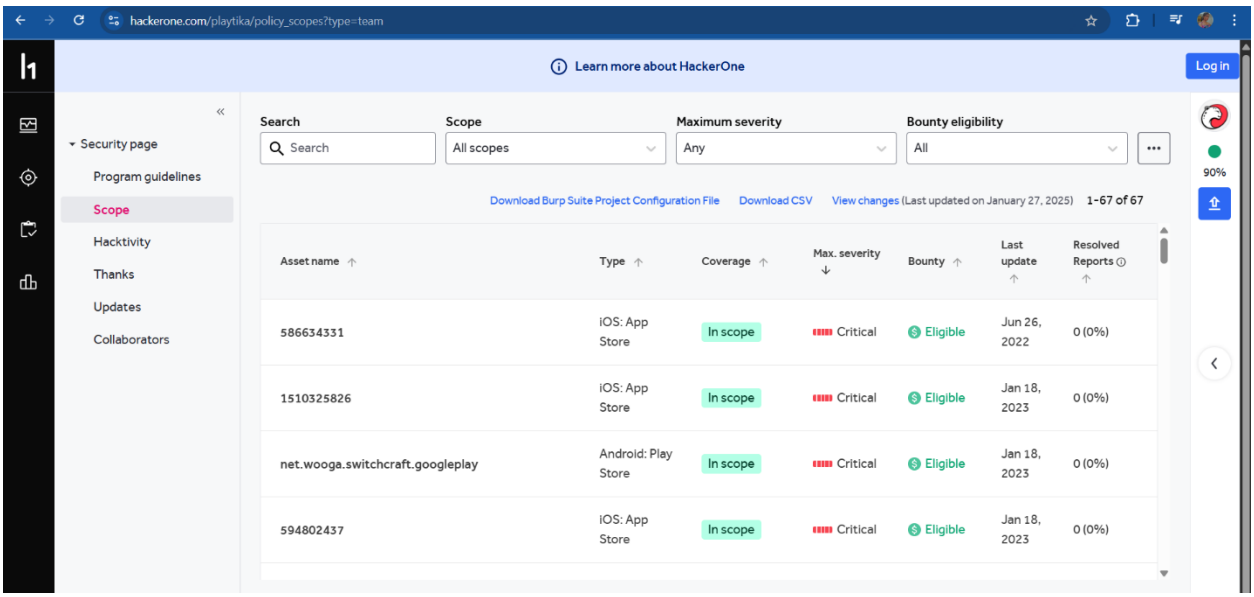
Introduction to Playtika and Audit Scope

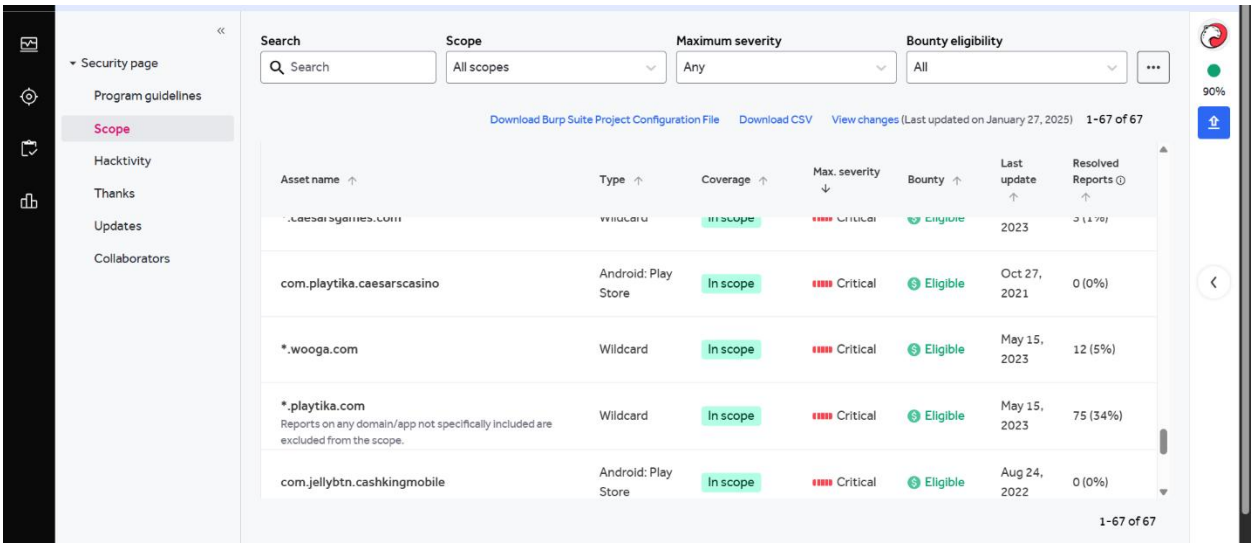


Known for creating captivating and immersive social games, **Playtika** is a leading company in mobile gaming worldwide. Millions of people throughout the world enjoy the company's extensive selection of casino-style and casual games, which were founded in 2010. To keep players engaged, Playtika blends cutting-edge analytics with imaginative design, emphasizing data-driven user experience and inventive gameplay. With well-known games like Slotomania and House of Fun, Playtika has become a significant force in the online gaming market.

These subdomains (and all included) have been approved as legitimate subdomains for testing in the **Hackerone** Bug Bounty program.

Eligible in-scope subdomains for bug bounty program are mentioned below.





Information gathering phase.

The information-gathering phase, often known as reconnaissance or recon, is essential to both assessments of security and cyberattacks. In order to map out the target's structure and determine how it functions, the target of this stage is to gather as much information as possible about it. Because it helps auditors or attackers identify vulnerabilities that could be exploited later on, this fundamental understanding is essential.

There are two main approaches to information gathering

1.Active Scanning :

Involves direct interaction with the target, which can generate noticeable activity and typically uncovers a wealth of details about the system.

2.Passive Scanning :

Seeks to observe the target without direct engagement, resulting in less detectable activity but often providing more limited information

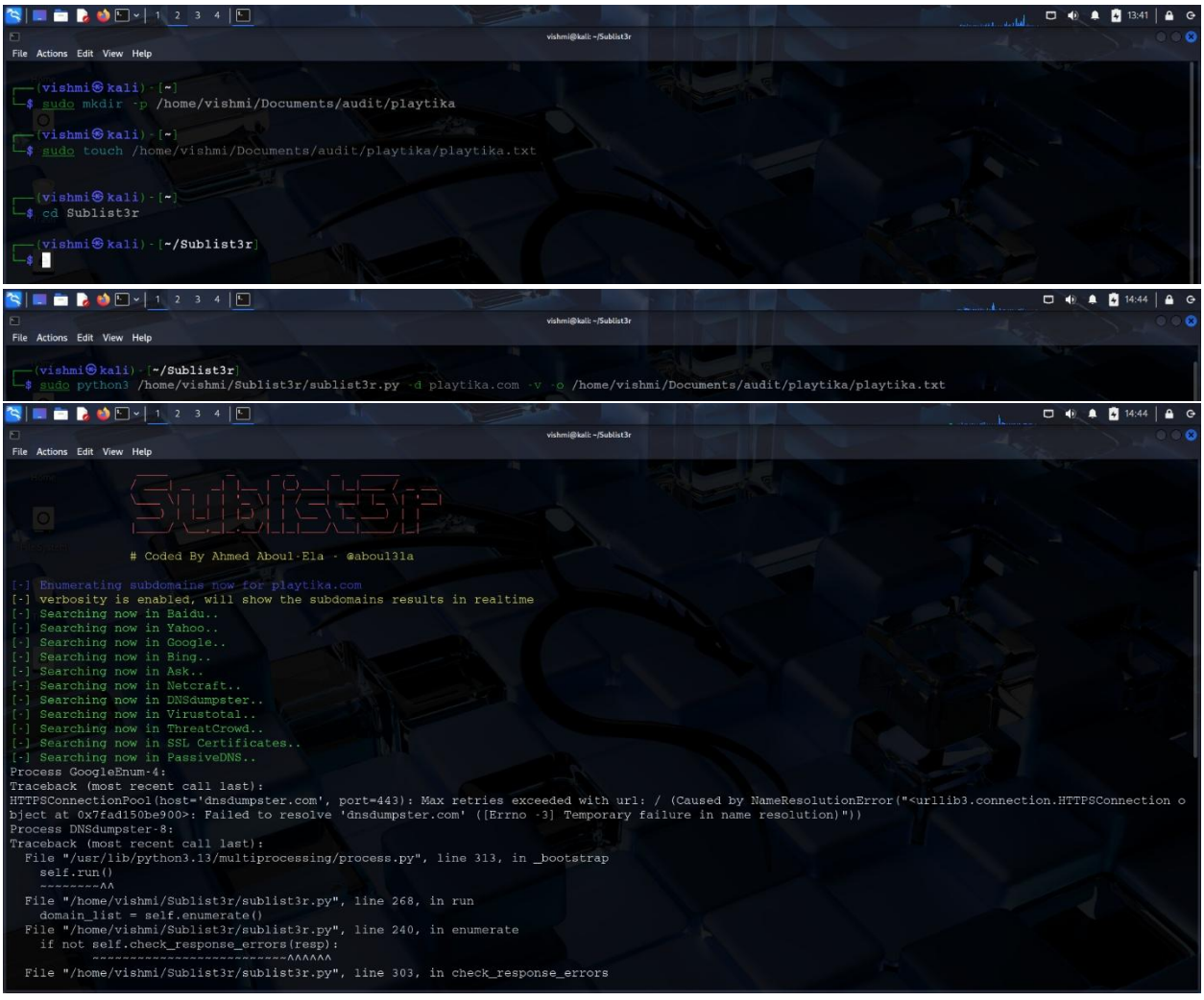
Finding active subdomains and their states

Sublist3r

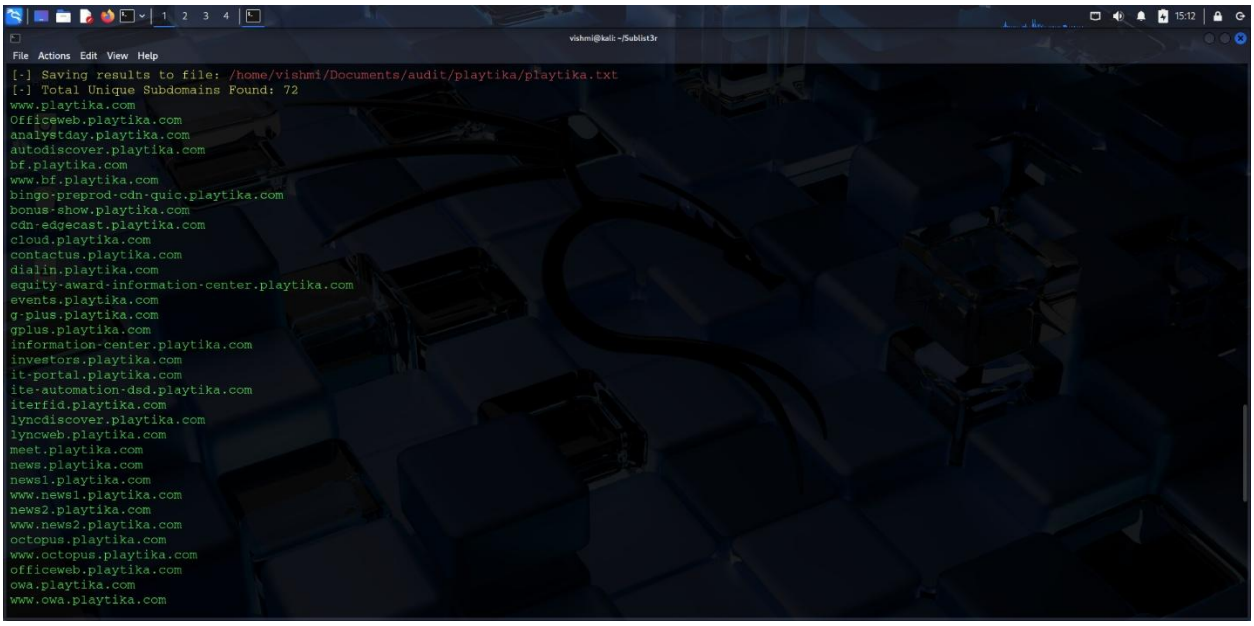
Sublist3r is an open-source Python application that uses OSINT (Open Source Intelligence) techniques to quickly and effectively scan subdomains. Subdomains linked to a target domain can be found by penetration testers, security researchers, and bug bounty hunters using a variety of search engine queries (including Google, Yahoo, Bing, Baidu, and Ask). Additionally, Sublist3r includes a brute-force module (subbrute) to employ a stronger wordlist to improve the probability of discovering more subdomains.

I created a .txt file to store the subdomain headers that were initiated via sublist3r.

Path to .txt file = ***home/vishmi/Documents/audit/ playtika / playtika.txt***



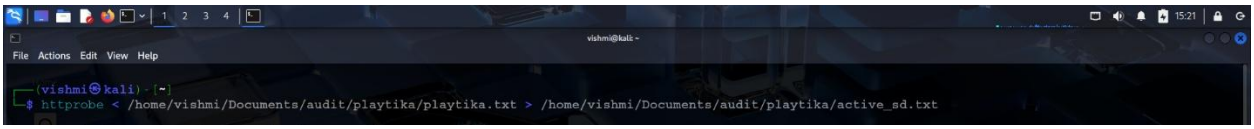
I got, these subdomains according to the ***playtika.com*** domain.



