

# **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 .....	3 <sup>Z</sup>
PURPOSE.....	4
Chapter 1: OWASP Top 10 Vulnerabilities .....	5
Chapter 2: Select a Program and Creating an Account .....	9
Chapter 3: Reconnaissance On The Target.....	10
Sublist3r.....	10
Httpprobe .....	11
Nuclei.....	12
SQLmap .....	13
Chapter 4:Searching for Vulnerabilities.....	15
Nmap .....	15
Nikto .....	16
Virustotal .....	17
OWASP ZAP .....	19
Report-01.....	21
Vulnerabilities.....	43
Report-02.....	44
Vulnerabilities .....	62
Report-03.....	63
Vulnerabilities .....	80
Report-04.....	81
Vulnerabilities .....	98
Report-05.....	99
Vulnerabilities .....	116
Report-06.....	117
Vulnerabilities .....	133
Report-07.....	134
Vulnerabilities .....	150
Report-08.....	151
Vulnerabilities .....	168
Report-09.....	169
Vulnerabilities .....	186
Report-10.....	187
Vulnerabilities .....	205
Challenges.....	206
Benefits of Participating in Bug Bounty.....	207
CONCLUSION .....	208
REFERENCES .....	209

# 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

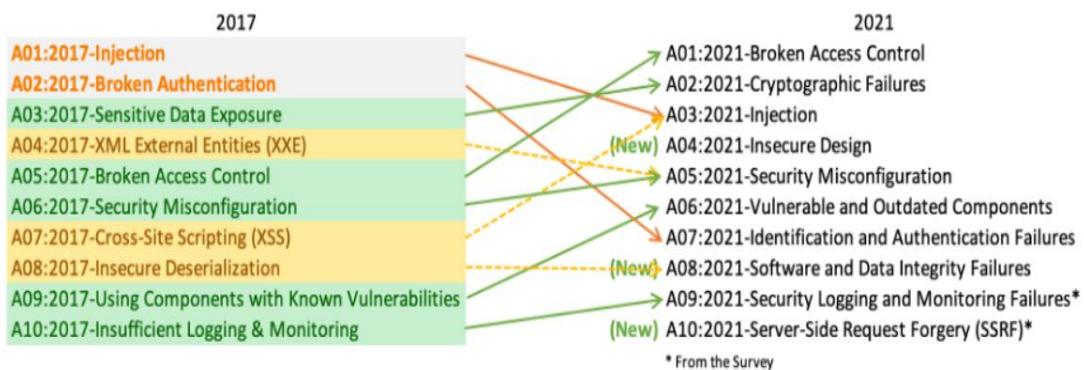
The objective of this assignment is to have a deeper understanding of web application vulnerabilities and effective mitigation techniques. We identified 10 vulnerabilities in 10 sub-domains by choosing a domain from bug bounty platforms such as **Bugcrowd**, **HackerOne**, or **Intigriti**. The objective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

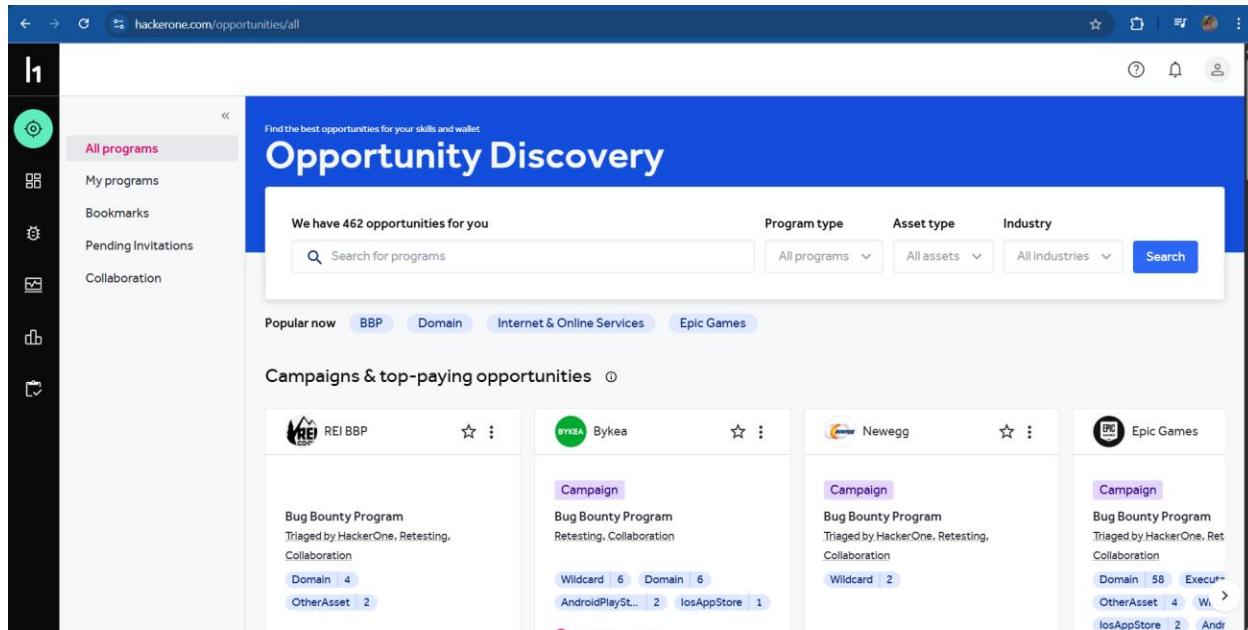
## **10. Server-side Request Forgery**

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

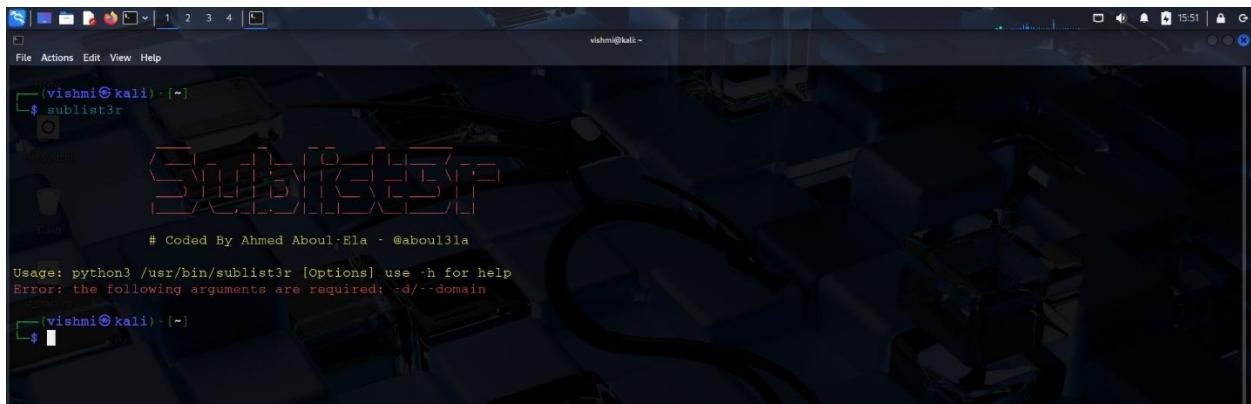
Before beginning my bug bounty journey, I thoroughly researched the various platforms and programs. Among them are **Intigriti**, **Bugcrowd**, and **HackerOne**. Knowing that the caller and variety of programs offered would affect the efficacy of my bug-hunting efforts, I spent some time researching 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



```
vishmi㉿kali:~$ sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la
Usage: python3 /usr/bin/sublist3r [Options] use -h for help
Error: the following arguments are required: -d/--domain
```

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.

## Httpprobe



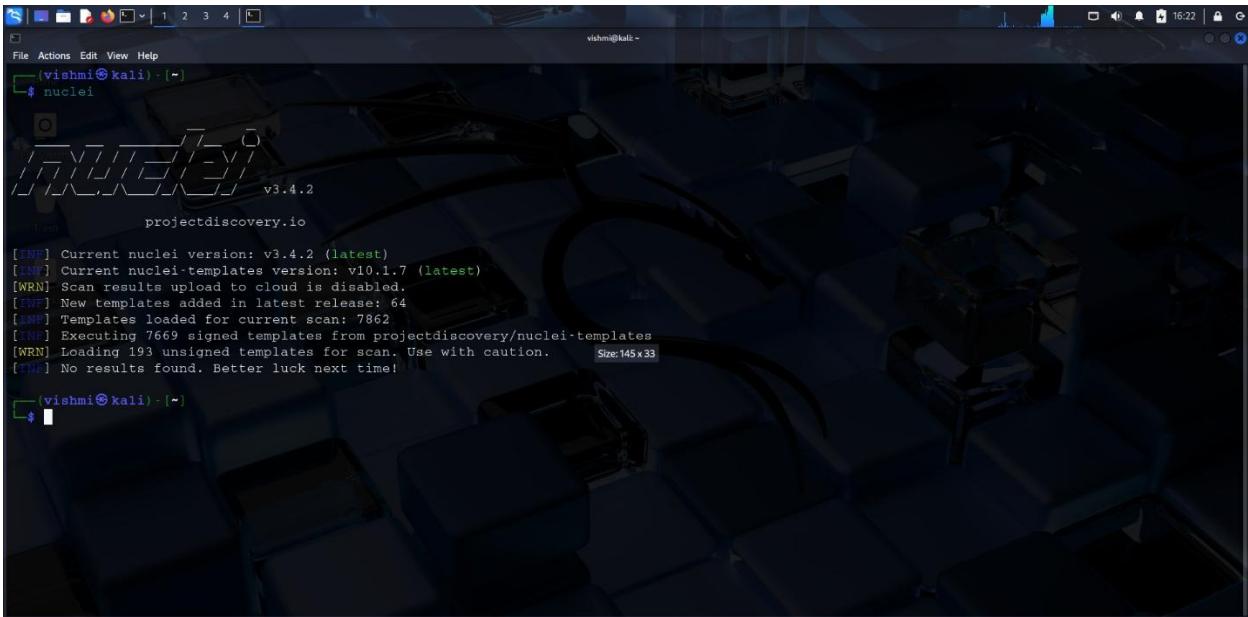
The screenshot shows a terminal window on a Kali Linux desktop. The terminal has two command-line sessions. The first session runs the command `httpprobe < /home/vishmi/Documents/audit/lichess/lichess.txt > /home/vishmi/Documents/audit/lichess/active_sd.txt`. The second session displays the contents of the file `/home/vishmi/Documents/audit/lichess/lichess.txt`, which lists various subdomains of lichess.org.

```
vishmi@kali:~$ httpprobe < /home/vishmi/Documents/audit/lichess/lichess.txt > /home/vishmi/Documents/audit/lichess/active_sd.txt
(vishmi@kali:~$ cat /home/vishmi/Documents/audit/lichess/lichess.txt
www/lichess.org
af/lichess.org
alerta/lichess.org
ar/lichess.org
as/lichess.org
az/lichess.org
be/lichess.org
bg/lichess.org
bn/lichess.org
```

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



```
vishmi㉿kali ~
$ nuclei
v3.4.2
projectdiscovery.io

[INF] Current nuclei version: v3.4.2 (latest)
[INF] Current nuclei-templates version: v10.1.7 (latest)
[NRN] Scan results upload to cloud is disabled.
[PRW] New templates added in latest release: 64
[LNT] Templates loaded for current scan: 7862
[ENI] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[NRN] Loading 193 unsigned templates for scan. Use with caution. Size:145x33
[TNL] No results found. Better luck next time!

(vishmi㉿kali) ~
```