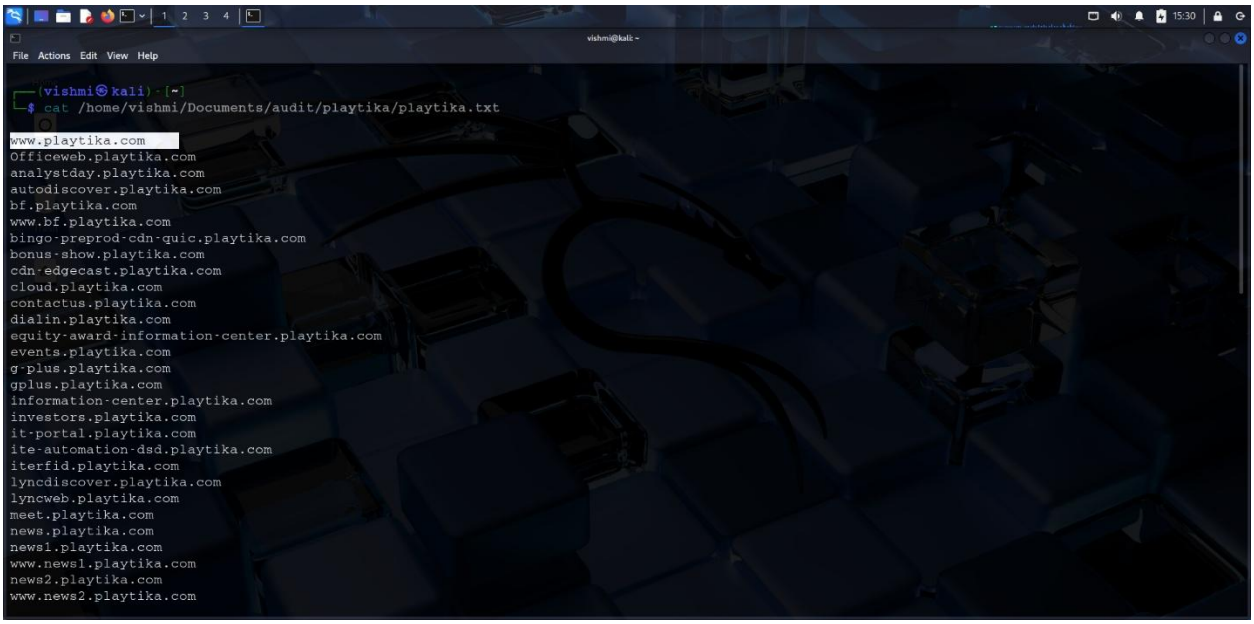
HTTProbe

HTTProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing on achievable goals by providing you with the URLs of active domains.

I am using the text file generated before by the sublist3r and stored the active subdomains to another new .txt file.



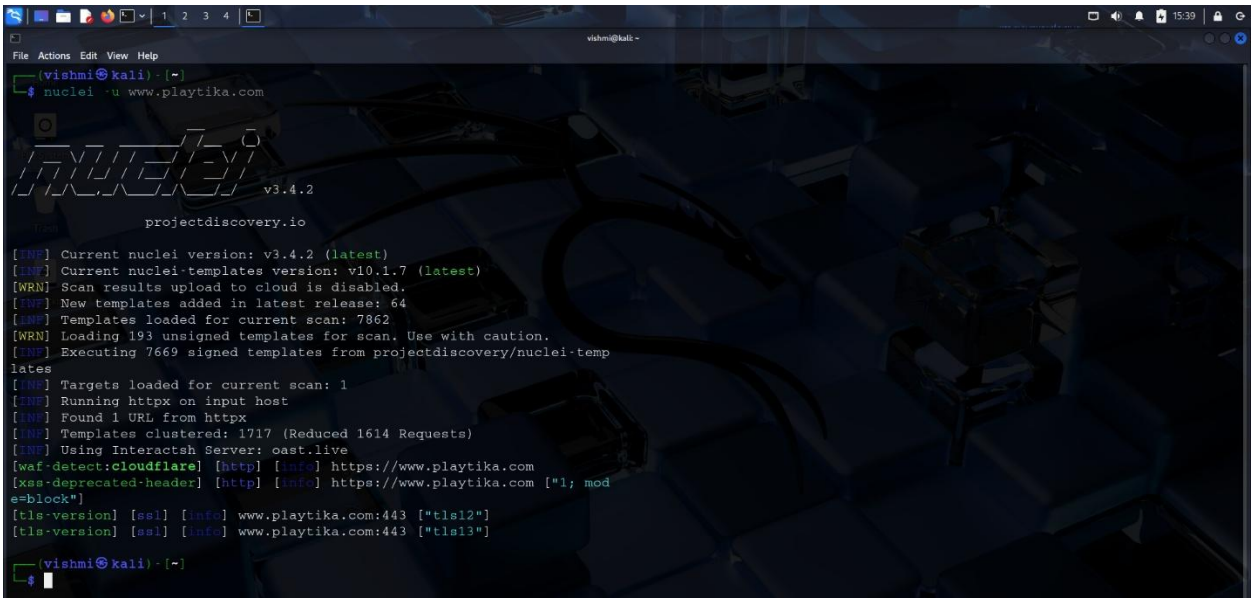
Below, we can see the active subdomains related to the ***playtika.com*** domain.



To move forward, I chose the active subdomain as **“www.playtika.com”.**

Nuclei

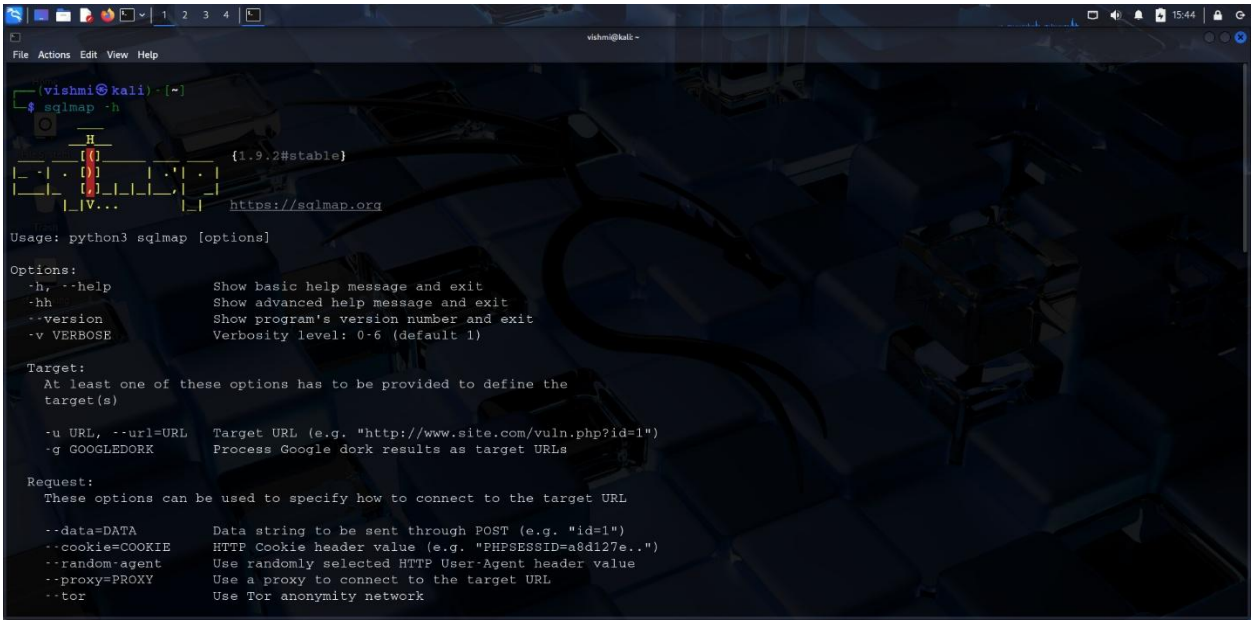
Nuclei is an open-source vulnerability scanner developed by ProjectDiscovery for security professionals, penetration testers, and bug bounty hunters. It uses customizable YAML("Yet Another Markup Language") -based templates to identify vulnerabilities such as misconfigurations, outdated software, and known CVEs (Common Vulnerabilities and Exposures).

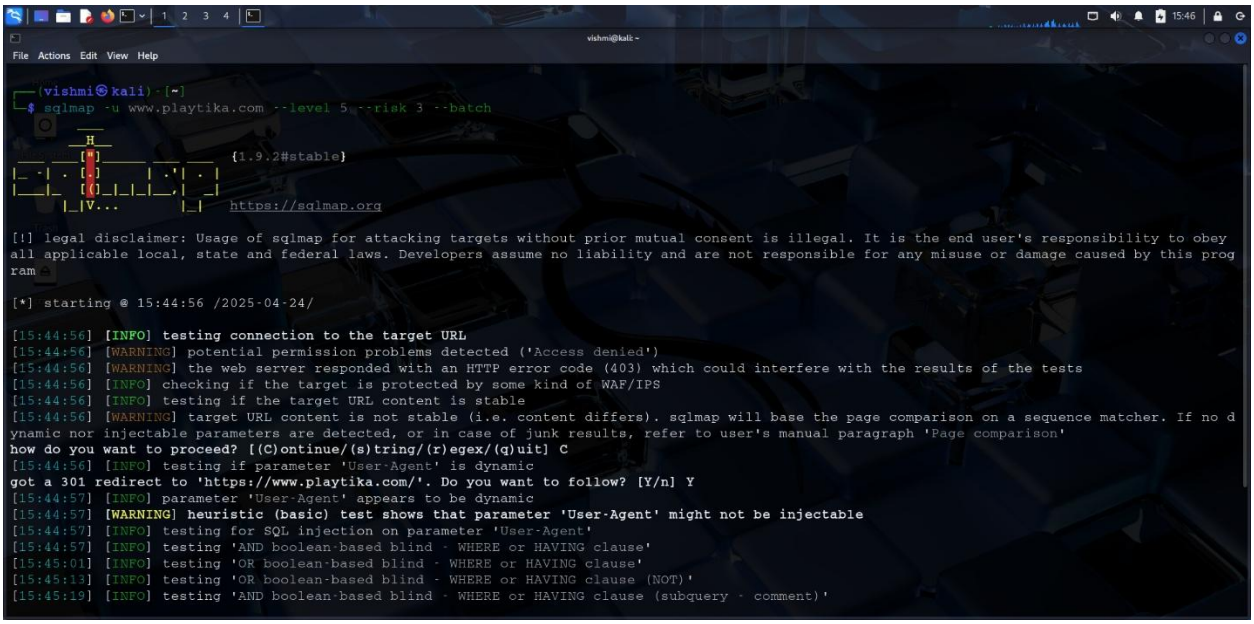


Vulnerability Type	Description	Risk
Cloudflare WAF (Web Application Firewall)	Cloudflare, a reverse proxy and security platform that offers a WAF, DDoS protection, bot control, and other features, protects the target.	Low/ Informational
xss-deprecated.header [http]	The header, used to control the browser's XSS filter, is no longer supported by most modern browsers like Chrome and Edge.	Low/ Informational
SSL/TLS Certificate Expiry	SSL/TLS certificate expired for go.figma.com:443.	High

SQLmap

An open-source penetration testing tool called SQLmap makes it easier to find and take advantage of SQL injection flaws in web apps. If the database permits, it can even access the underlying file system or run commands on the server in addition to identifying the type of database and extracting data. Security experts frequently use it to evaluate and protect web apps from SQL injection attacks.





Option	Meaning
-u	For basic testing, the target URL is required.
--level5	Increases the number of payloads and tests that are done (maximum is 5).
--risk3	Increase the danger level of the payloads used (maximum is 3)
--batch	Executes SQLMap in a non-interactive mode, selecting default responses automatically.

Detected Information

* ***[WARNING] heuristic (basic) test shows that parameter 'User-Agent' might be injectable***

[This is a *potential* vulnerability, but not confirmed.]

* ***[INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'***

[SQLmap is still in the process of testing for SQL injection using Boolean-based techniques.]