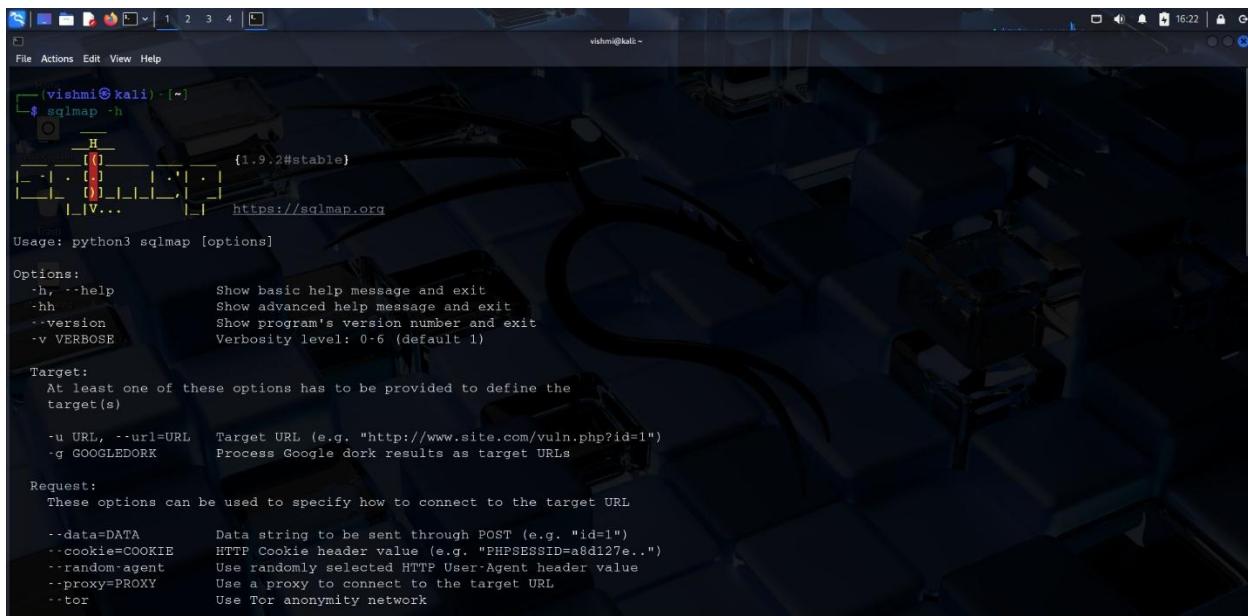
Nuclei is a robust vulnerability scanner that scans for known vulnerabilities through customizable YAML(Yet Another Markup Language) templates. It enables fast and automated scanning for exposures, misconfigurations, and CVEs(Common Vulnerabilities and Exposures). It is perfect for integrating into automated 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.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is '(vishmi㉿kali)'. The command \$ sqlmap -h is run, displaying the SQLmap help menu. The menu includes:

- Usage: python3 sqlmap [options]
- Options:
  - h, --help Show basic help message and exit
  - hh Show advanced help message and exit
  - version Show program's version number and exit
  - v VERBOSE Verbosity level: 0-6 (default 1)
- Target:
  - At least one of these options has to be provided to define the target(s)
  - u URL, --url=URL Target URL (e.g. "http://www.site.com/vuln.php?id=1")
  - g GOOGLEDORK Process Google dork results as target URLs
- Request:
  - These options can be used to specify how to connect to the target URL
  - data=DATA Data string to be sent through POST (e.g. "id=1")
  - cookie=COOKIE HTTP Cookie header value (e.g. "PHPSESSID=a8d127e...")
  - random-agent Use randomly selected HTTP User-Agent header value
  - proxy=PROXY Use a proxy to connect to the target URL
  - tor Use Tor anonymity network

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



```
vishmi㉿kali: ~$ nmap af.lichess.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 18:42 EDT
Nmap scan report for af.lichess.org (37.187.205.99)
Host is up (0.027s latency).
Other addresses for af.lichess.org (not scanned): 2001:41d0:307:b200::
rDNS record for 37.187.205.99: lichess.org
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https

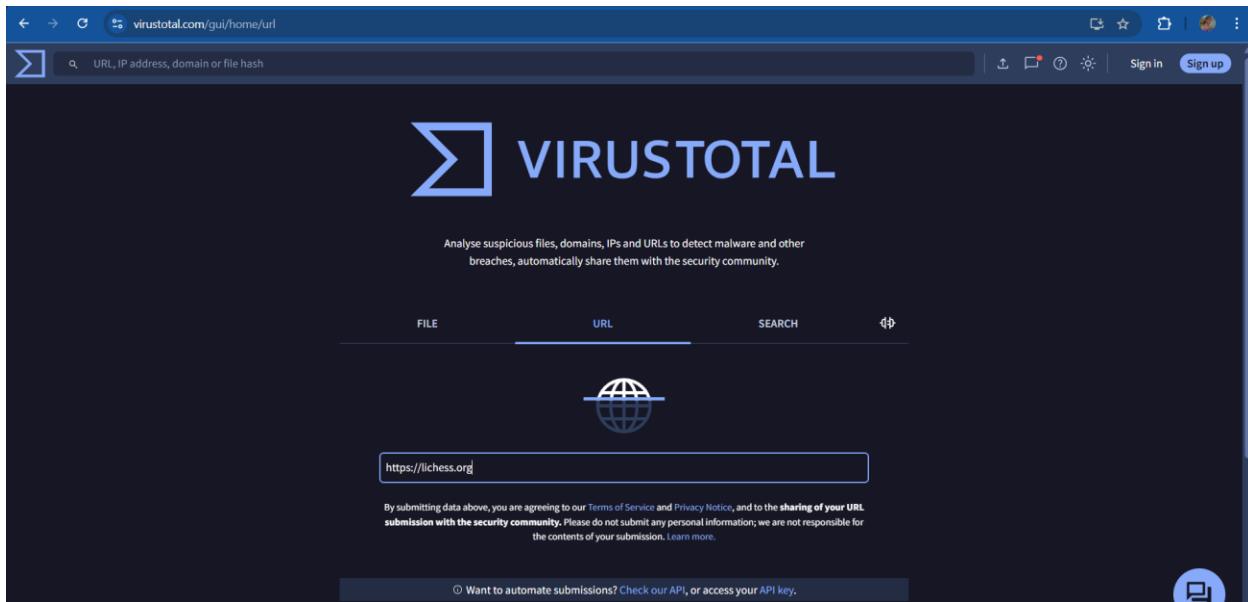
Nmap done: 1 IP address (1 host up) scanned in 9.68 seconds
vishmi㉿kali: ~$
```

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.

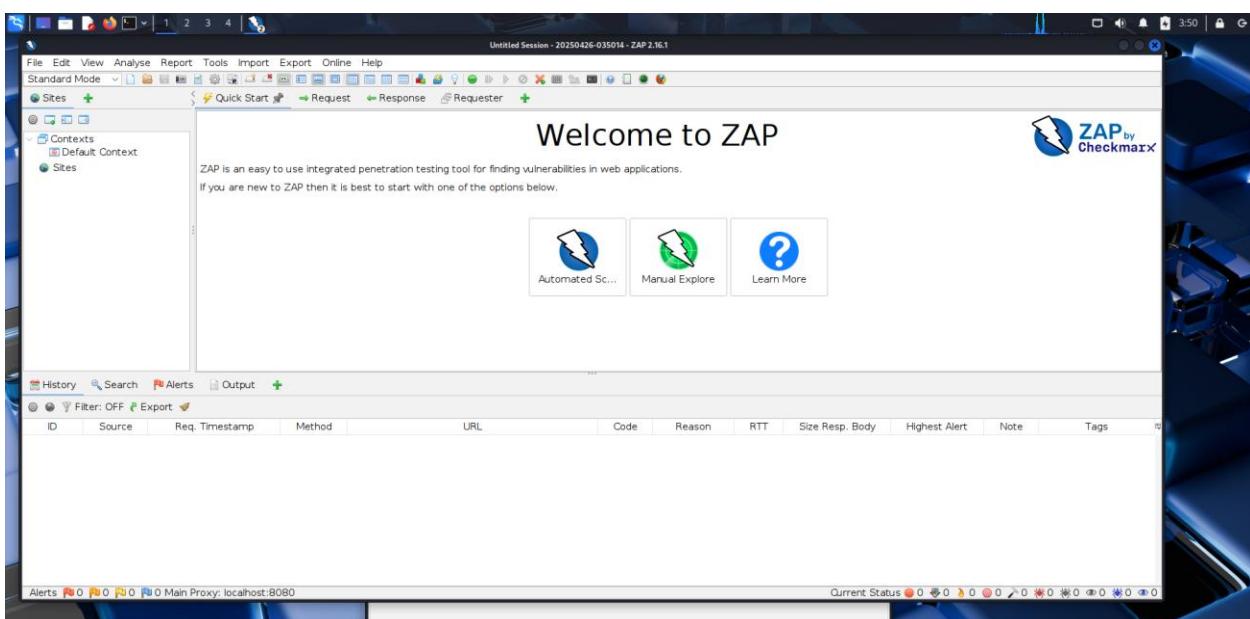
OWASP ZAP

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.

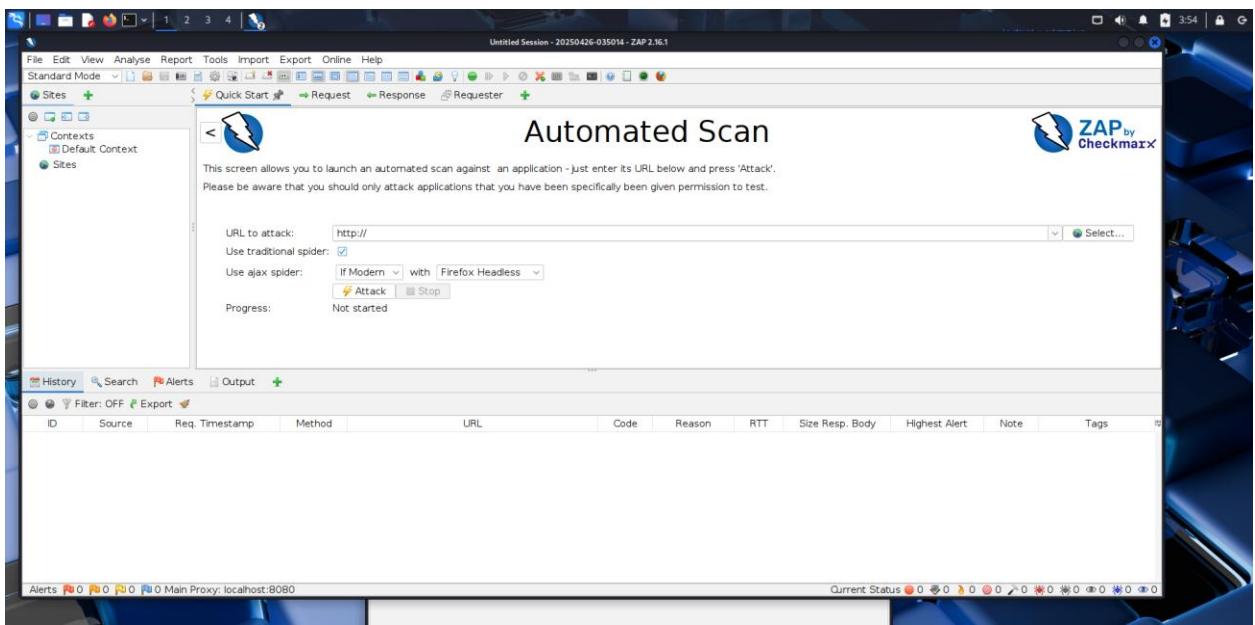
First, we should install “**Zaproxy**” in kali.

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*

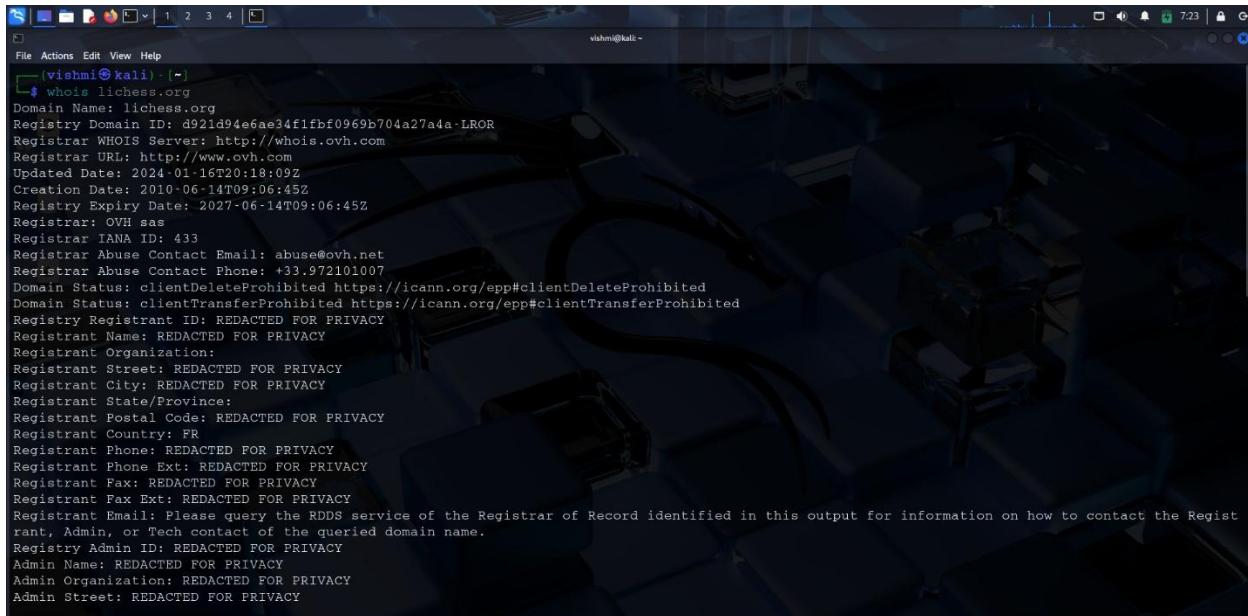
**Domain** = *lichess.org*

**Sub-domain** = *af.lichess.org*

**URL** = *https://lichess.org*

# Target Reconnaissance

## Introduction to Lichess and Audit Scope



```
(vishni㉿kali)-[~]
$ whois lichess.org
Domain Name: lichess.org
Registry Domain ID: d921d94e6ae34f1fb0969b704a27a4a-LROR
Registrar WHOIS Server: http://whois.ovh.com
Registrar URL: http://www.ovh.com
Updated Date: 2024-01-16T20:18:09Z
Creation Date: 2010-06-14T09:06:45Z
Registry Expiry Date: 2027-06-14T09:06:45Z
Registrar: OVH sas
Registrar IANA ID: 433
Registrar Abuse Contact Email: abuse@ovh.net
Registrar Abuse Contact Phone: +33.972101007
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization:
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: FR
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
```

“**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

The screenshot shows a web browser displaying the Lichess Vulnerability Disclosure page at [hackerone.com/lichess/policy\\_scopes](https://hackerone.com/lichess/policy_scopes). The page lists 54 eligible in-scope subdomains. The columns include Asset name, Type, Coverage, Max. severity, Bounty, Last update, and Resolved Reports. Most subdomains are marked as In scope with Critical severity and Ineligible for bounty. Some have Medium severity and 0% resolved reports.

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
socket.lichess.org	Domain	In scope	■■■ Critical	⌚ Ineligible	Oct 2, 2020	0 (0%)
socket1.lichess.org	Domain	In scope	■■■ Critical	⌚ Ineligible	Oct 2, 2020	0 (0%)
socket2.lichess.org	Domain	In scope	■■■ Critical	⌚ Ineligible	Oct 2, 2020	1 (2%)
socket3.lichess.org	Domain	In scope	■■■ Critical	⌚ Ineligible	Oct 2, 2020	0 (0%)
lichess.org	Domain	In scope	■■■ Critical	⌚ Ineligible	Oct 2, 2020	32 (70%)
database.lichess.org	Domain	In scope	■■■■ Medium	⌚ Ineligible	Oct 2, 2020	0 (0%)
explorer.lichess.ovh	Domain	In scope	■■■■ Medium	⌚ Ineligible	Oct 2, 2020	0 (0%)
syrup.lichess.ovh	Domain	In scope	■■■■ Medium	⌚ Ineligible	Oct 2, 2020	0 (0%)
tablebase.lichess.ovh	Domain	In scope	■■■■ Medium	⌚ Ineligible	Oct 2, 2020	0 (0%)
taffy.lichess.ovh	Domain	In scope	■■■■ Medium	⌚ Ineligible	Oct 2, 2020	0 (0%)
terra.lichess.ovh	Domain	In scope	■■■■ Medium	⌚ Ineligible	Oct 2, 2020	1 (2%)
uluru.lichess.ovh	Domain	In scope	■■■■ Medium	⌚ Ineligible	Oct 2, 2020	0 (0%)

# **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

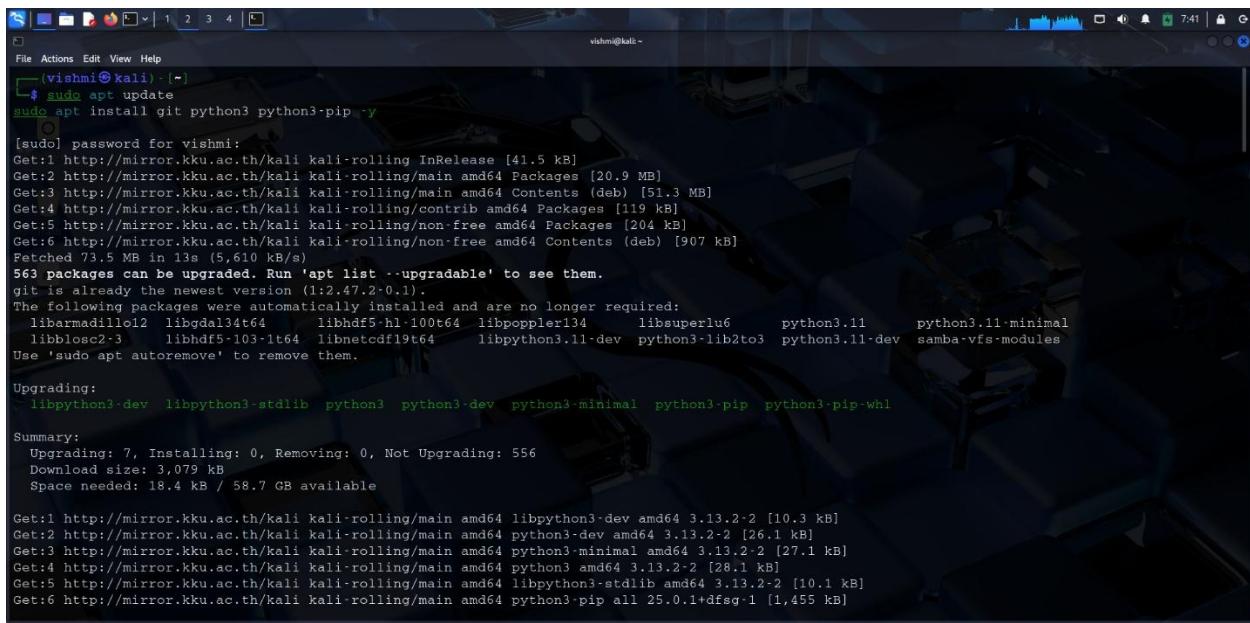
# Finding active subdomains and their states

## 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*”**



```
vishmi@kali:~$ sudo apt update
[vishmi@kali:~]$ sudo apt install git python3 python3-pip -y
[sudo] password for vishmi:
Get:1 http://mirror.kku.ac.th/kali kali-rolling InRelease [41.5 kB]
Get:2 http://mirror.kku.ac.th/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://mirror.kku.ac.th/kali kali-rolling/main amd64 Contents (deb) [51.3 MB]
Get:4 http://mirror.kku.ac.th/kali kali-rolling/contrib amd64 Packages [119 kB]
Get:5 http://mirror.kku.ac.th/kali kali-rolling/non-free amd64 Packages [204 kB]
Get:6 http://mirror.kku.ac.th/kali kali-rolling/non-free amd64 Contents (deb) [907 kB]
Fetched 73.5 MB in 13s (5,610 kB/s)
563 packages can be upgraded. Run 'apt list --upgradable' to see them.
git is already the newest version (1:2.47.2-0.1).
The following packages were automatically installed and are no longer required:
  libarmadillo2  libgdal3dt64  libhdf5-hl-100t64  libpoppler134  libsuperlu6  python3.11  python3.11-minimal
  libblosc2-3  libhdf5-103-1t64  libnetcdf19t64  libpython3.11-dev  python3.1b2t03  python3.11-dev  samba-vfs-modules
Use 'sudo apt autoremove' to remove them.

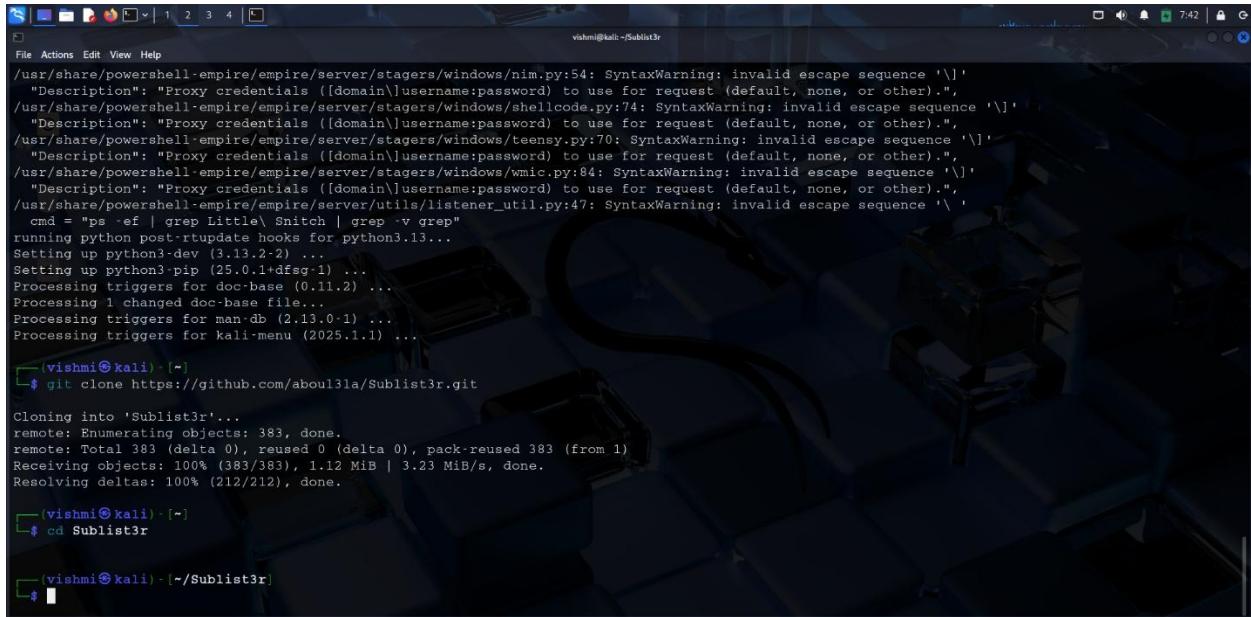
Upgrading:
  libpython3-dev  libpython3-stdlib  python3  python3-dev  python3-minimal  python3-pip  python3-pip-whl

Summary:
  Upgrading: 7, Installing: 0, Removing: 0, Not Upgrading: 556
  Download size: 3,079 kB
  Space needed: 18.4 kB / 58.7 GB available

Get:1 http://mirror.kku.ac.th/kali kali-rolling/main amd64 libpython3-dev amd64 3.13.2-2 [10.3 kB]
Get:2 http://mirror.kku.ac.th/kali kali-rolling/main amd64 python3-dev amd64 3.13.2-2 [26.1 kB]
Get:3 http://mirror.kku.ac.th/kali kali-rolling/main amd64 python3-minimal amd64 3.13.2-2 [27.1 kB]
Get:4 http://mirror.kku.ac.th/kali kali-rolling/main amd64 python3 amd64 3.13.2-2 [28.1 kB]
Get:5 http://mirror.kku.ac.th/kali kali-rolling/main amd64 libpython3-stdlib amd64 3.13.2-2 [10.1 kB]
Get:6 http://mirror.kku.ac.th/kali kali-rolling/main amd64 python3-pip all 25.0.1+dfsg-1 [1,455 kB]
```