**** [WARNING] potential permission problems detected***

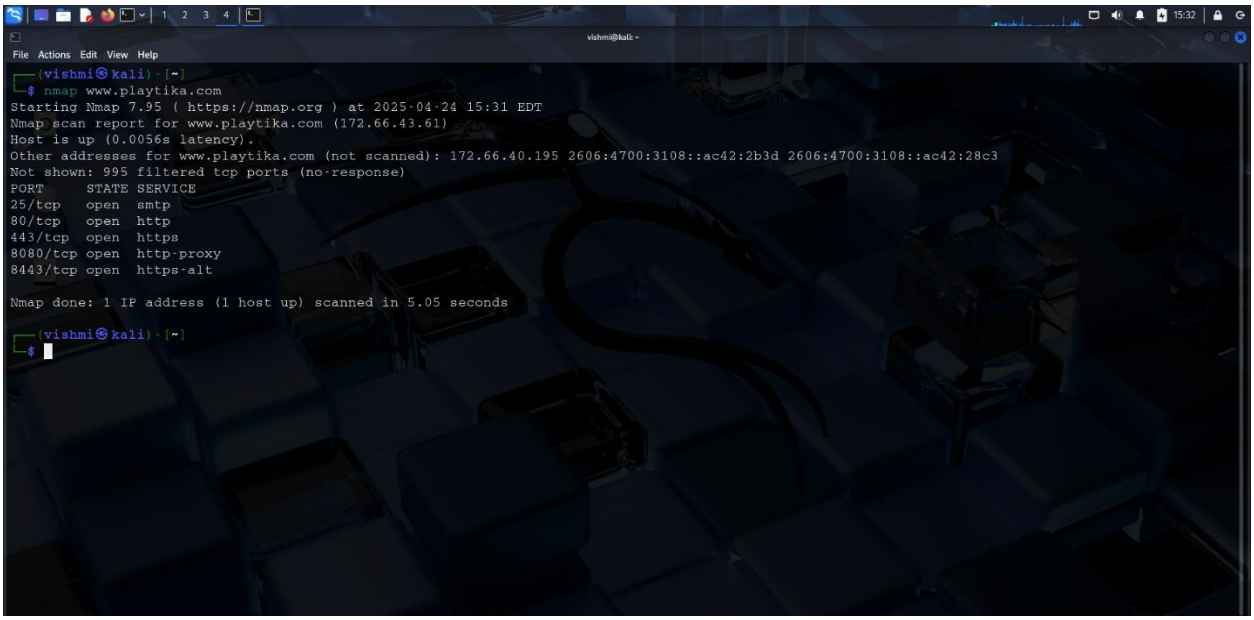
**** [WARNING] target URL content is not stable***

**** [WARNING] the web server responded with an HTTP error code***

Searching for vulnerabilities

Nmap

Nmap (Network Mapper) is a strong, open-source network scanning program that uses packet transmission and response analysis to find hosts and services on a computer network. To find open ports, running services, operating systems, and active devices on a network, network managers and security experts utilize Nmap. Network inventory, vulnerability assessment, security auditing, and penetration testing are among its many uses.



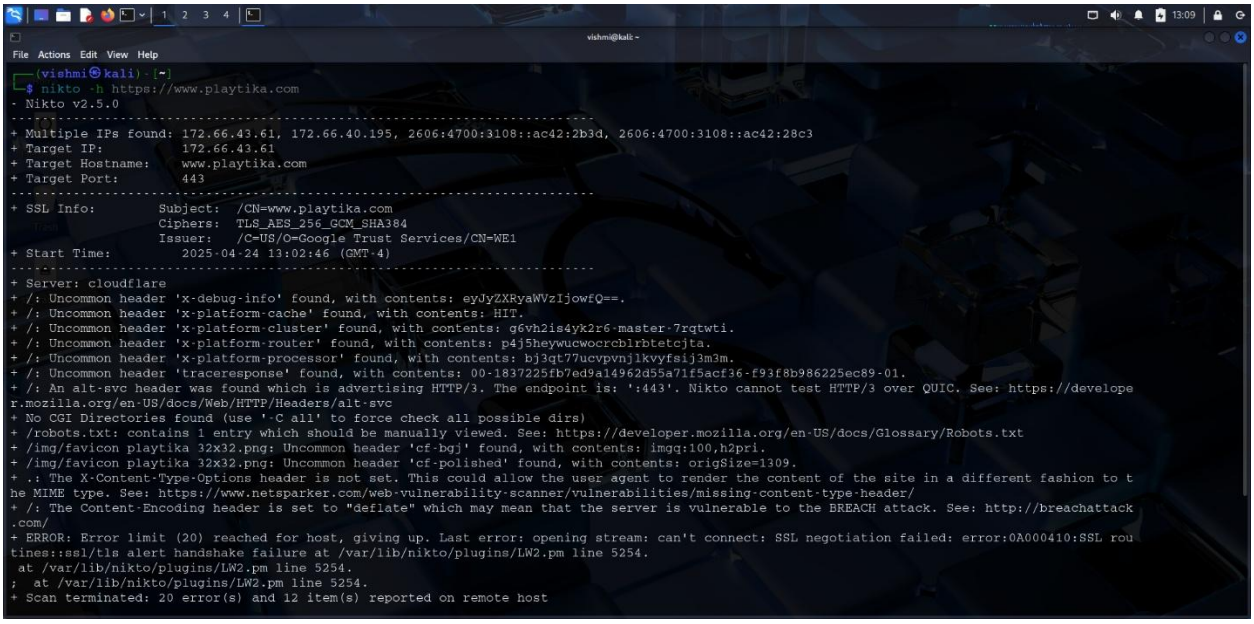
I discovered these details by using Nmap to search *www.playtika.com.*

PORT	STATE	SERVICE
25/tcp	open	smtp
80/tcp	open	http
443/tcp	open	https
8080/tcp	open	http-proxy
8443/tcp	open	https-alt

PORT	SERVICE	Vulnerabilities
25/tcp	smtp	Allows open relay if misconfigured; transmits credentials in plaintext.
80/tcp	http	Transmits plain text data.
443/tcp	https	Deprecated TLS versions are supported.
8080/tcp	http-proxy	May expose internal services; often lacks proper authentication.
8443/tcp	https-alt	May support weak SSL/TLS ciphers or self-signed certificates.

Nikto

An open-source program called Nikto scans web servers for common vulnerabilities, malicious files, outdated software, and improperly configured settings, among other potential security issues. It is widely used for penetration testing and assessments, but it functions best when combined with other tools.



Security issues found on ***https://www.playtika.com's*** by Nikto Scan.

* An alt-svc header was found which is advertising HTTP/3.

* No CGI Directories found.

* The X-Content-Type-Options header is not set.

* The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack.

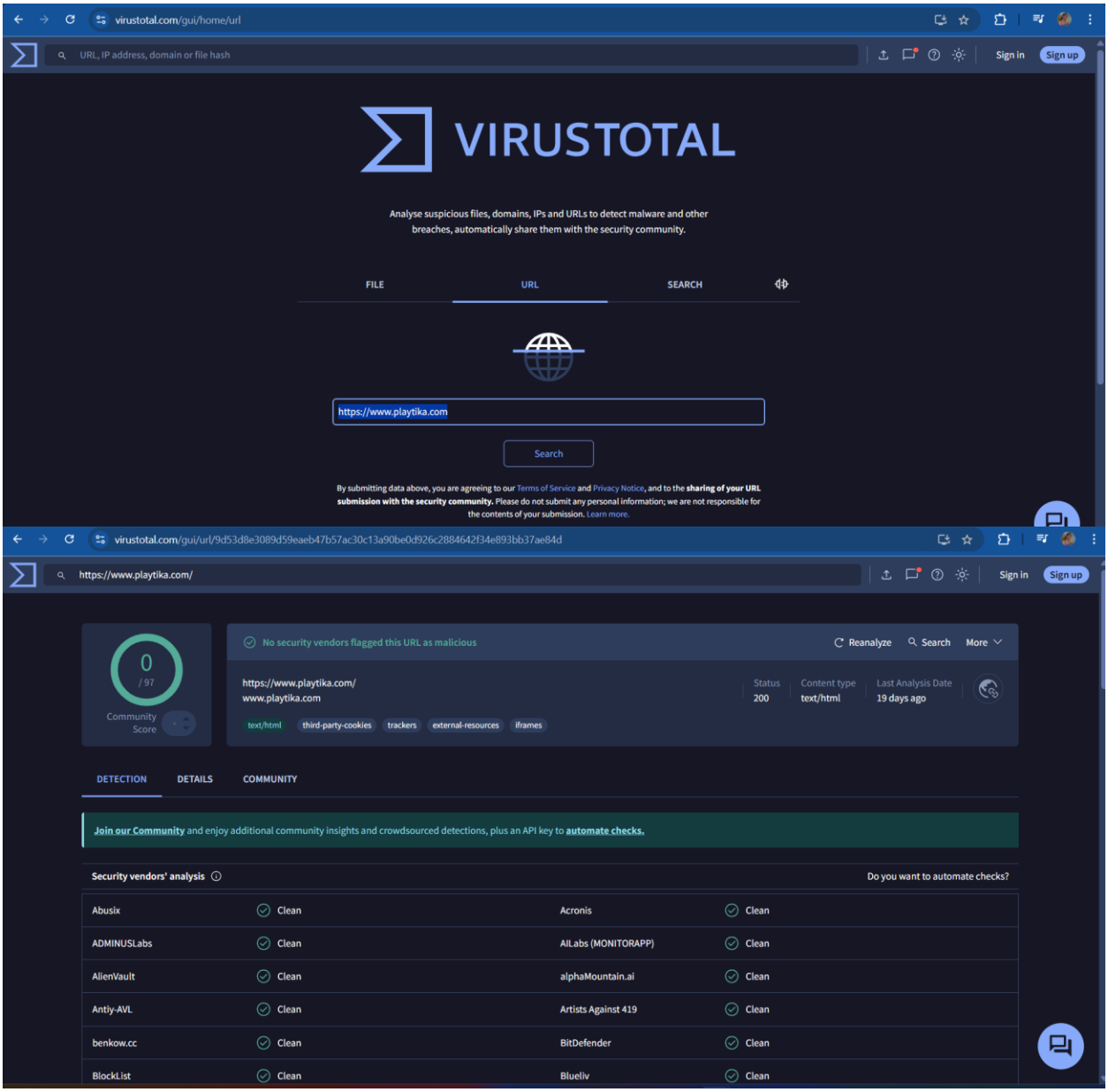
* Uncommon header 'x-debug-info' found.

*Uncommon header 'x-platform-cache' found.

Virustotal

Virustotal is a free web service called VirusTotal employs 70 antivirus engines and URL blocklisting services to scan files and URLs for malware, adware, and other malicious content.

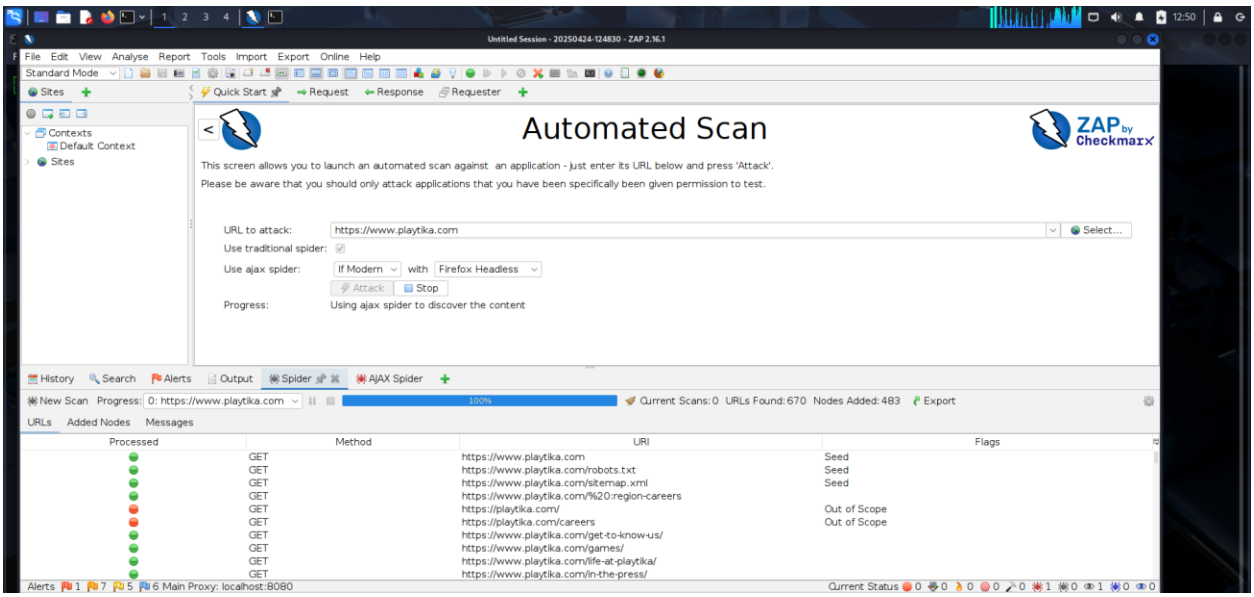
I entered https://www.playtika.com in URL section .