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>”**



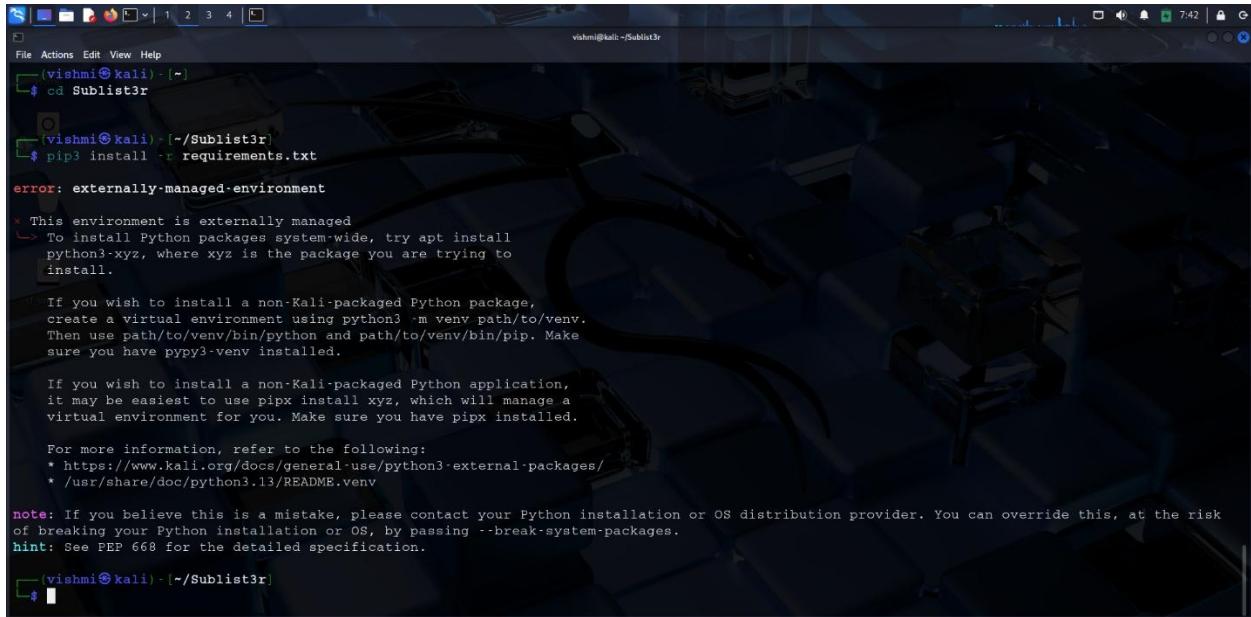
```
vishmi@kali:~/Sublist3r
File Actions Edit View Help
/usr/share/powershell-empire/server/stagers/windows/nim.py:54: SyntaxWarning: invalid escape sequence '\\'
  "Description": "Proxy credentials ([domain]username:password) to use for request (default, none, or other).",
/usr/share/powershell-empire/server/stagers/windows/shellcode.py:74: SyntaxWarning: invalid escape sequence '\\'
  "Description": "Proxy credentials ([domain]username:password) to use for request (default, none, or other).",
/usr/share/powershell-empire/server/stagers/windows/teensy.py:70: SyntaxWarning: invalid escape sequence '\\'
  "Description": "Proxy credentials ([domain]username:password) to use for request (default, none, or other).",
/usr/share/powershell-empire/server/stagers/windows/wmic.py:84: SyntaxWarning: invalid escape sequence '\\'
  "Description": "Proxy credentials ([domain]username:password) to use for request (default, none, or other).",
/usr/share/powershell-empire/server/stagers/windows/listener_util.py:47: SyntaxWarning: invalid escape sequence '\\'
  "Description": "Proxy credentials ([domain]username:password) to use for request (default, none, or other)."
cmd = "ps -ef | grep Little\ Snitch | grep -v grep"
running python post-rtupdate hooks for python3.13...
Setting up python3-dev (3.13.2.2) ...
Setting up python3-pip (25.0.1+dfsg-1) ...
Processing triggers for doc-base (0.11.2) ...
Processing 1 changed doc-base file...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...

[vishmi@kali: ~]
$ git clone https://github.com/aboul3la/Sublist3r.git
Cloning into 'Sublist3r'...
remote: Enumerating objects: 383, done.
remote: Total 383 (delta 0), reused 0 (delta 0), pack-reused 383 (from 1)
Receiving objects: 100% (383/383) 1.12 MiB | 3.23 MiB/s, done.
Resolving deltas: 100% (212/212), done.

[vishmi@kali: ~]
$ cd Sublist3r
[vishmi@kali: ~/Sublist3r]
$
```

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

**“pip3 install -r requirements.txt “**



```
vishmi㉿kali:~/Sublist3r
$ cd Sublist3r
(vishmi㉿kali) - [~]
$ pip3 install -r requirements.txt

error: externally-managed-environment

* This environment is externally managed
  To install Python packages system-wide, try apt install
  python3-xyz, where xyz is the package you are trying to
  install.

If you wish to install a non-Kali-packaged Python package,
create a virtual environment using python3 -m venv path/to/venv.
Then use path/to/venv/bin/python and path/to/venv/bin/pip. Make
sure you have pypy3-venv installed.

If you wish to install a non-Kali-packaged Python application,
it may be easiest to use pipx install xyz, which will manage a
virtual environment for you. Make sure you have pipx installed.

For more information, refer to the following:
 * https://www.kali.org/docs/general-use/python3-external-packages/
 * /usr/share/doc/python3.13/README.venv

note: If you believe this is a mistake, please contact your Python installation or OS distribution provider. You can override this, at the risk
of breaking your Python installation or OS, by passing --break-system-packages.
hint: See PEP 668 for the detailed specification.

(vishmi㉿kali) - [~/Sublist3r]
$
```

After installing the requirements, enter

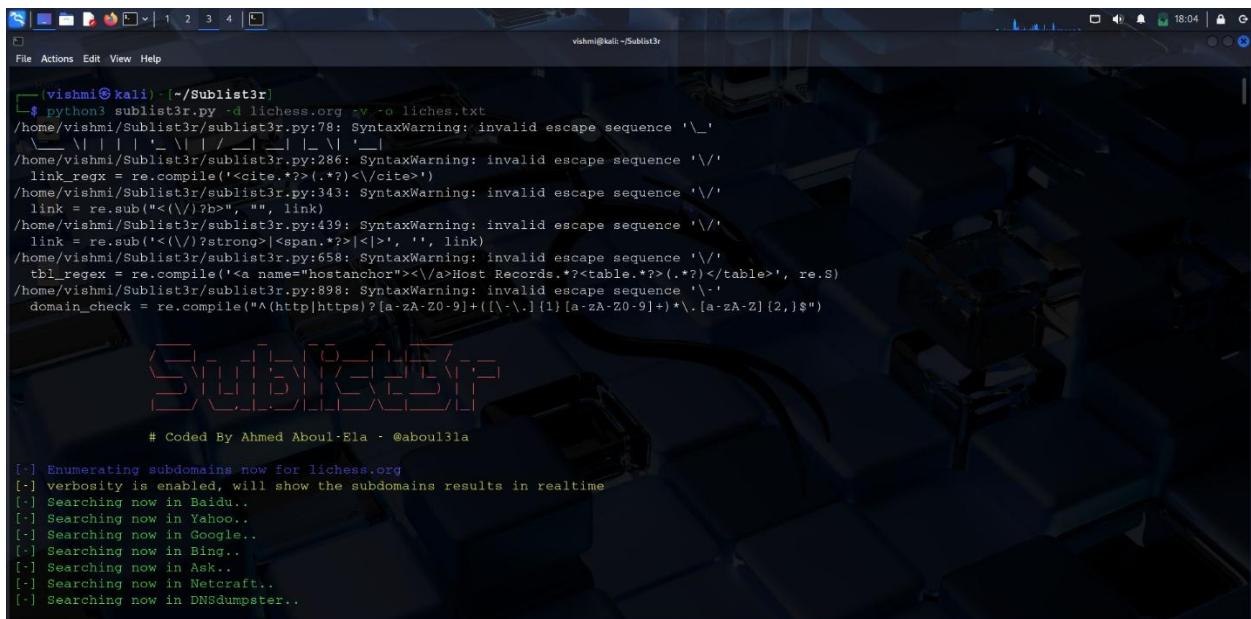
*python3 sublist3r.py -d <domain\_name>*

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**



```
vishmi㉿kali: ~]$ sudo mkdir -p /home/kali/Documents/audit/lichess
[vishmi㉿kali: ~]$ sudo touch /home/kali/Documents/audit/lichess/lichess.txt
[vishmi㉿kali: ~]$ cd ~/Sublist3r
```

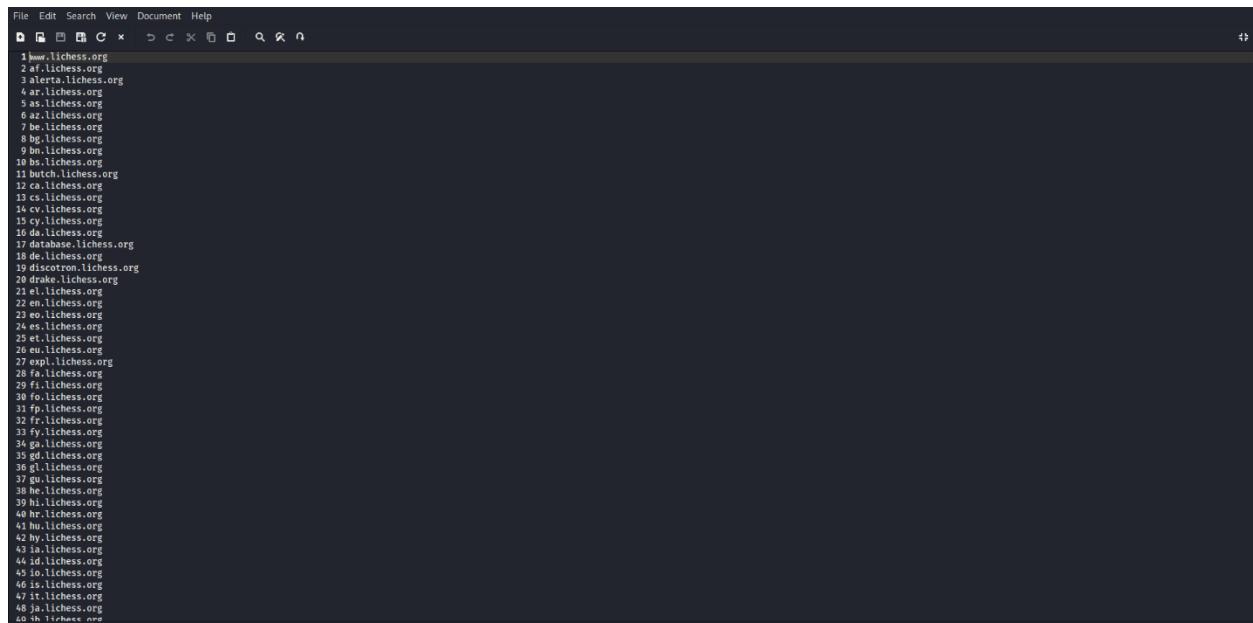


```
vishmi㉿kali: ~/Sublist3r]$ python3 sublist3r.py -d lichess.org >v -o liches.txt
/home/vishmi/Sublist3r/sublist3r.py:78: SyntaxWarning: invalid escape sequence '\_'
  \_\_ \_ | | | | \_ | | / \_ | | | \_ | | ' \_
/home/vishmi/Sublist3r/sublist3r.py:286: SyntaxWarning: invalid escape sequence '\'
link_regex = re.compile('<cite.*?>(.*)</cite>')
/home/vishmi/Sublist3r/sublist3r.py:343: SyntaxWarning: invalid escape sequence '\'
link = re.sub('<(\w)/?b>', "", link)
/home/vishmi/Sublist3r/sublist3r.py:439: SyntaxWarning: invalid escape sequence '\'
link = re.sub('<(\w)/?strong>|<span.*?>|<|>', '', link)
/home/vishmi/Sublist3r/sublist3r.py:658: SyntaxWarning: invalid escape sequence '\'
tbl_regex = re.compile('<a name="hostanchor"><\a>Host Records.*?<table.*?>(.*)</table>', re.S)
/home/vishmi/Sublist3r/sublist3r.py:898: SyntaxWarning: invalid escape sequence '\'
domain_check = re.compile("^(http|https)?[a-zA-Z0-9]+([\\.-\\.]{}1)[a-zA-Z0-9]+)*\\.[a-zA-Z]{2,}$")
```

# Coded By Ahmed Aboul-Ela - @aboul3la

```
[+] Enumerating subdomains now for lichess.org
[-] 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..
```

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



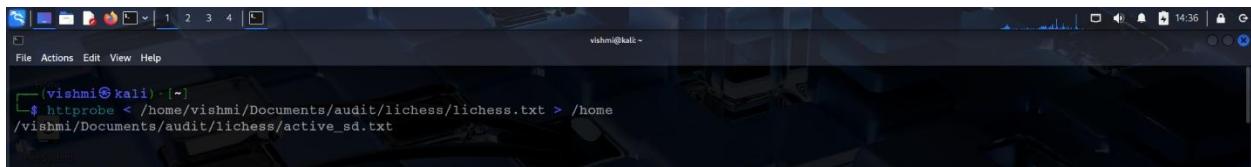
```
File Edit Search View Document Help
1 bw.lichess.org
2 cl.lichess.org
3 alerta.lichess.org
4 ar.lichess.org
5 as.lichess.org
6 az.lichess.org
7 be.lichess.org
8 bg.lichess.org
9 bn.lichess.org
10 bs.lichess.org
11 butch.lichess.org
12 ca.lichess.org
13 cs.lichess.org
14 da.lichess.org
15 cy.lichess.org
16 da.lichess.org
17 database.lichess.org
18 de.lichess.org
19 dinamic.lichess.org
20 dzone.lichess.org
21 el.lichess.org
22 en.lichess.org
23 eo.lichess.org
24 es.lichess.org
25 et.lichess.org
26 fi.lichess.org
27 expl.lichess.org
28 fa.lichess.org
29 fi.lichess.org
30 fo.lichess.org
31 fr.lichess.org
32 gl.lichess.org
33 fy.lichess.org
34 ga.lichess.org
35 gd.lichess.org
36 gl.lichess.org
37 gu.lichess.org
38 he.lichess.org
39 hi.lichess.org
40 hr.lichess.org
41 hu.lichess.org
42 hy.lichess.org
43 id.lichess.org
44 id.lichess.org
45 io.lichess.org
46 is.lichess.org
47 it.lichess.org
48 ja.lichess.org
49 zh.lichess.org
```

## HTTPProbe

HTTPProbe 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.

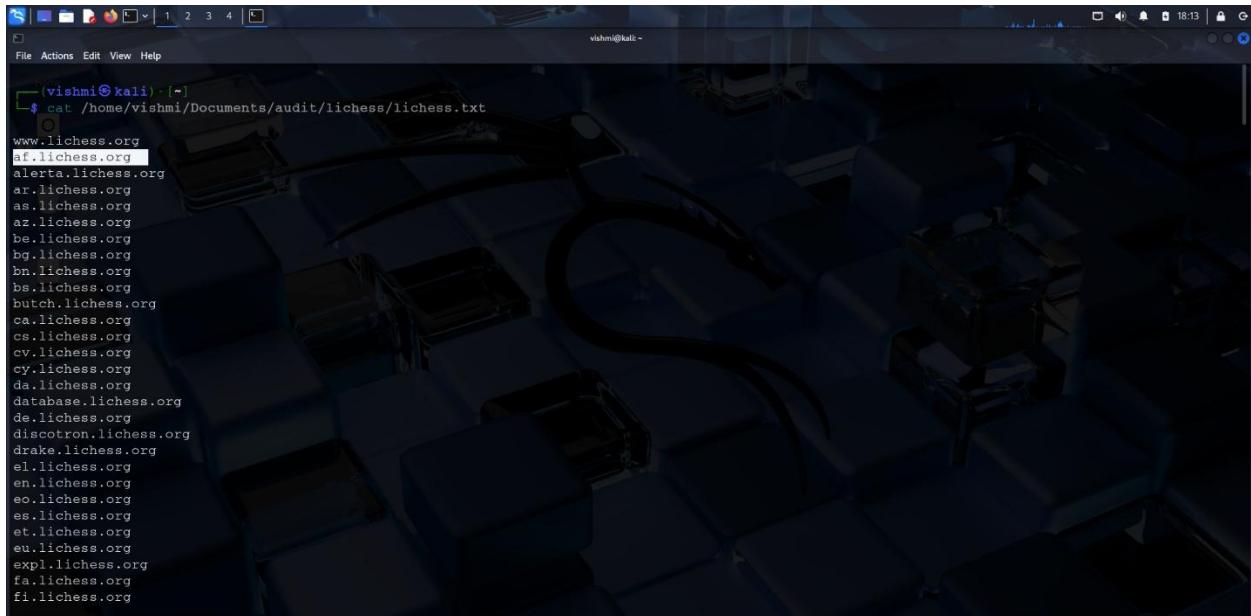
First, I installed `httpprobe`.

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



```
vishmi@kali:~$ httpprobe </home/vishmi/Documents/audit/lichess/lichess.txt > /home/vishmi/Documents/audit/lichess/active_sd.txt
```

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



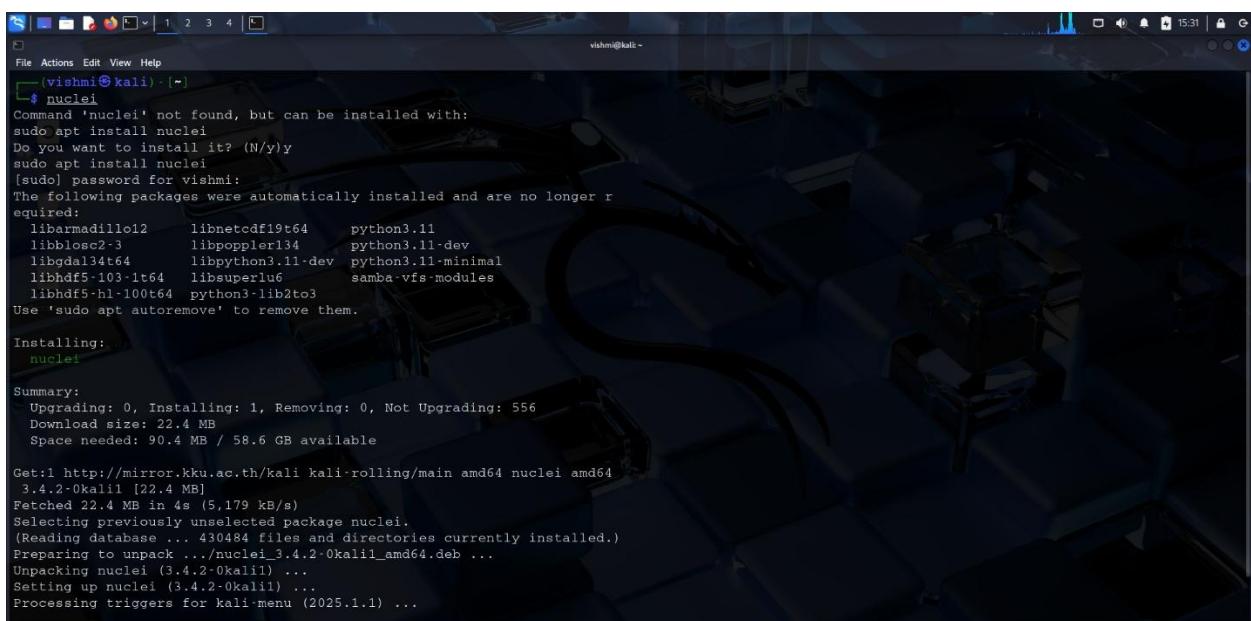
```
vishmi@kali:~$ cat /home/vishmi/Documents/audit/lichess/lichess.txt
www.lichess.org
af.lichess.org
alerta.lichess.org
ar.lichess.org
as.lichess.org
az.lichess.org
be.lichess.org
bg.lichess.org
bn.lichess.org
bs.lichess.org
butch.lichess.org
ca.lichess.org
cs.lichess.org
cv.lichess.org
cy.lichess.org
da.lichess.org
database.lichess.org
de.lichess.org
discotron.lichess.org
drake.lichess.org
el.lichess.org
en.lichess.org
eo.lichess.org
es.lichess.org
et.lichess.org
eu.lichess.org
expl.lichess.org
fa.lichess.org
fi.lichess.org
```

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.



```
vishmi@kali: ~
$ nuclei
Command 'nuclei' not found, but can be installed with:
sudo apt install nuclei
Do you want to install it? (N/y)y
sudo apt install nuclei
[sudo] password for vishmi:
The following packages were automatically installed and are no longer required:
 libarmadillo12  libnetcdf19t64  python3.11
 libblosc2-3   libpoppler134  python3.11-dev
 libgdal34t64  libpython3.11-dev  python3.11-minimal
 libhdf5-103-1t64  libsuperlu6  samba-vfs-modules
 libhdf5-hl-100t64  python3-lib2to3
Use 'sudo apt autoremove' to remove them.

Installing:
 nuclei

Summary:
 Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 556
 Download size: 22.4 MB
 Space needed: 90.4 MB / 58.6 GB available

Get:1 http://mirror.kku.ac.th/kali kali-rolling/main amd64 nuclei amd64
 3.4.2-0kali1 [22.4 MB]
Fetched 22.4 MB in 4s (5,179 kB/s)
Selecting previously unselected package nuclei.
(Reading database ... 430484 files and directories currently installed.)
Preparing to unpack .../nuclei_3.4.2-0kali1_amd64.deb ...
Unpacking nuclei (3.4.2-0kali1) ...
Setting up nuclei (3.4.2-0kali1) ...
Processing triggers for kali-menu (2025.1.1) ...
```

```

[vishmi㉿kali:~] $ nuclei -u af.lichess.org
v3.4.2
projectdiscovery.io

[INFO] Current nuclei version: v3.4.2 (latest)
[INFO] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 64
[INFO] Templates loaded for current scan: 7862
[INFO] Executing 7669 signed templates from projectdiscovery/nuclei-temp
lates
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[INFO] Targets loaded for current scan: 1
[INFO] Running httpx on input host
[INFO] Found 0 URL from httpx
[INFO] Templates clustered: 1717 (Reduced 1614 Requests)
[dns-waf-detect:cloudflare] [dns] [info] af.lichess.org
[INFO] Using Interactsh Server: oast.online

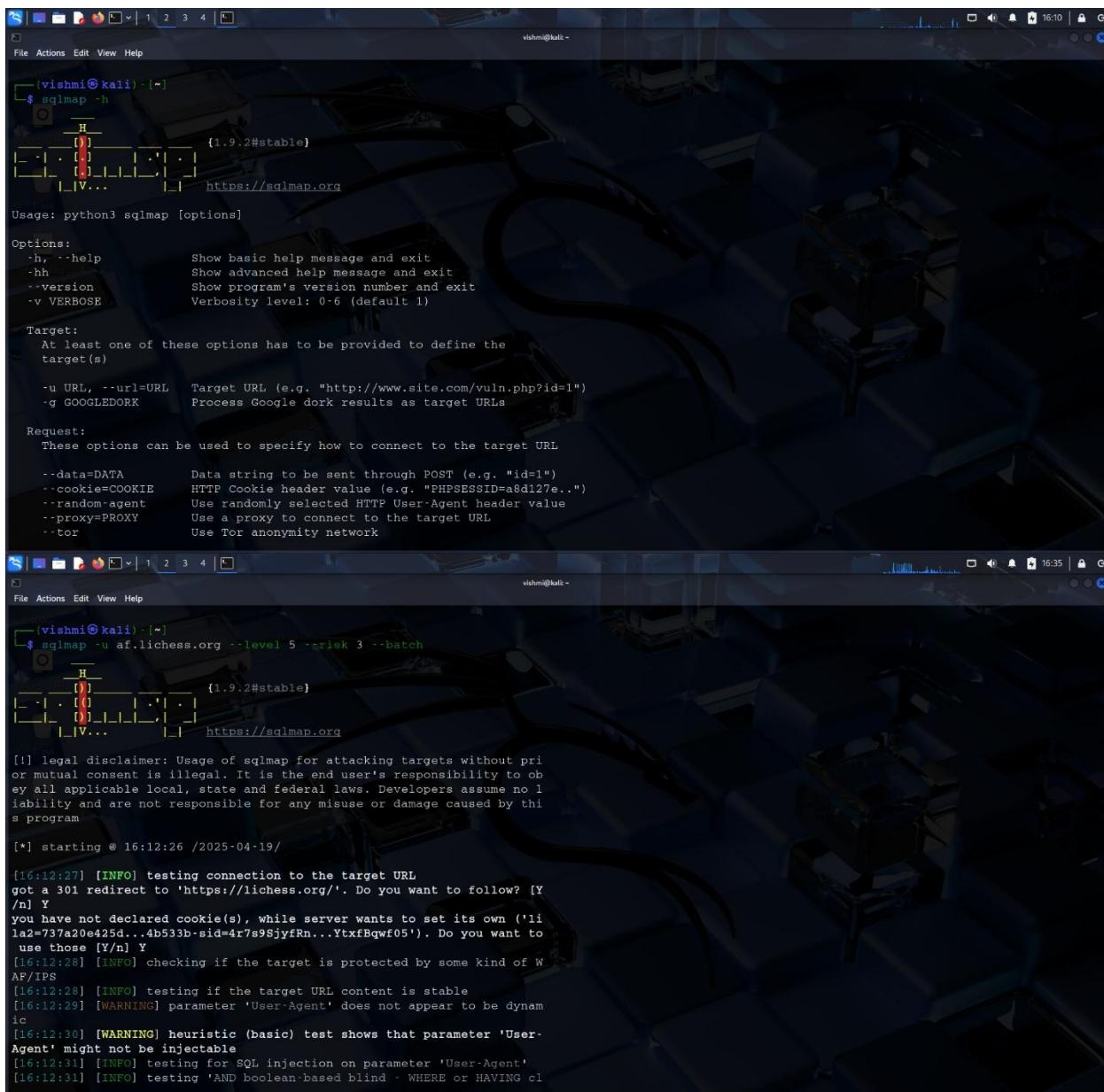
[vishmi㉿kali:~] $

```

Vulnerability Type	Description	Risk
<b>Dns-waf-detect [cloudflare]</b>	By using Cloudflare Web Application Firewall (WAF), the domain <i>af.lichess.org</i> 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.