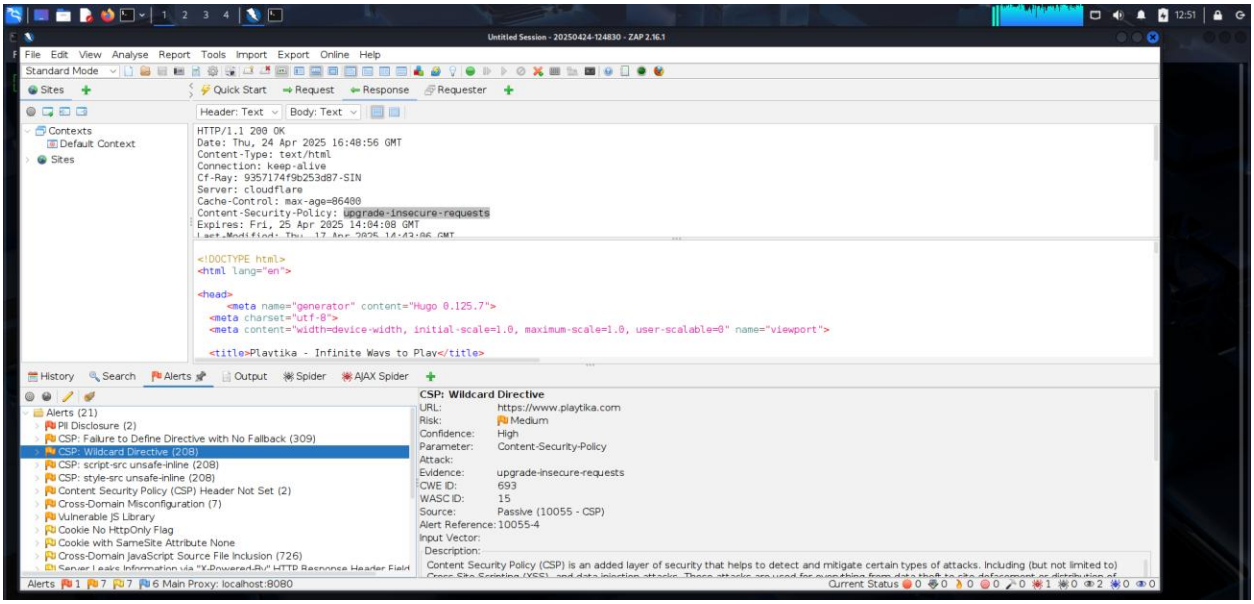
OWASP ZAP

A free and open-source security tool called ***OWASP ZAP (Zed Attack Proxy)*** simulates attacks and examines how an application behaves when it is running to help in discovering and fixing vulnerabilities in web applications.

In here, I entered the target URL [***https://www.playtika.com***] designated textbox, simply select "Attack" to initiate the scanning process.



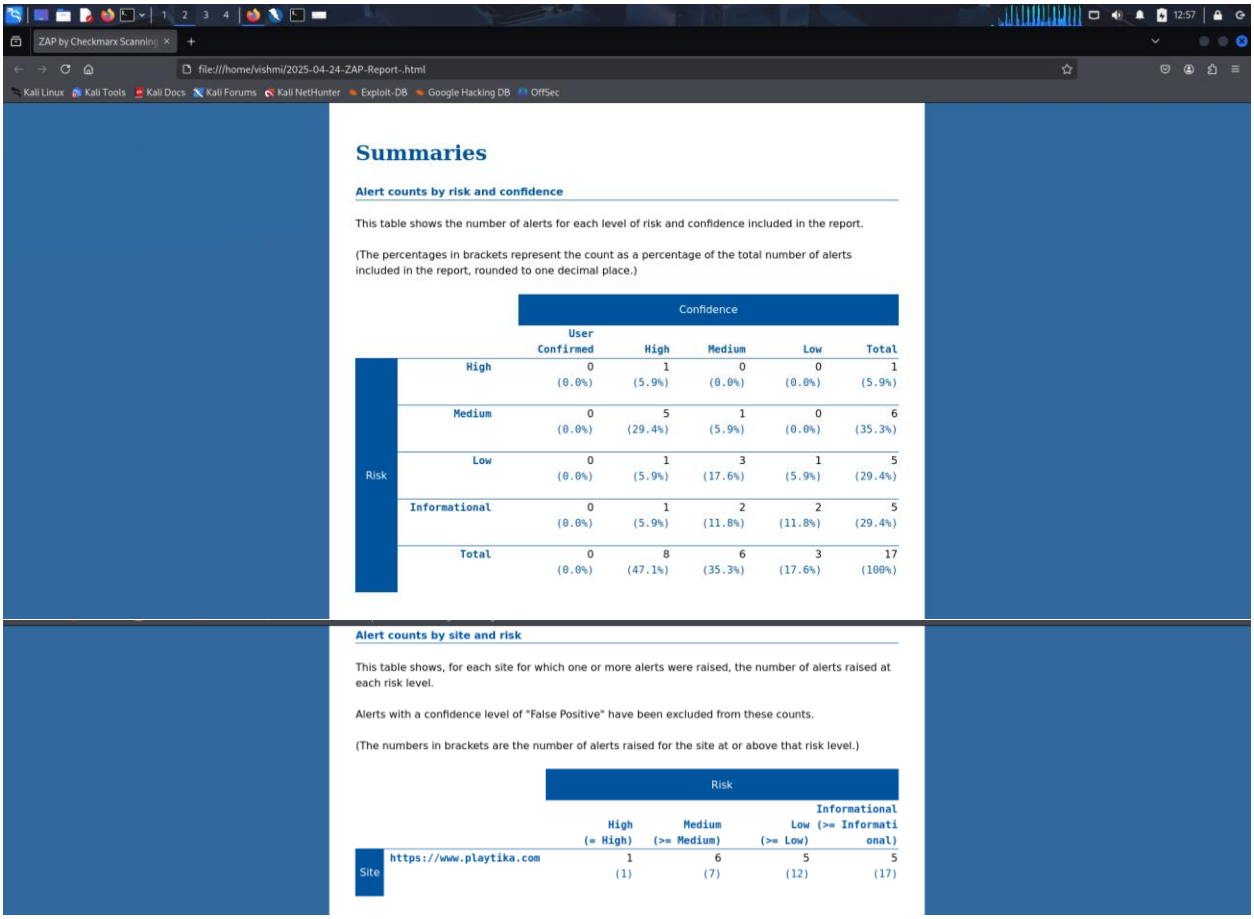
As next step, I entered to the Alerts tab. Here it's detected a vulnerability.



After finishing, it is possible to obtain a thorough report of the results by choosing "Report." The results of scanning many domains are displayed in the screenshots below.

Report = file:///home/vishmi/2025-04-24-ZAP-Report-.html

Please take note that these vulnerabilities have been rated using the OWASP risk rating methodology, which is available at this link.[*OWASP Risk Rating Methodology*]



Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	1 (5.9%)	0 (0.0%)	0 (0.0%)	1 (5.9%)
	Medium	0 (0.0%)	5 (29.4%)	1 (5.9%)	0 (0.0%)	6 (35.3%)
	Low	0 (0.0%)	1 (5.9%)	3 (17.6%)	1 (5.9%)	5 (29.4%)
	Informational	0 (0.0%)	1 (5.9%)	2 (11.8%)	2 (11.8%)	5 (29.4%)
	Total	0 (0.0%)	8 (47.1%)	6 (35.3%)	3 (17.6%)	17 (100%)

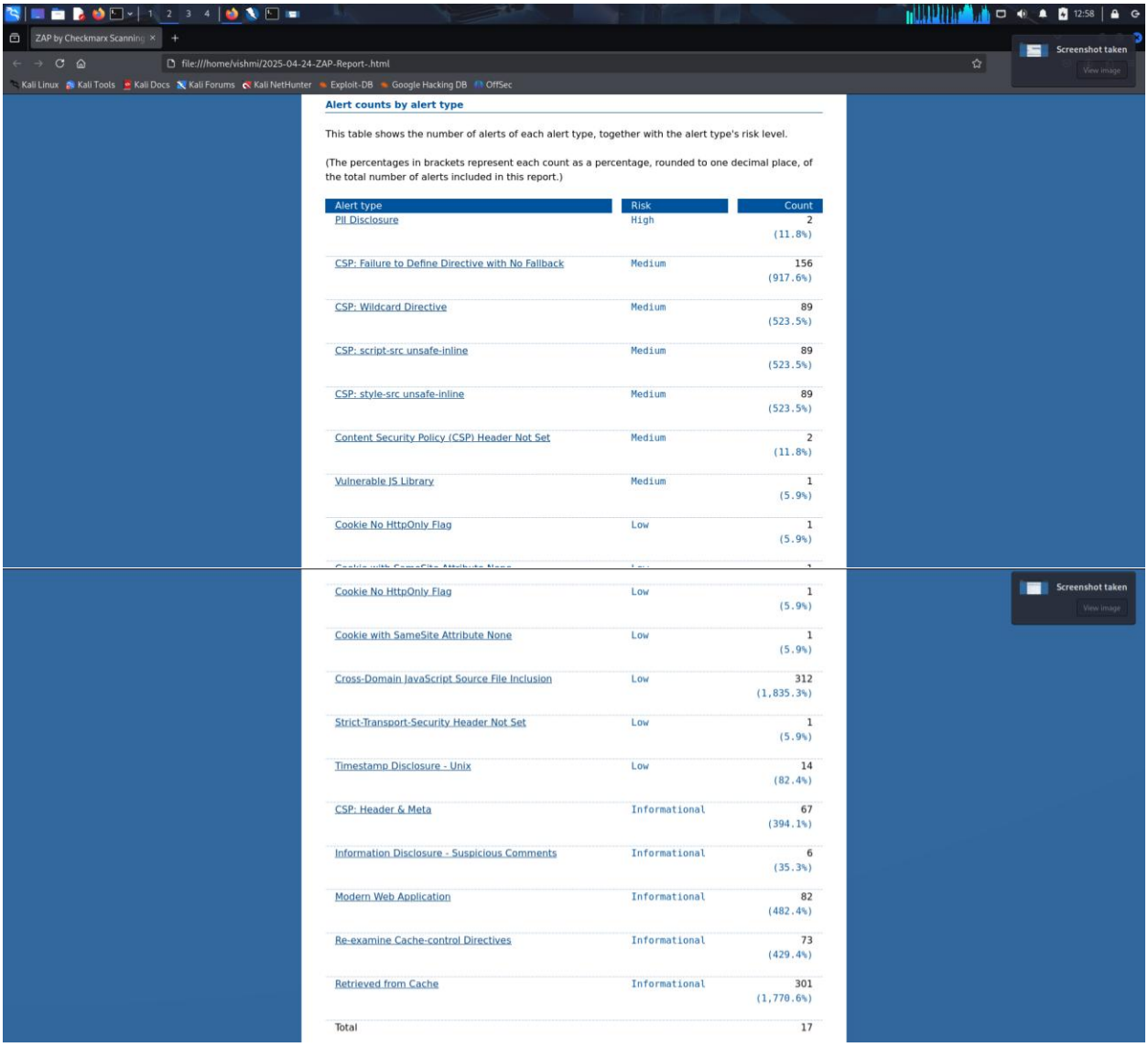
Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://www.playtika.com	1 (1)	6 (7)	5 (12)	5 (17)



Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
PII Disclosure	High	2 (11.8%)
CSP: Failure to Define Directive with No Fallback	Medium	156 (917.6%)
CSP: Wildcard Directive	Medium	89 (523.5%)
CSP: script-src unsafe-inline	Medium	89 (523.5%)
CSP: style-src unsafe-inline	Medium	89 (523.5%)
Content Security Policy (CSP) Header Not Set	Medium	2 (11.8%)
Vulnerable JS Library	Medium	1 (5.9%)
Cookie No HttpOnly Flag	Low	1 (5.9%)
Cookie No HttpOnly Flag	Low	1 (5.9%)
Cookie with SameSite Attribute None	Low	1 (5.9%)
Cross-Domain JavaScript Source File Inclusion	Low	312 (1,835.3%)
Strict-Transport-Security Header Not Set	Low	1 (5.9%)
Timestamp Disclosure - Unix	Low	14 (82.4%)
CSP: Header & Meta	Informational	67 (394.1%)
Information Disclosure - Suspicious Comments	Informational	6 (35.3%)
Modern Web Application	Informational	82 (482.4%)
Re-examine Cache-control Directives	Informational	73 (429.4%)
Retrieved from Cache	Informational	301 (1,770.6%)
Total		17

Vulnerabilities

a.Vulnerability Title	**CSP:Wildcard directive**
b.Vulnerability Description	The Content Security Policy (CSP) is compromised by a configuration error involving a wildcard directive, allowing malicious programs to be inserted and run, thereby compromising its goal of limiting resource loading.
c.Affected Components	HTTP response headers defining the Content Security Policy. Directives like script-src, style-src, img-src, and others using the wildcard (*).
d.Impact Assessment	1.Attackers can insert and run any script thanks to Cross-Site Scripting (XSS) assaults. 2.Theft of data and illegal access to private user data. 3.Phishing, clickjacking, and theft of websites. 4.Application security is generally worse as a result of uncontrolled resource loading.
e.Steps to Reproduce	1.Open the affected website in a browser. 2. Inspect the HTTP response headers using developer tools (F12 → Network tab → Headers). 3.Locate the CSP header and identify any directives that use * (e.g., script-src *). 4. Inject a simple JavaScript payload via an input field or URL parameter to test if the wildcard directive allows execution, such as:html *<script>alert('Vulnerability Confirmed');</script>*
f.Proof of Concept (if applicable)	Create a URL and insert a malicious script into the request body or query parameter, verifying vulnerability if wildcard directive in CSP allows script to run freely.
g.Proposed Mitigation or Fix	Replace wildcard (*) directives with specific, trusted sources. Avoid using *unsafe-inline or unsafe-eval* in CSP directives.

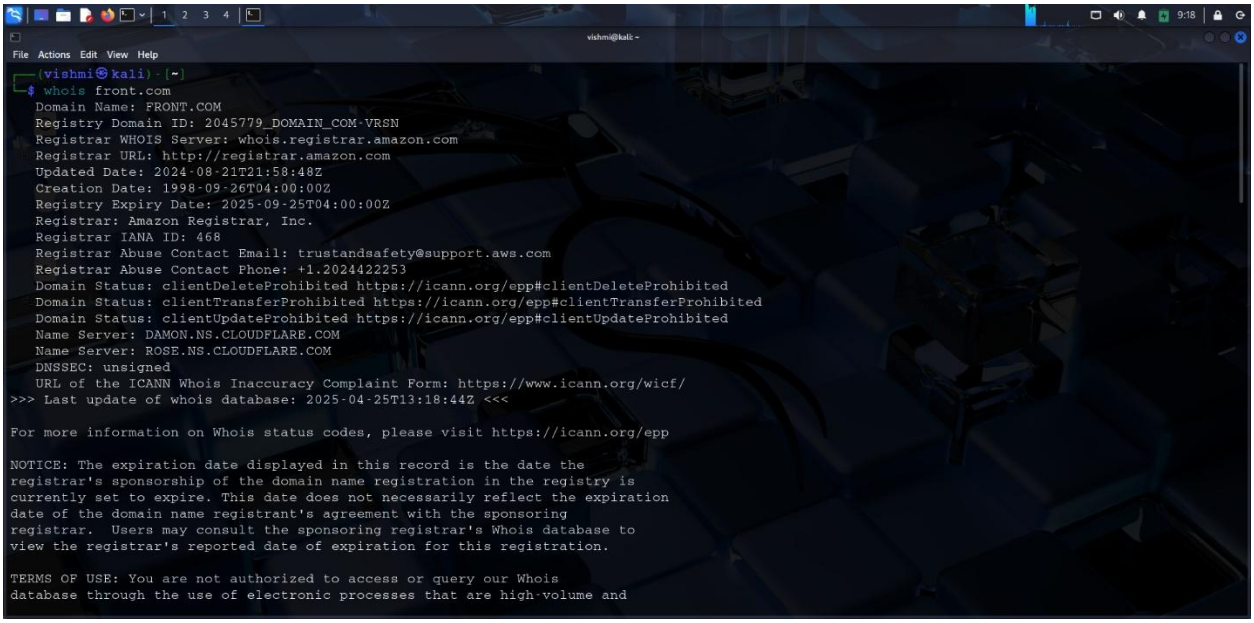
Report-10

Web Audit
front.com

Domain = *front.com*
Sub-domain = *help.front.com*
URL = *https://front.com*

Target Reconnaissance

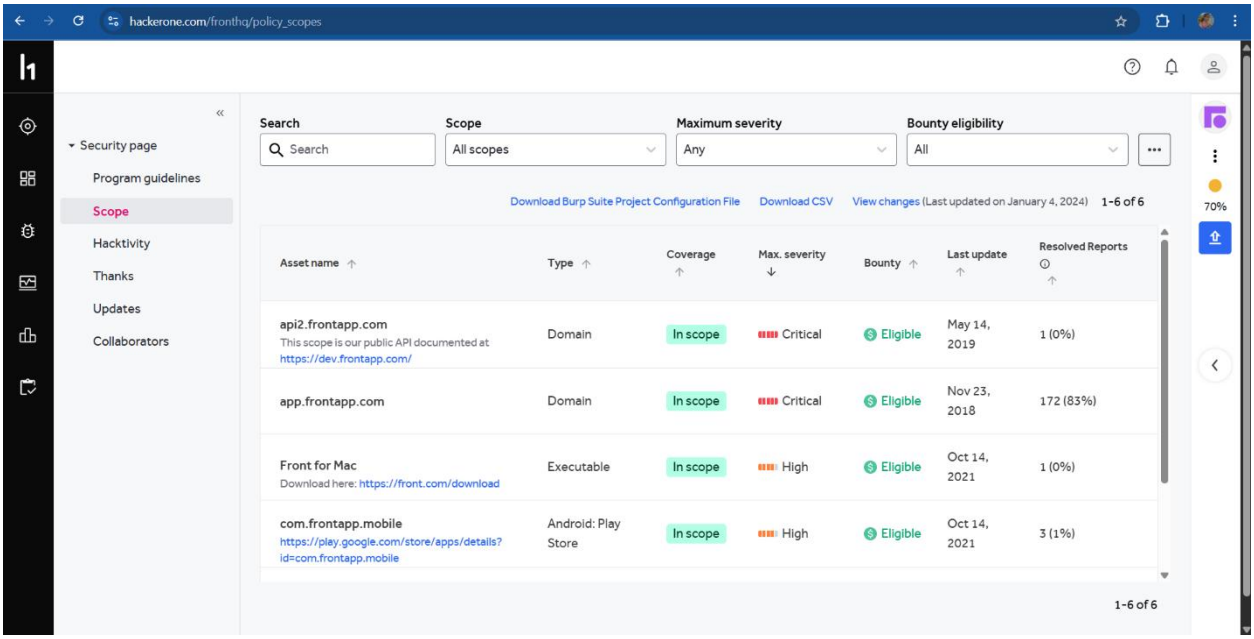
Introduction to Front and Audit Scope.

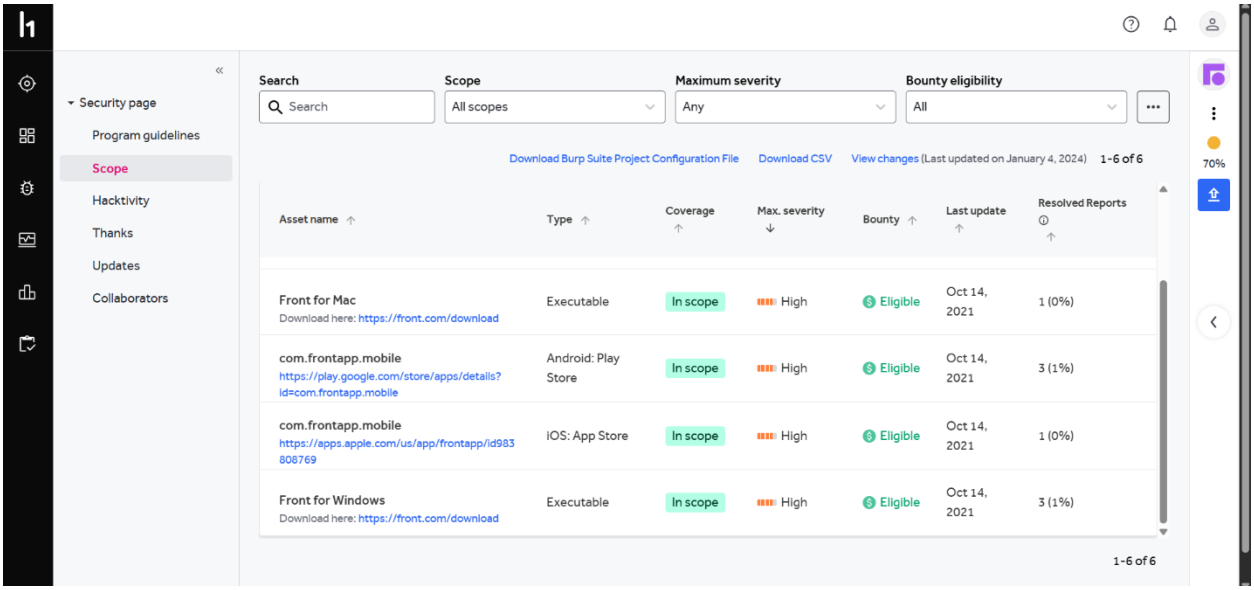


Front is a platform for client communication that combines the strength of a help desk with the ease of use of email. By working together directly on messages, it enables teams to more effectively handle shared inboxes like support@ or sales@. Front helps businesses streamline customer service and sales communications by integrating with systems like Slack, Salesforce, and more. Its primary objective is to improve internal productivity and customer experience by facilitating faster, more individualized, and better team communication.

These subdomains (and all included) have been approved as legitimate subdomains for testing in the **Hackerone** Bug Bounty program.

Eligible in-scope subdomains for bug bounty program are mentioned below.





Information gathering phase.

The information-gathering phase, often known as reconnaissance or recon, is essential to both assessments of security and cyberattacks. In order to map out the target's structure and determine how it functions, the target of this stage is to gather as much information as possible about it. Because it helps auditors or attackers identify vulnerabilities that could be exploited later on, this fundamental understanding is essential.

There are two main approaches to information gathering

1.Active Scanning :

Involves direct interaction with the target, which can generate noticeable activity and typically uncovers a wealth of details about the system.

2Passive Scanning :

Seeks to observe the target without direct engagement, resulting in less detectable activity but often providing more limited information

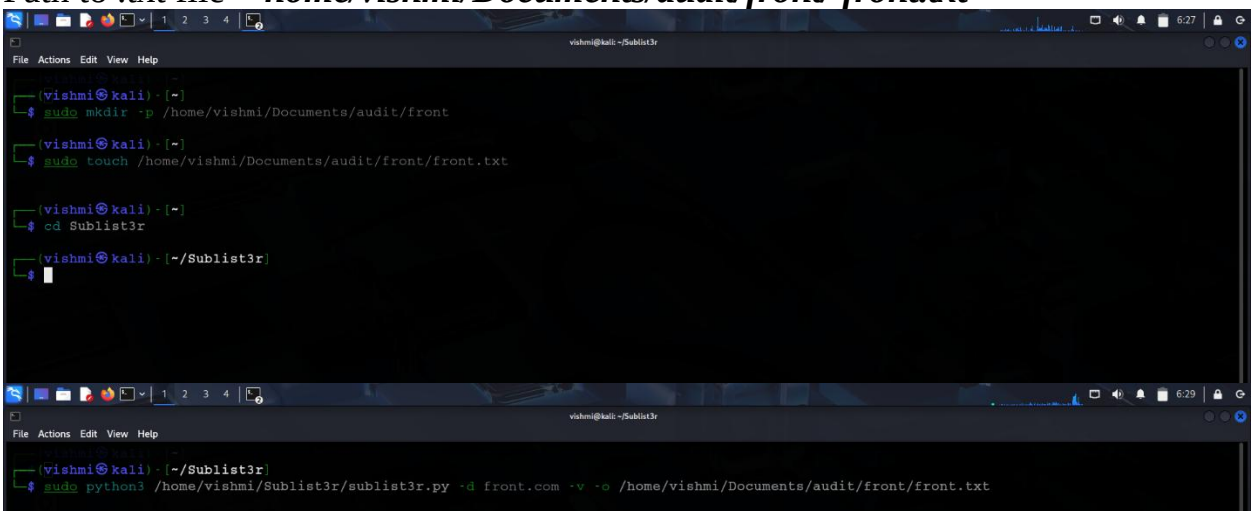
Finding active subdomains and their states

Sublist3r

Sublist3r is an open-source Python application that uses OSINT (Open Source Intelligence) techniques to quickly and effectively scan subdomains. Subdomains linked to a target domain can be found by penetration testers, security researchers, and bug bounty hunters using a variety of search engine queries (including Google, Yahoo, Bing, Baidu, and Ask). Additionally, Sublist3r includes a brute-force module (subbrute) to employ a stronger wordlist to improve the probability of discovering more subdomains.

I created a .txt file to store the subdomain headers that were initiated via sublist3r.

Path to .txt file = ***home/vishmi/Documents/audit/front/ front.txt***



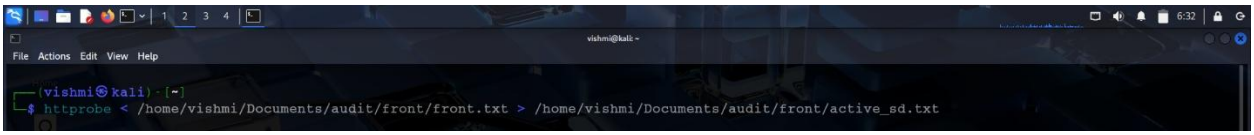
```
                 ____        _     _ _     _____
                / ___| _   _| |__ | (_)___|_   _|__  __ _ _ __ ___
                \___ \| | | | '_ \| | / __| | |/ _ \/ _` | '_ ` _ \
                 ___) | |_| | |_) | | \__ \ | |  __/ (_| | | | | | |
                |____/ \__,_|_.__/|_|_|___/ |_|\___|\__,_|_| |_| |_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for front.com
[-] verbosity is enabled, will show the subdomains results in realtime
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap
    self.run()
    ~~~~~~~~^^
  File "/home/vishmi/Sublist3r/sublist3r.py", line 268, in run
    domain_list = self.enumerate()
  File "/home/vishmi/Sublist3r/sublist3r.py", line 647, in enumerate
    token = self.get_csrftoken(resp)
  File "/home/vishmi/Sublist3r/sublist3r.py", line 641, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
            ~~~~~~~~~~~~~~~~~~~~~~~^^^
```

I got, these subdomains according to the ***front.com*** domain.