The screenshot shows two terminal windows side-by-side. Both windows have a dark blue background with a 3D geometric pattern. The top window displays the SQLmap help menu:

```
vishmi㉿kali:~[*]$ sqlmap -h
[!] [H] {1.9.2#stable}
[!] [.] [.] [.] [.] [V...]
[!] https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help           Show basic help message and exit
  -hh, --hh            Show advanced help message and exit
  --version           Show program's version number and exit
  -v VERBOSE          Verbosity level: 0-6 (default 1)

Target:
  At least one of these options has to be provided to define the target(s)

  -u URL, --url=URL  Target URL (e.g. "http://www.site.com/vuln.php?id=1")
  -g GOOGLEDORK      Process Google dork results as target URLs

Request:
  These options can be used to specify how to connect to the target URL

  --data=DATA         Data string to be sent through POST (e.g. "id=1")
  --cookie=COOKIE    HTTP Cookie header value (e.g. "PHPSESSID=a8d127e...")
  --random-agent     Use randomly selected HTTP User-Agent header value
  --proxy=PROXY       Use a proxy to connect to the target URL
  --tor              Use Tor anonymity network
```

The bottom window shows the execution of a SQLmap command against the `af.lichess.org` target:

```
vishmi㉿kali:~[*]$ sqlmap -u af.lichess.org --level 5 --risk 3 --batch
[!] [H] {1.9.2#stable}
[!] [.] [.] [.] [.] [V...]
[!] https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:12:26 /2025-04-19

[16:12:27] [INFO] testing connection to the target URL
got a 301 redirect to 'https://lichess.org/'. Do you want to follow? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('l1a2=737a20e425d...4b533b-sid=4r7s9SjyfRn...YtxfBqwf05'). Do you want to use those [Y/n] Y
[16:12:28] [INFO] checking if the target is protected by some kind of WAF/IPS
[16:12:28] [INFO] testing if the target URL content is stable
[16:12:29] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[16:12:30] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[16:12:31] [INFO] testing for SQL injection on parameter 'User-Agent'
[16:12:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING cl
```

<b>Option</b>	<b>Meaning</b>
<b>-u</b>	For basic testing, the target URL is required.
<b>--level5</b>	Increases the number of payloads and tests that are done (maximum is 5).
<b>--risk3</b>	Increase the danger level of the payloads used (maximum is 3)
<b>--batch</b>	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.]

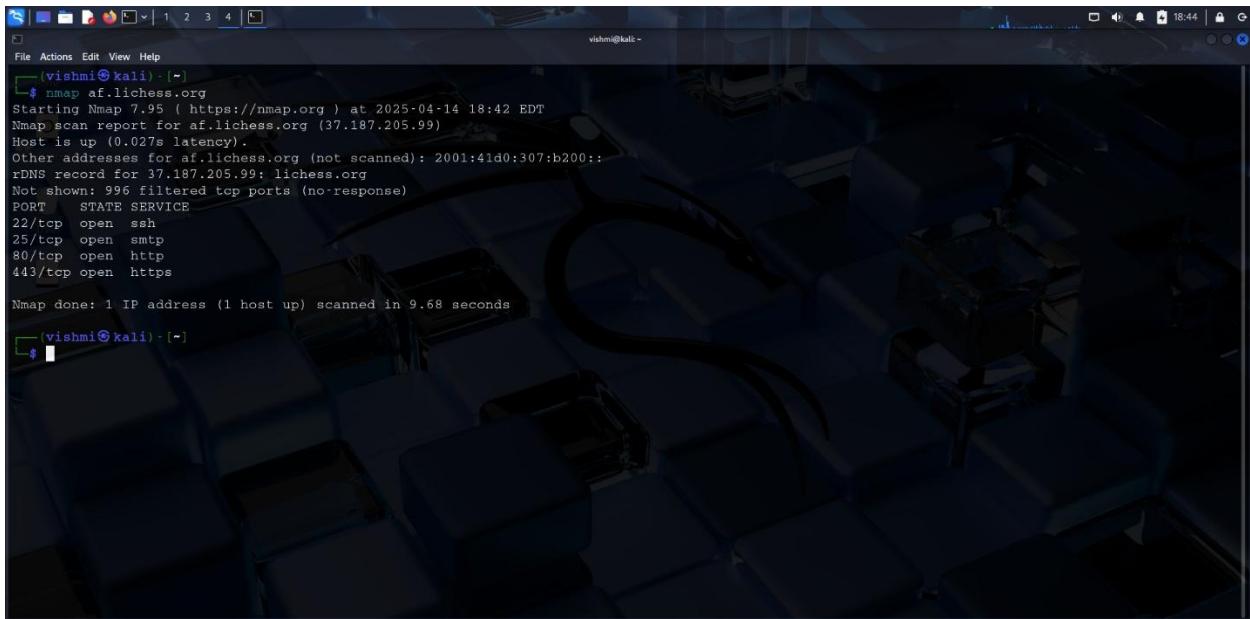
\* **[INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'**

[ 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.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal window title is 'vishmi@kali: ~'. The command entered is '# nmap af.lichess.org'. The output of the Nmap scan is displayed:

```
vishmi@kali: ~
# nmap af.lichess.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 18:42 EDT
Nmap scan report for af.lichess.org (37.187.205.99)
Host is up (0.027s latency).
Other addresses for af.lichess.org (not scanned): 2001:41d0:307:b200::1
rDNS record for 37.187.205.99: lichess.org
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 9.68 seconds
```

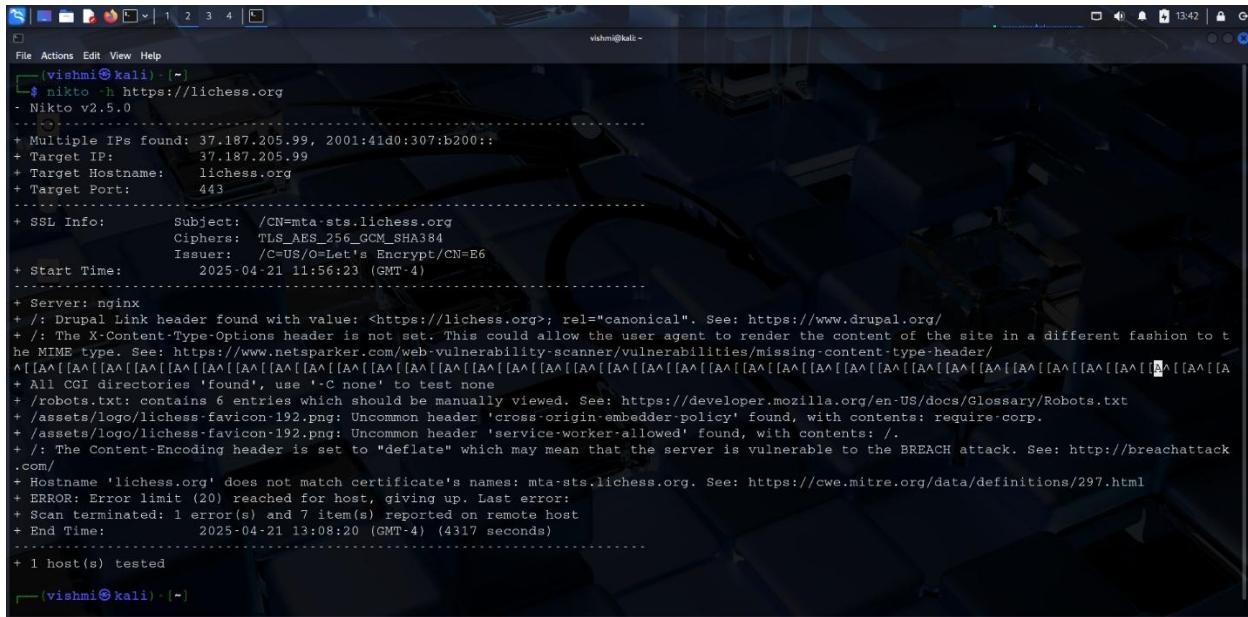
I discovered these details by using Nmap to search [af.lichess.org](http://af.lichess.org).

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

PORT	SERVICE	Vulnerabilities
<b>22/tcp</b>	ssh	Vulnerable to outdated versions with known exploits and brute-force attacks.
<b>25/tcp</b>	smtp	Abuseable for spoofing/phishing attacks or as an open relay
<b>80/tcp</b>	http	Vulnerable to popular online threats such as SQLi and XSS, as well as unencrypted data transfer.
<b>443/tcp</b>	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.



The screenshot shows a terminal window titled 'vishmi@kali' running on a Kali Linux desktop environment. The terminal displays the output of a Nikto scan against the target website 'https://lichess.org'. The output provides detailed information about the server configuration, SSL/TLS settings, and various security findings. Key findings include:

- SSL Info: Subject: /CN=mta-sts.lichess.org, Ciphers: TLS\_AES\_256\_GCM\_SHA384, Issuer: /C=US/O=Let's Encrypt/CN=E6
- Start Time: 2025-04-21 11:56:23 (GMT -4)
- Server: nginx
- X-Content-Type-Options header found with value: <https://lichess.org>, rel="canonical". See: https://www.drupal.org/
- The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
- All CGI directories 'found', use '-C none' to test none
- /robots.txt: contains 6 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
- /assets/logo/lichess-favicon-192.png: Uncommon header 'cross-origin-embedder-policy' found, with contents: require-corp.
- /assets/logo/lichess-favicon-192.png: Uncommon header 'service-worker-allowed' found, with contents: /.
- The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
- Hostname 'lichess.org' does not match certificate's names: mta-sts.lichess.org. See: https://cwe.mitre.org/data/definitions/297.html
- ERROR: Error limit (20) reached for host, giving up. Last error:
- Scan terminated: 1 error(s) and 7 item(s) reported on remote host
- End Time: 2025-04-21 13:08:20 (GMT -4) (4317 seconds)

+ 1 host(s) tested

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.