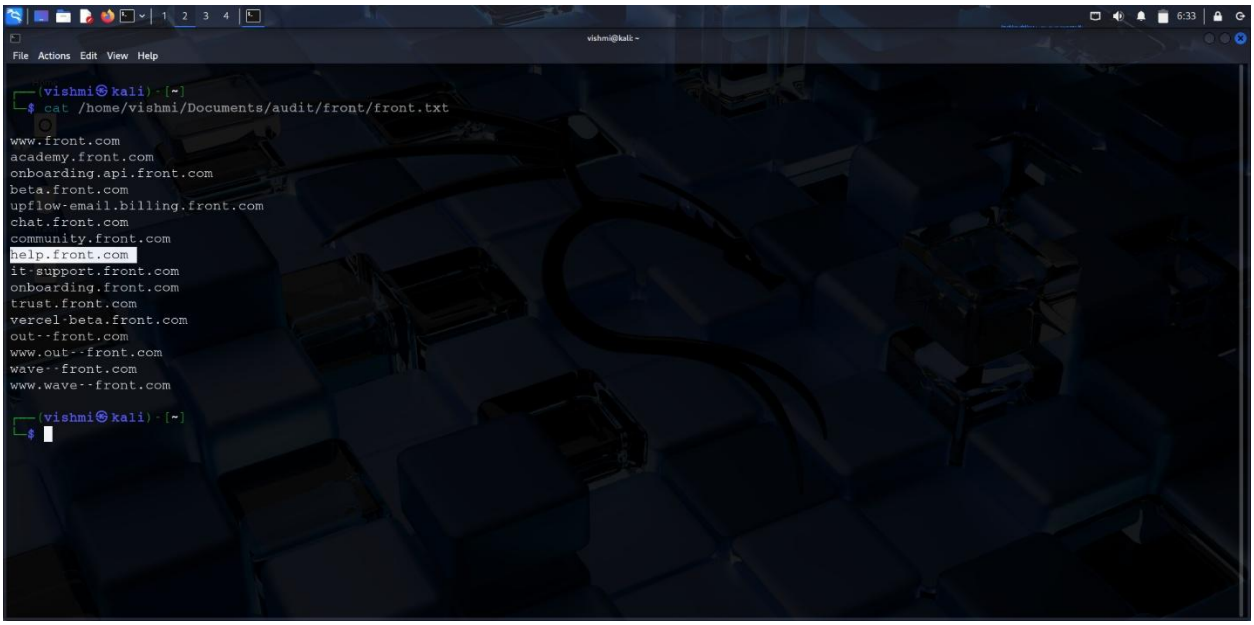
HTTProbe

HTTProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing on achievable goals by providing you with the URLs of active domains.

I am using the text file generated before by the sublist3r and stored the active subdomains to another new .txt file.



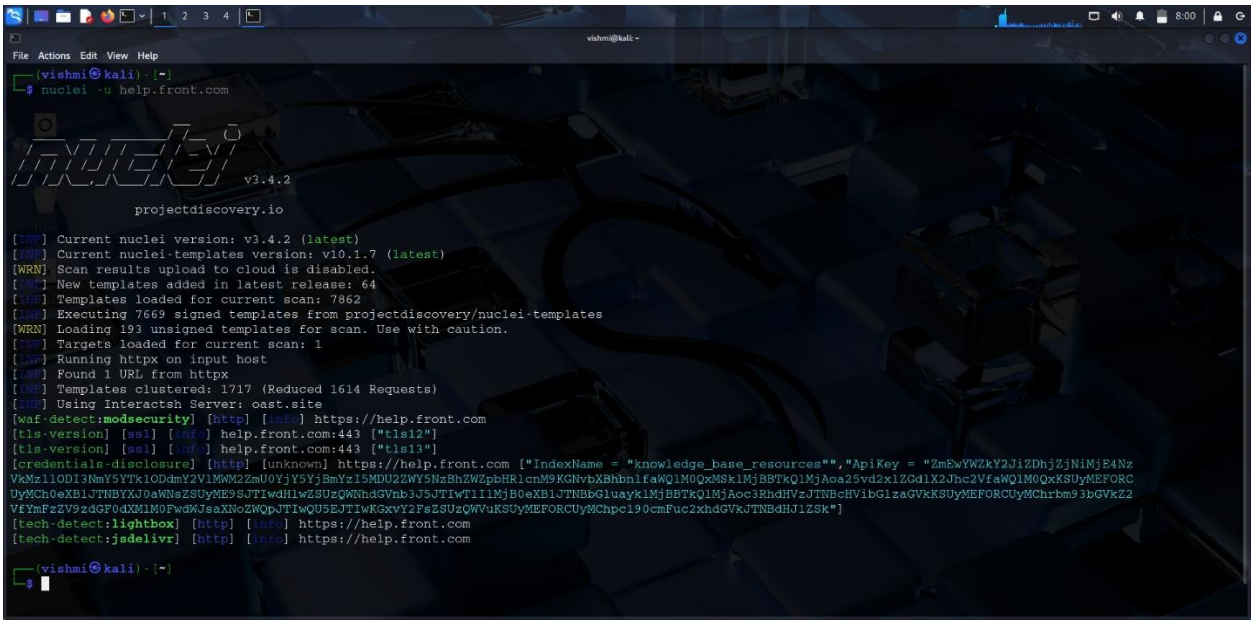
Below, we can see the active subdomains related to the ***front.com*** domain.



To move forward, I chose the active subdomain as **“help.front.com”.**

Nuclei

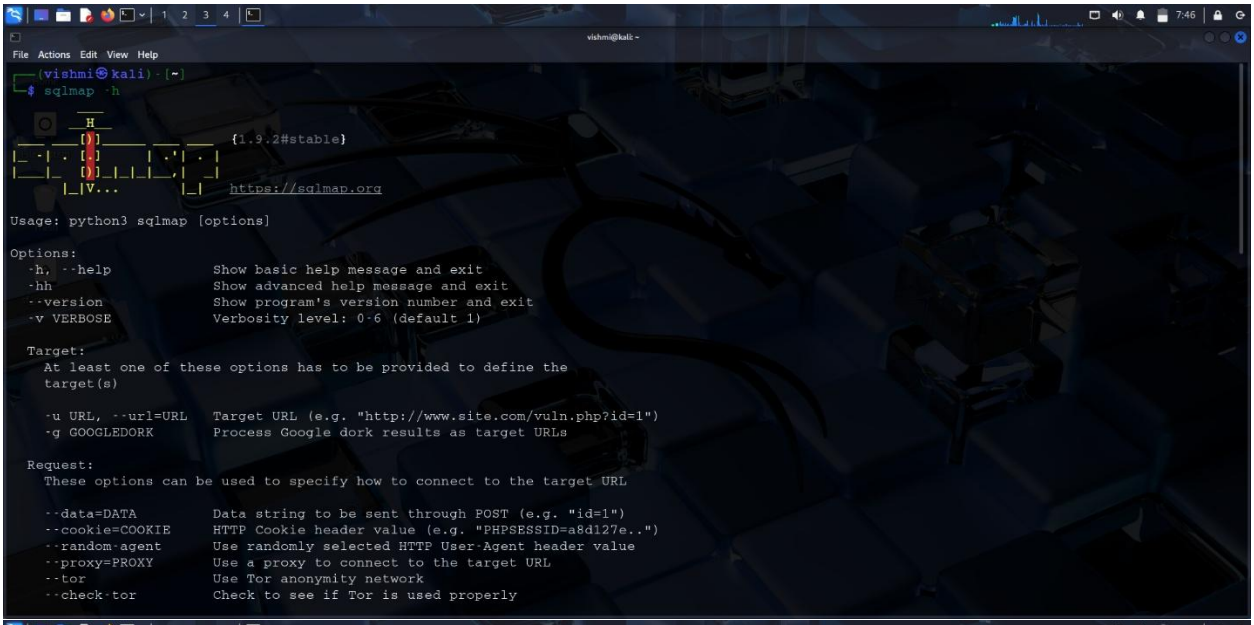
Nuclei is an open-source vulnerability scanner developed by ProjectDiscovery for security professionals, penetration testers, and bug bounty hunters. It uses customizable YAML("Yet Another Markup Language") -based templates to identify vulnerabilities such as misconfigurations, outdated software, and known CVEs (Common Vulnerabilities and Exposures).

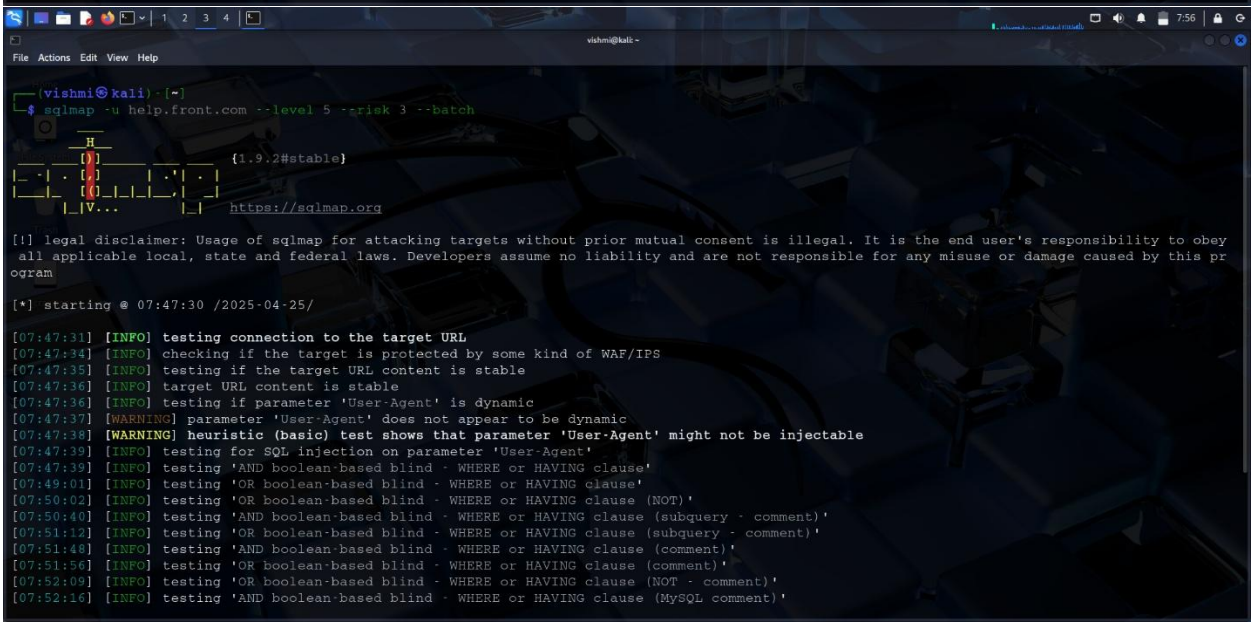


Vulnerability Type	Description	Risk
Modsecurity WAF (Web Application Firewall)	Web firewall detected	Low/ Informational
Tech-detect:lightbox	Possibly allowing illegal access to data or information by implementing weak protections.	Medium
SSL/TLS Certificate Expiry	SSL/TLS certificate expired for go.figma.com:443.	High
Tech-detect:jsdelivr	Outdated or vulnerable JavaScript libraries on jsdelivr can lead to XSS or injection attacks through malicious updates or misconfigurations.	High

SQLmap

An open-source penetration testing tool called SQLmap makes it easier to find and take advantage of SQL injection flaws in web apps. If the database permits, it can even access the underlying file system or run commands on the server in addition to identifying the type of database and extracting data. Security experts frequently use it to evaluate and protect web apps from SQL injection attacks.





Option	Meaning
-u	For basic testing, the target URL is required.
--level5	Increases the number of payloads and tests that are done (maximum is 5).
--risk3	Increase the danger level of the payloads used (maximum is 3)
--batch	Executes SQLMap in a non-interactive mode, selecting default responses automatically.

Detected Information

* ***[WARNING] heuristic (basic) test shows that parameter 'User-Agent' might be injectable***

[This is a *potential* vulnerability, but not confirmed.]

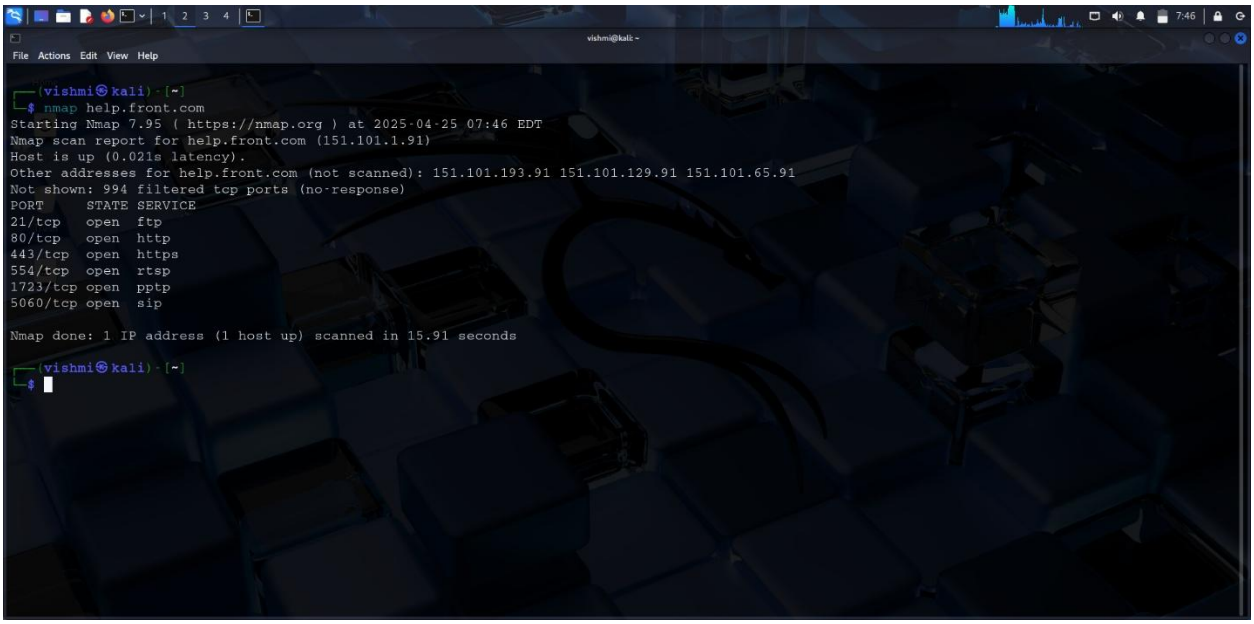
* ***[INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'***

[SQLmap is still in the process of testing for SQL injection using Boolean-based techniques.]