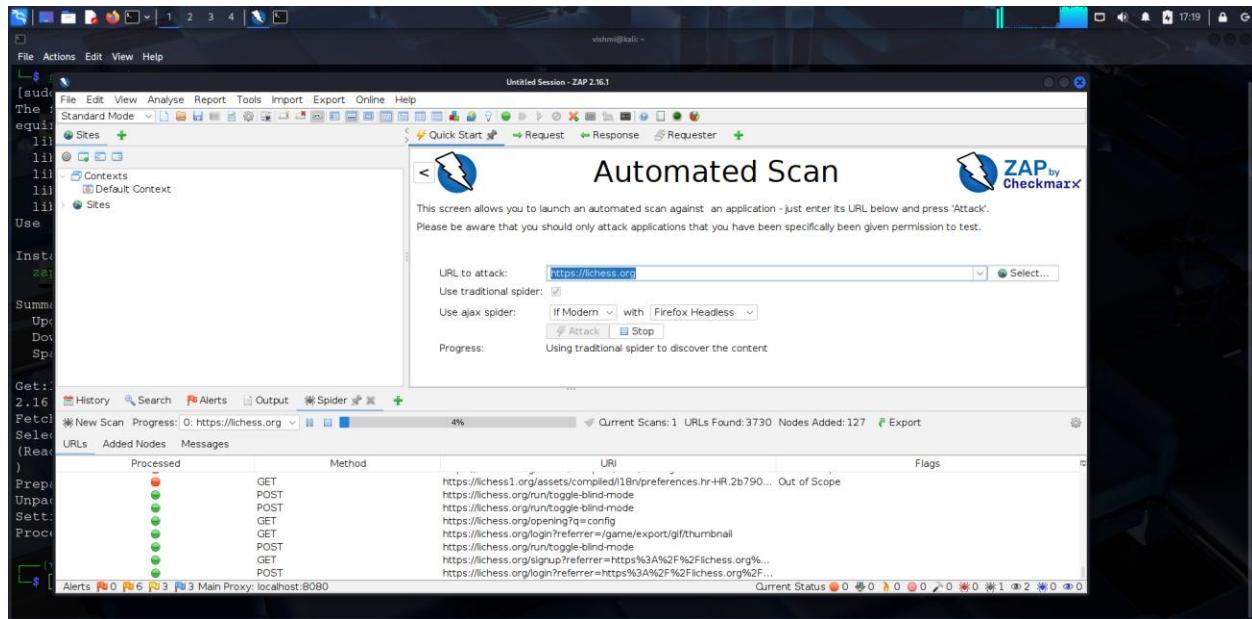
I entered <https://lichess.org> in URL section .

As a result, I got this summary .

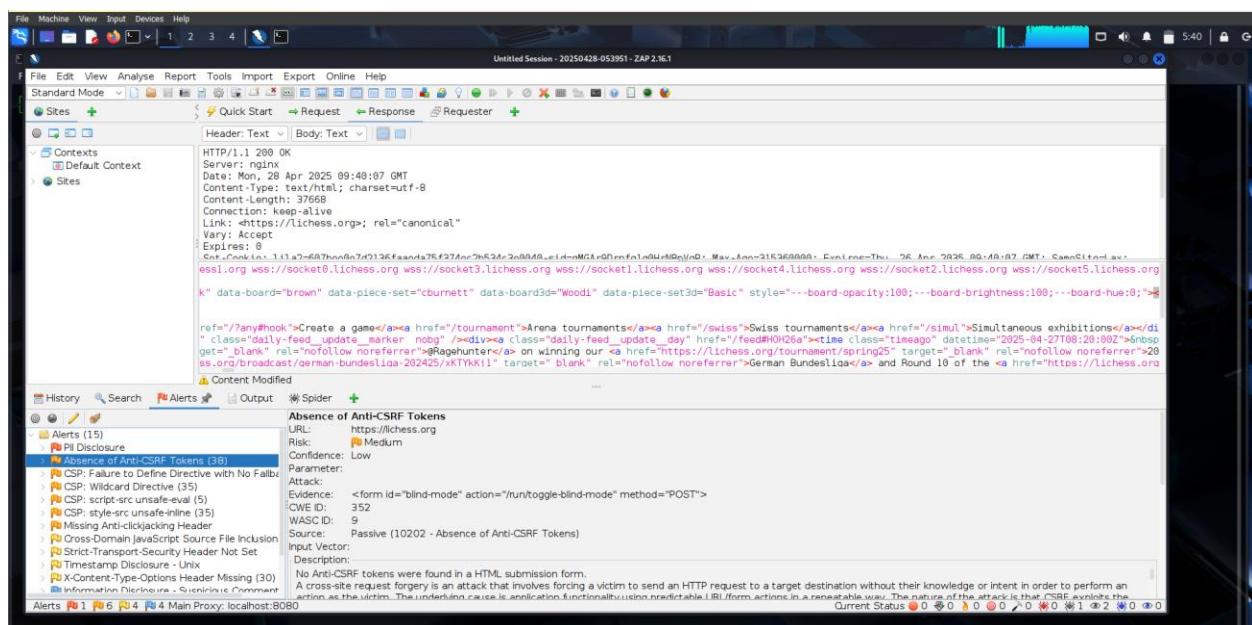
# OWASP ZAP

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.)

Risk	User Confirmed	Confidence				Total
		High	Medium	Low		
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 Checkmark 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 (4,284.8%)
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 View image

ZAP by Checkmark 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

Timestamp Disclosure - Unix	Low	6 (28.6%)
X-Content-Type-Options Header Missing	Low	883 (4,284.8%)
Charset Mismatch (Header Versus Meta Charset)	Informational	1 (4.8%)
Information Disclosure - Suspicious Comments	Informational	136 (647.6%)
Modern Web Application	Informational	884 (4,289.5%)
Re-examine Cache-control Directives	Informational	569 (2,789.5%)
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

The screenshot shows a Firefox browser window displaying a ZAP report. The title bar says "ZAP by Checkmark Scanning". The address bar shows "file:///home/vishnu/2025-04-19-ZAP-Report-.html#alert-type-2". The page content is a detailed alert report.

**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)

▼ Response

► Status line and header section (500 bytes)

# Vulnerabilities

<b>a.Vulnerability Title</b>	<b>Absence of Anti-CSRF Tokens</b>
<b>b.Vulnerability Description</b>	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.
<b>c.Affected Components</b>	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.
<b>d.Impact Assessment</b>	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.
<b>e.Steps to Reproduce</b>	<ol style="list-style-type: none"><li>1. Sign in as an authorized user.</li><li>2. Find an endpoint or form (such updating a profile) that is missing an anti-CSRF token.</li><li>3. Make a malicious page that sends the identical form data to the intended application by copying the form's HTML.</li><li>4. Use a phishing email, for example, to trick a logged-in user into visiting the malicious page.</li><li>5. Verify the lack of CSRF protection by noting that the action was carried out on the user's behalf without their consent.</li></ol>
<b>f.Proof of Concept (if applicable)</b>	HTML form without CSRF token: <i>html&lt;br&gt;&lt;form action="https://vulnerable-app.com/change-email" method="POST"&gt;&lt;br&gt;&lt;input type="email" name="email" value="attacker@example.com"&gt;&lt;br&gt; &lt;input type="submit" value="Change Email"&gt;&lt;br&gt;&lt;/form&gt;&lt;br&gt;</i>
<b>g.Proposed Mitigation or Fix</b>	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*

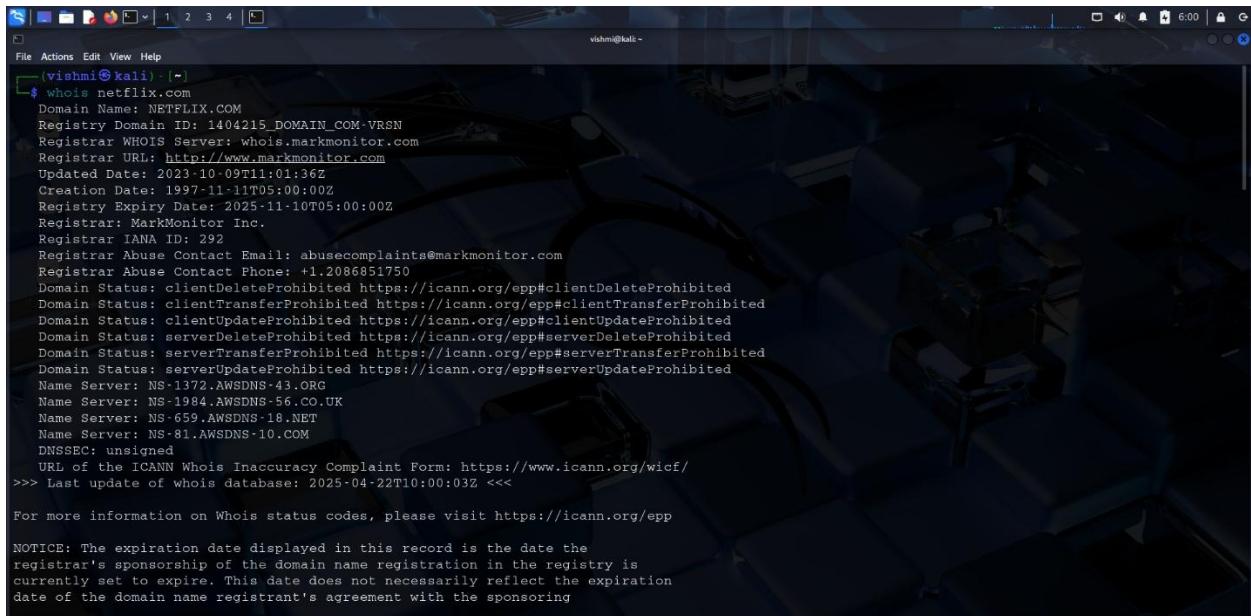
**Domain** = *netflix.com*

**Sub-domain** = *www.netflix.com*

**URL** = *https://www.netflix.com*

# Target Reconnaissance

## Introduction to Netflix and Audit Scope



```
vishni@kali: ~]$ whois netflix.com
Domain Name: NETFLIX.COM
Registry Domain ID: 1404215_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-10-09T11:01:36Z
Creation Date: 1997-11-11T05:00:00Z
Registry Expiry Date: 2025-11-10T05:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS-1372.AWSDNS-43.ORG
Name Server: NS-1984.AWSDNS-56.CO.UK
Name Server: NS-659.AWSDNS-18.NET
Name Server: NS-81.AWSDNS-10.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-22T10:00:03Z <<
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
```

“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

Search Scope Maximum severity Bounty eligibility

Download Burp Suite Project Configuration File Download CSV View changes (Last updated on May 24, 2024) 1-38 of 38

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
Netflix Gaming Target Non-Rewardable	Other	In scope	Critical	Ineligible	Jan 12, 2024	0 (0%)
nmtracking.netflix.com Primary Target customerevents.netflix.com, nmtracking.netflix.com, and presentationtracking.netflix.com are all alias of beacon.netflix.com.	Domain	In scope	Critical	Eligible	Jan 12, 2024	3 (0%)
Submissions containing variations of the URL will not be treated as unique.						
*.prod.drredis.netflix.com Primary Target	Other	In scope	Critical	Ineligible	Jan 12, 2024	0 (0%)

Search Scope Maximum severity Bounty eligibility

Download Burp Suite Project Configuration File Download CSV View changes (Last updated on May 24, 2024) 1-38 of 38

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
www.netflix.com/api/*	Wildcard	In scope	Critical	Eligible	Jan 12, 2024	3 (0%)
*.prod.ftl.netflix.com Primary Target The primary Netflix experience is driven by microservices that are hosted and called through our API.	Wildcard	In scope	Critical	Eligible	Jan 12, 2024	3 (0%)
You may see the API referenced as api*.netflix.com as well as www.netflix.com/api/*						
Content authorization vulnerabilities affecting only the in-browser player Non-Rewardable	Other	In scope	Critical	Ineligible	Jan 12, 2024	0 (0%)