Searching for vulnerabilities

Nmap

Nmap (Network Mapper) is a strong, open-source network scanning program that uses packet transmission and response analysis to find hosts and services on a computer network. To find open ports, running services, operating systems, and active devices on a network, network managers and security experts utilize Nmap. Network inventory, vulnerability assessment, security auditing, and penetration testing are among its many uses.



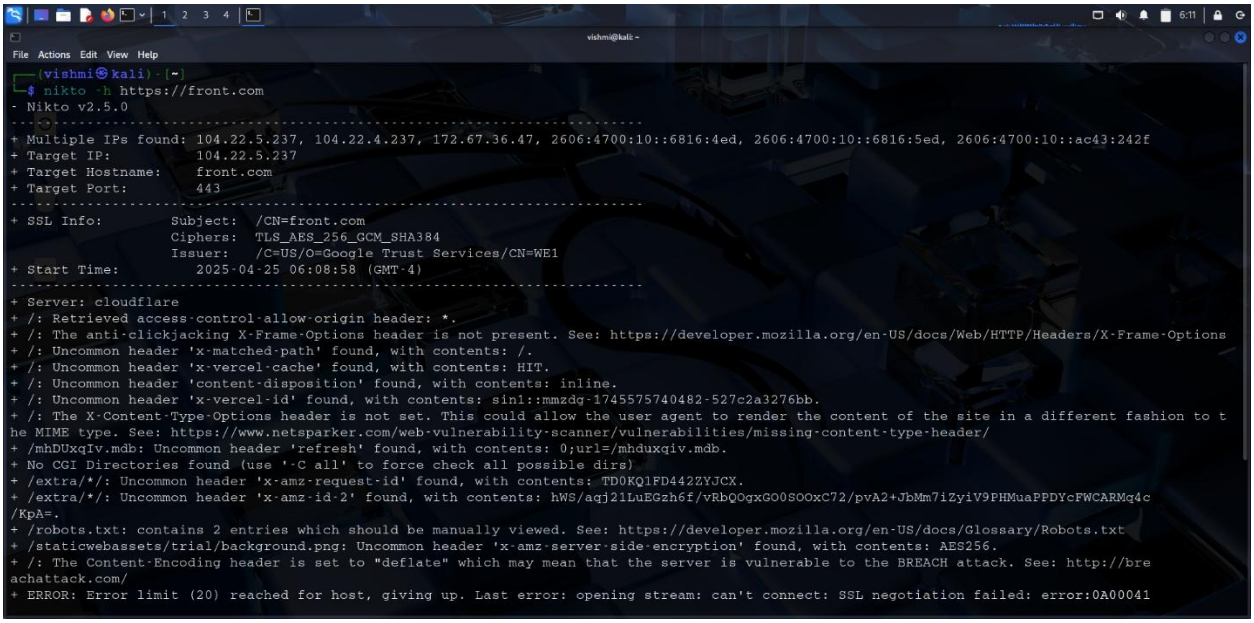
I discovered these details by using Nmap to search *help.front.com.*

PORT	STATE	SERVICE
21/tcp	open	ftp
80/tcp	open	http
443/tcp	open	https
554/tcp	open	rtsp
1723/tcp	open	pptp
5060/tcp	open	sip

PORT	SERVICE	Vulnerabilities
21/tcp	ftp	Unencrypted credentials are accepted.
80/tcp	http	Transmits plain text data.
443/tcp	https	Deprecated TLS versions are supported.
554/tcp	Rtsp	Usually doesn't have authenticity.
1723/tcp	pptp	Makes use of a weak encryption
5060/tcp	sip	Susceptible to spoofing and DoS due to lack of encryption.

Nikto

An open-source program called Nikto scans web servers for common vulnerabilities, malicious files, outdated software, and improperly configured settings, among other potential security issues. It is widely used for penetration testing and assessments, but it functions best when combined with other tools.



Security issues found on ***https://front.com's*** by Nikto Scan

*The anti-clickjacking X-Frame-Options header is not present.

*Uncommon header 'x-matched-path' found.

*Uncommon header 'x-vercel-cache' found.

*Uncommon header 'content-disposition' found.

**Uncommon header 'x-vercel-id', 'x-matched-path' found.

*Uncommon header 'x-vercel-cache' found.

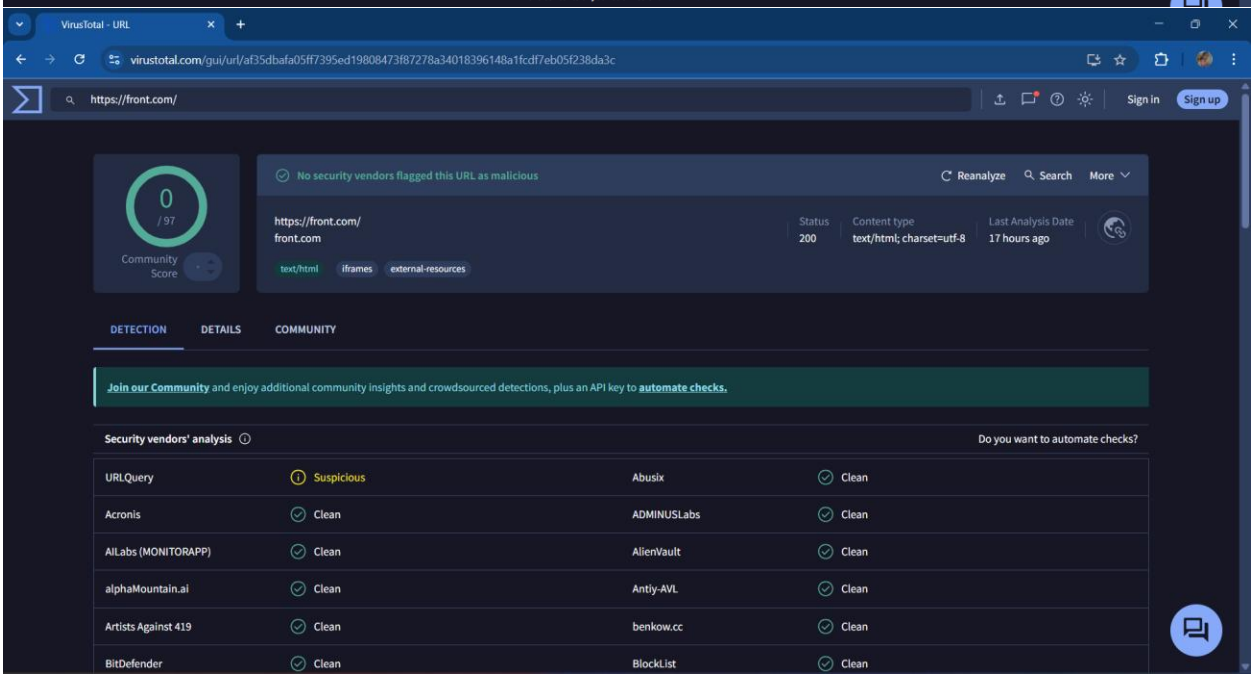
*Uncommon header 'content-disposition' and 'x-vercel-id' found.

*No CGI Directories found.

Virustotal

Virustotal is a free web service called VirusTotal employs 70 antivirus engines and URL blocklisting services to scan files and URLs for malware, adware, and other malicious content.

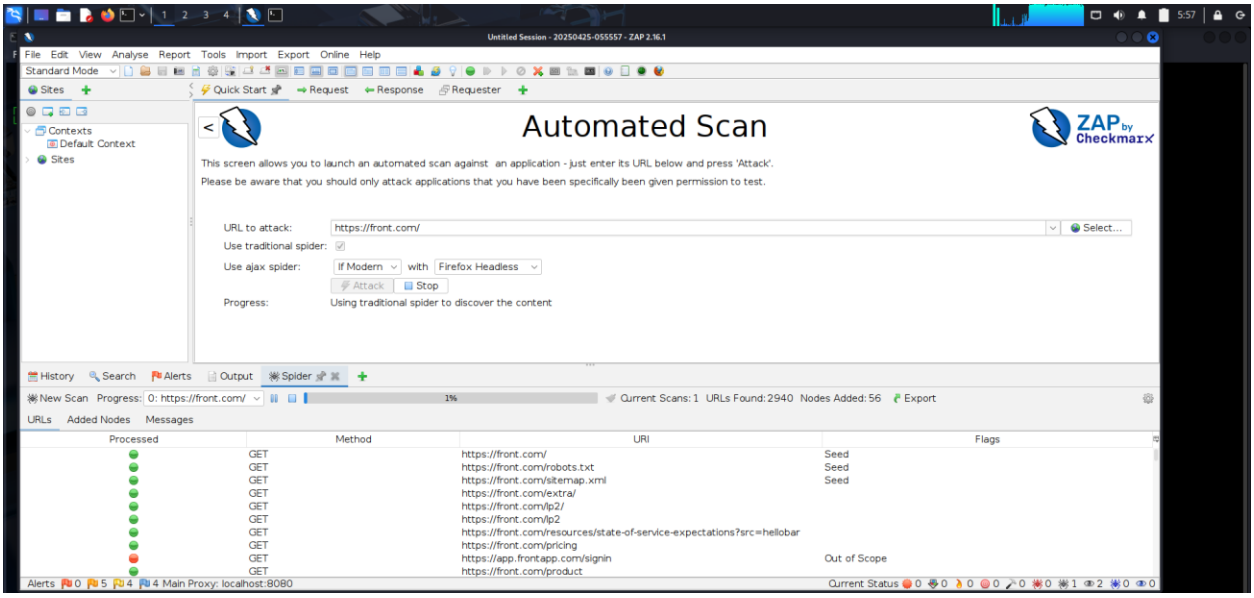
I entered https://front.com in URL section .



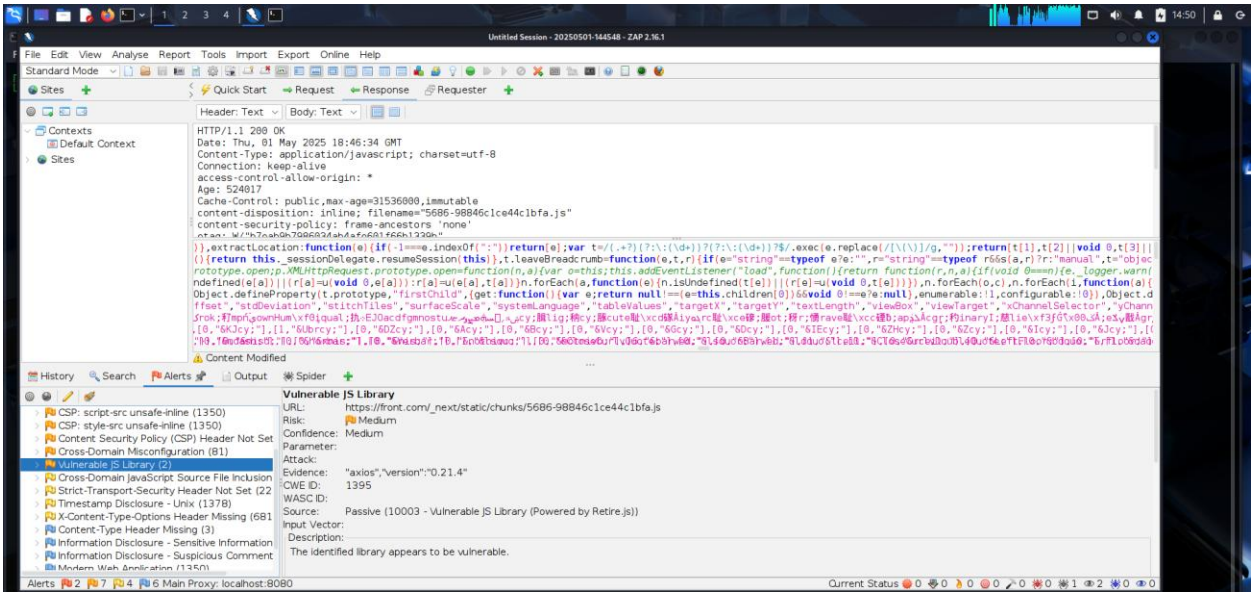
OWASP ZAP

A free and open-source security tool called ***OWASP ZAP (Zed Attack Proxy)*** simulates attacks and examines how an application behaves when it is running to help in discovering and fixing vulnerabilities in web applications.

In here, I entered the target URL [***https://front.com***] designated textbox, simply select "Attack" to initiate the scanning process.



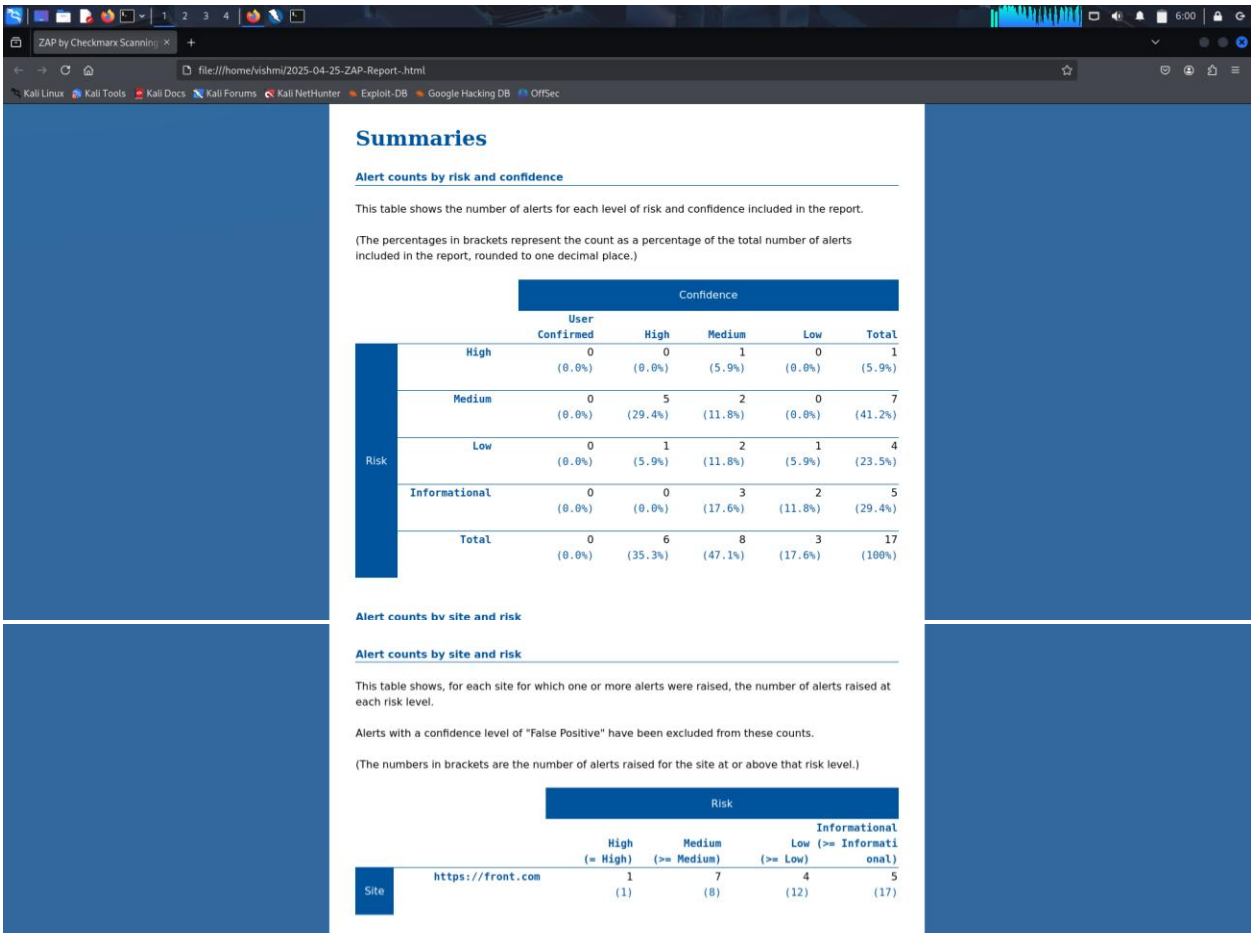
As next step, I entered to the Alerts tab. Here it's detected a vulnerability.



After finishing, it is possible to obtain a thorough report of the results by choosing "Report." The results of scanning many domains are displayed in the screenshots below.

Report = file:///home/vishmi/2025-04-25-ZAP-Report-.html

Please take note that these vulnerabilities have been rated using the OWASP risk rating methodology, which is available at this link.[*OWASP Risk Rating Methodology*]



Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	1 (5.9%)	0 (0.0%)	1 (5.9%)
	Medium	0 (0.0%)	5 (29.4%)	2 (11.8%)	0 (0.0%)	7 (41.2%)
	Low	0 (0.0%)	1 (5.9%)	2 (11.8%)	1 (5.9%)	4 (23.5%)
	Informational	0 (0.0%)	0 (0.0%)	3 (17.6%)	2 (11.8%)	5 (29.4%)
	Total	0 (0.0%)	6 (35.3%)	8 (47.1%)	3 (17.6%)	17 (100%)

Alert counts by site and risk

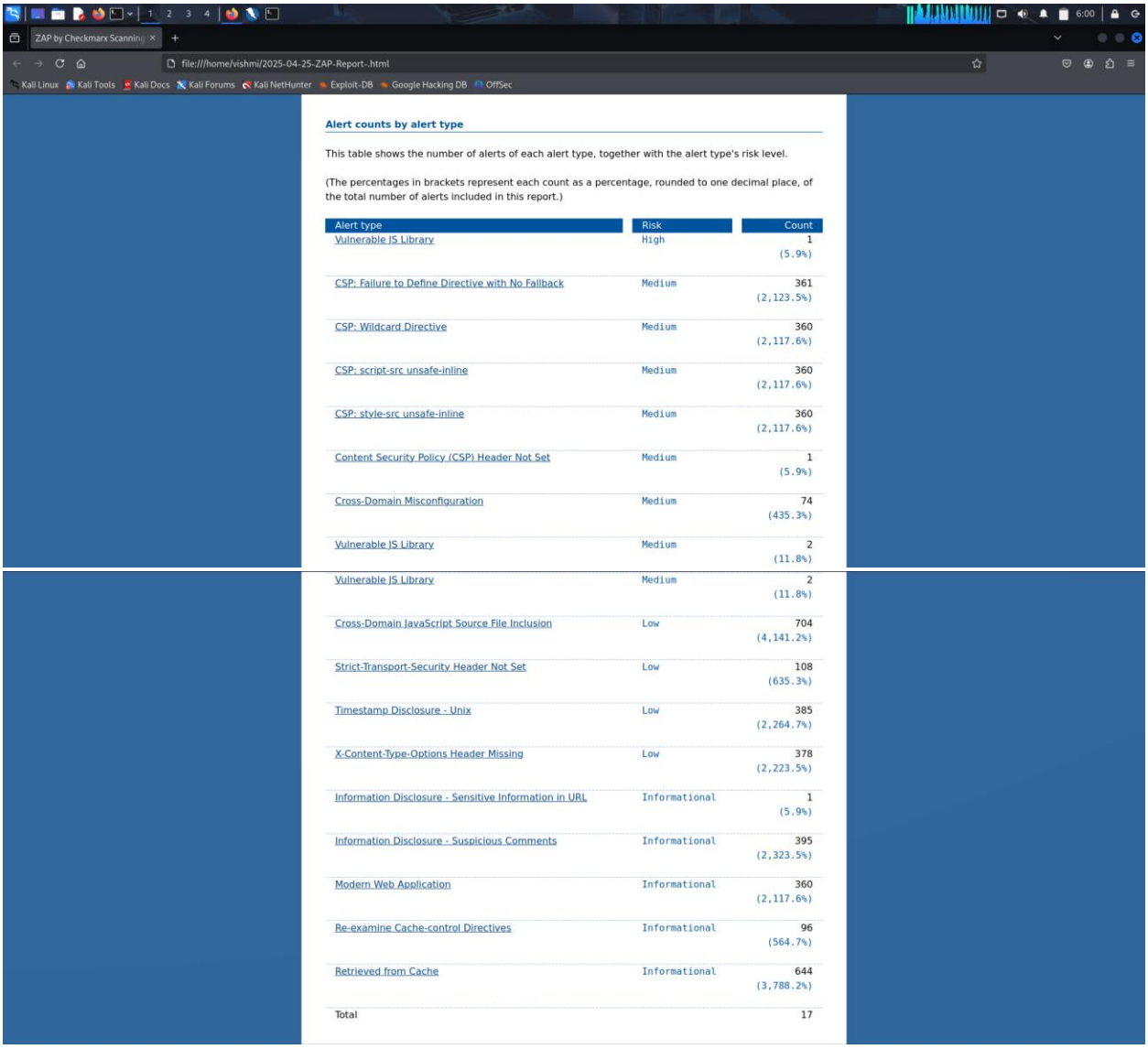
Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://front.com	1 (1)	7 (8)	4 (12)	5 (17)



Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Vulnerable JS Library	High	1 (5.9%)
CSP: Failure to Define Directive with No Fallback	Medium	361 (2,123.5%)
CSP: Wildcard Directive	Medium	360 (2,117.6%)
CSP: script-src unsafe-inline	Medium	360 (2,117.6%)
CSP: style-src unsafe-inline	Medium	360 (2,117.6%)
Content Security Policy (CSP) Header Not Set	Medium	1 (5.9%)
Cross-Domain Misconfiguration	Medium	74 (435.3%)
Vulnerable JS Library	Medium	2 (11.8%)
Vulnerable JS Library	Medium	2 (11.8%)
Cross-Domain JavaScript Source File Inclusion	Low	704 (4,141.2%)
Strict-Transport-Security Header Not Set	Low	108 (635.3%)
Timestamp Disclosure - Unix	Low	385 (2,264.7%)
X-Content-Type-Options Header Missing	Low	378 (2,223.5%)
Information Disclosure - Sensitive Information in URL	Informational	1 (5.9%)
Information Disclosure - Suspicious Comments	Informational	395 (2,323.5%)
Modern Web Application	Informational	360 (2,117.6%)
Re-examine Cache-control Directives	Informational	96 (564.7%)
Retrieved from Cache	Informational	644 (3,788.2%)
Total		17

Vulnerabilities

a.Vulnerability Title	**Vulnerable JavaScript Library(Axios v0.21.4)**
b.Vulnerability Description	The application's Axios JavaScript library version (v0.21.4) is vulnerable to security flaws, increasing the attack surface and potentially affecting data integrity.
c.Affected Components	https://front.com/_next/static/chunks/5686-98846c1ce44c1bfa.js
d.Impact Assessment	Client-side application security and user confidence can be weakened by security misconfigurations and Man-in-the-middle MITM attack vectors that result in data manipulation or leaking.
e.Steps to Reproduce	1. Start OWASP ZAP, then crawl the application (in this case, https://front.com). 2. Find the "Vulnerable JS Library" notice under the "Alerts" tab. 3. Examine the information indicating that Axios version="0.21.4" is marked as problematic. 4. Use *Retire.js* to compare this version to known vulnerabilities.
f.Proof of Concept (if applicable)	Select the alert associated with the JS chunk *5686-98846c1ce44c1bfa.js* after opening ZAP. Verify the Axios version that is vulnerable in the metadata that Retire.js provides. Open the JS file or look for version metadata in the headers to manually check the library version.
g.Proposed Mitigation or Fix	Regularly update the Axios library, audit third-party libraries, and incorporate dependency checking tools like Retire.js, Snyk, or npm audit into your CI/CD process to avoid vulnerabilities.

Challenges

Even though the experience was quite satisfying there were some difficulties along the way. At first, understanding a domain's scope felt difficult, and it took continual care to make sure testing remained within permitted bounds. Another difficulty was writing thorough and expert bug reports, which required accuracy, clarity, and a thorough understanding of the vulnerabilities. It required a lot of time and practice to become proficient with several tools because of their steep stages of learning. While automatic techniques occasionally overlooked minor problems that only human inspection could detect, manual testing frequently seemed tiresome and required patience. Another ability that required constant development was the ability to explain findings in a way that both technical and non-technical stakeholders could understand.

Also ,effective time management and regular monitoring of daily progress were personal challenges.

Benefits of Participating in Bug Bounty

- Testing live websites for vulnerabilities gave me practical experience.
- Improved practical abilities important to the cybersecurity industry.
- Learned the ability to write professional and clear bug bounty reports.
- Identified how to appropriately define and respect a domain's limits.
- Utilized a variety of cybersecurity tools and technologies with effectiveness.
- Both automatic and manual testing methods were balanced.
- Examined and examined possible solutions for vulnerabilities found.
- Developed a better knowledge of vulnerabilities and how they behave.
- Web application behavior in various contexts was observed and examined.

CONCLUSION

Starting this bug bounty adventure has been a significant and hugely fulfilling experience. I have learned more about threat analysis, web application security, and the importance of ongoing monitoring in securing digital environments as a result of this approach. This experience confirmed the value of dedication, curiosity, and flexibility in the ever-changing field of cyber security.

In addition to improving my technical ability, each vulnerability found, and problem fixed has highlighted the duty we bear as guardians of the digital environment. This encounter encourages a lifetime dedicated to education, development, and promoting a safer online environment for everybody.

REFERENCES

1. https://owasp.org/www-project-top-ten/

2. https://hackerone.com/opportunities/all

3. https://www.youtube.com/watch?v=bf2YuqgaeWo&list=PLH8n_ayg-60J9i3nsLybper-DR3zJw6Z5

4. https://github.com/sqlmapproject/sqlmap/wiki/usage

5. https://owasp.org/www-community/vulnerabilities/

6. https://www.yeswehack.com/learn-bug-bounty/write-effective-bug-bounty-reports