## **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***

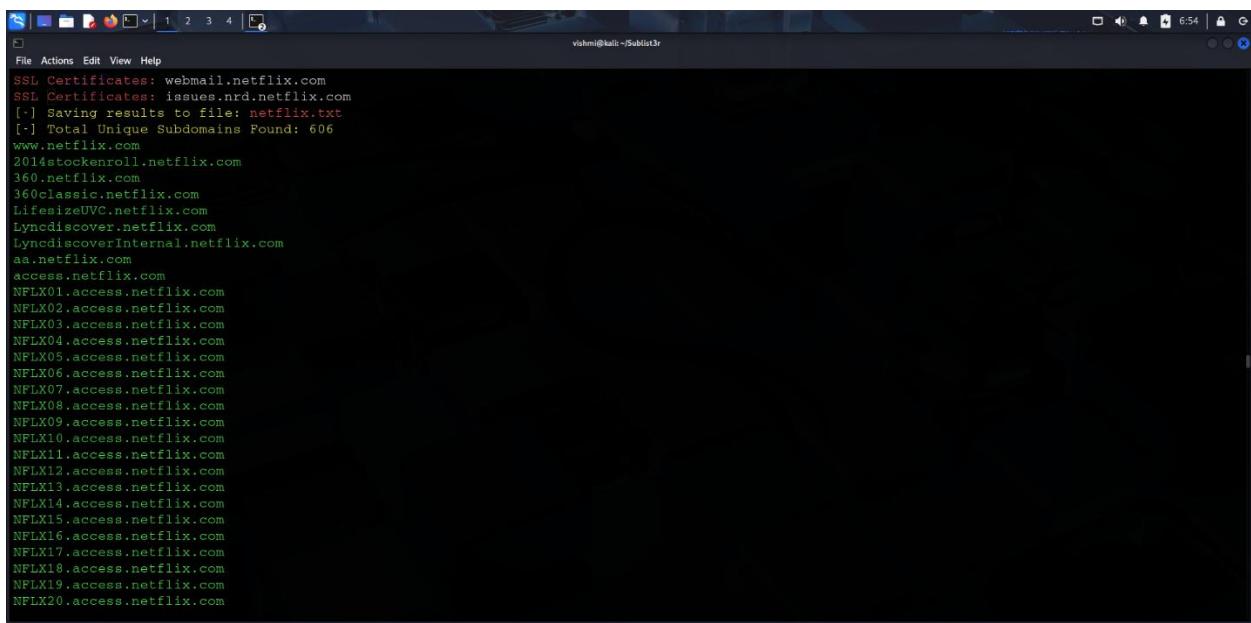
```
vishmi@kali:~/Sublist3r
File Actions Edit View Help
└── (vishmi㉿kali) - [~]
    $ sudo mkdir -p /home/vishmi/Documents/audit/netflix/
    $ sudo touch /home/vishmi/Documents/audit/netflix/netflix.txt

└── (vishmi㉿kali) - [~]
    $ cd ~/Sublist3r
```

```
(vishmi㉿kali)-[~/Sublist3r]
└$ python3 sublist3r.py -d netflix.com > netflix.txt
/home/vishmi/Sublist3r/sublist3r.py:78: SyntaxWarning: invalid escape
sequence '\\'
    \\\\" | \\ | | \\ | / | \\ | / | \\ | ' |
/home/vishmi/Sublist3r/sublist3r.py:286: SyntaxWarning: invalid escape
sequence '\\'
link_regex = re.compile('<site.*?>(.*)</site>')
/home/vishmi/Sublist3r/sublist3r.py:343: SyntaxWarning: invalid escape
sequence '\\'
link = re.sub("<(\\/)?b>", "", link)
/home/vishmi/Sublist3r/sublist3r.py:439: SyntaxWarning: invalid escape
sequence '\\'
link = re.sub('<(\\/)?strong>|<span.*?>|<br>', '', link)
/home/vishmi/Sublist3r/sublist3r.py:658: SyntaxWarning: invalid escape
sequence '\\'
tbl_regex = re.compile('<a name="hostanchor"></a>Host Records.*?<ta
ble.*?>(.*)</table>', re.S)
/home/vishmi/Sublist3r/sublist3r.py:898: SyntaxWarning: invalid escape
sequence '\\'
domain_check = re.compile("^(http|https)?[a-zA-Z0-9]+([\\-\\.]{1}[a-zA
-20-9]+)*.[a-zA-Z]{2,}$")

```

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

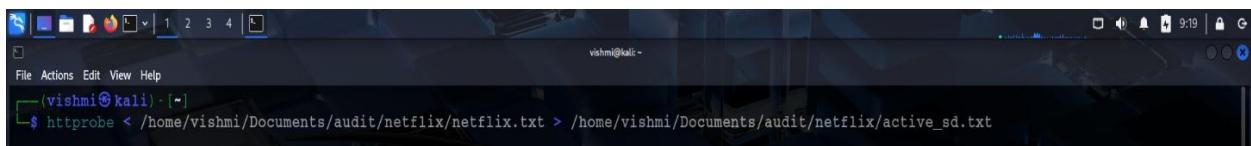


```
vishnu@kali:~/Sublist3r$ SSL Certificates: webmail.netflix.com
SSL Certificates: issues.nrd.netflix.com
[-] Saving results to file: netflix.txt
[!] Total Unique Subdomains Found: 606
www.netflix.com
2014stockenroll.netflix.com
360.netflix.com
360classic.netflix.com
LifesizeUVC.netflix.com
Lyncdiscover.netflix.com
Lyncdiscoverinternal.netflix.com
aa.netflix.com
access.netflix.com
NFLX01.access.netflix.com
NFLX02.access.netflix.com
NFLX03.access.netflix.com
NFLX04.access.netflix.com
NFLX05.access.netflix.com
NFLX06.access.netflix.com
NFLX07.access.netflix.com
NFLX08.access.netflix.com
NFLX09.access.netflix.com
NFLX10.access.netflix.com
NFLX11.access.netflix.com
NFLX12.access.netflix.com
NFLX13.access.netflix.com
NFLX14.access.netflix.com
NFLX15.access.netflix.com
NFLX16.access.netflix.com
NFLX17.access.netflix.com
NFLX18.access.netflix.com
NFLX19.access.netflix.com
NFLX20.access.netflix.com
```

## HTTPProbe

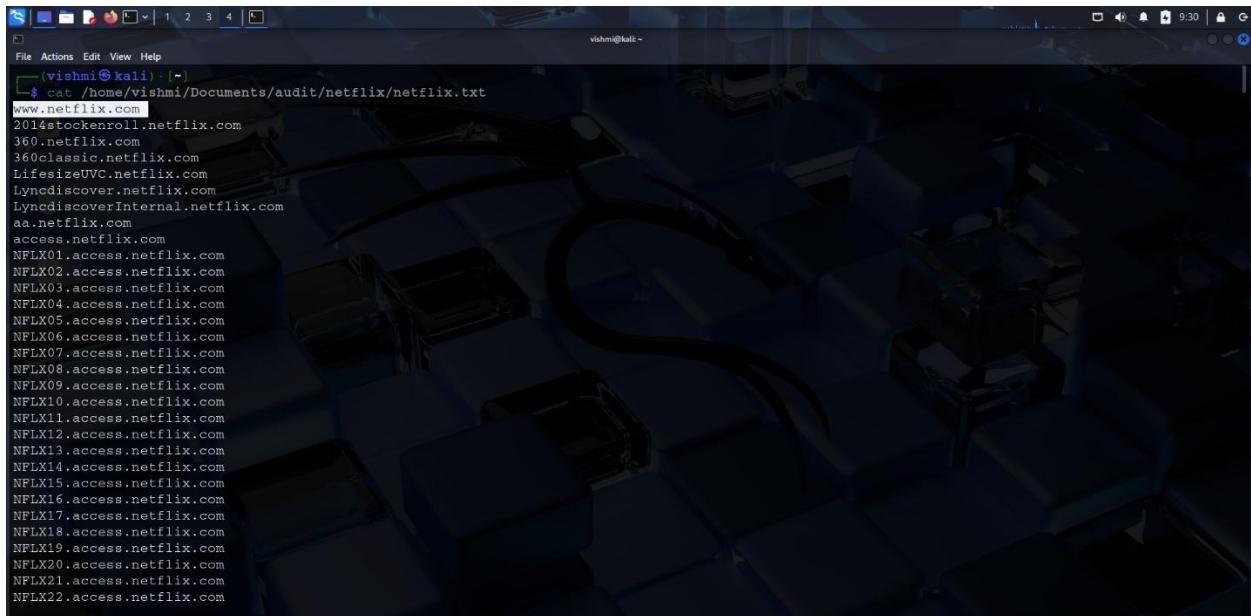
HTTPProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing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



```
vishmi@kali: ~
File Actions Edit View Help
(wishmi@kali) [~]
$ httpprobe < /home/vishmi/Documents/audit/netflix/netflix.txt > /home/vishmi/Documents/audit/netflix/active_sd.txt
```

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

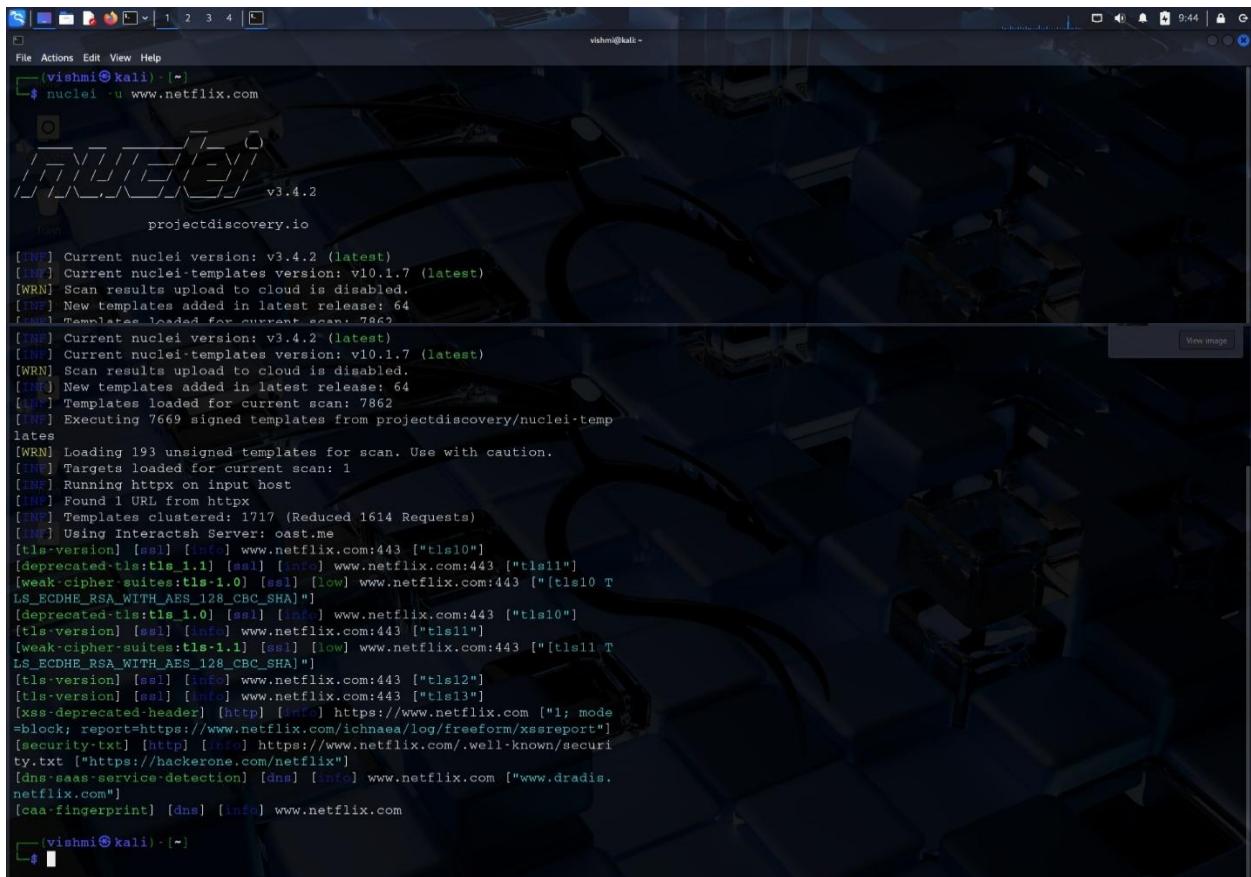


```
vishmi@kali: ~
File Actions Edit View Help
(wishmi@kali) [~]
$ cat /home/vishmi/Documents/audit/netflix/netflix.txt
www.netflix.com
2014stockenroll.netflix.com
360.netflix.com
360classic.netflix.com
LifesizeUVC.netflix.com
Lyncdiscover.netflix.com
LyncdiscoverInternal.netflix.com
aa.netflix.com
access.netflix.com
NFLX01.access.netflix.com
NFLX02.access.netflix.com
NFLX03.access.netflix.com
NFLX04.access.netflix.com
NFLX05.access.netflix.com
NFLX06.access.netflix.com
NFLX07.access.netflix.com
NFLX08.access.netflix.com
NFLX09.access.netflix.com
NFLX10.access.netflix.com
NFLX11.access.netflix.com
NFLX12.access.netflix.com
NFLX13.access.netflix.com
NFLX14.access.netflix.com
NFLX15.access.netflix.com
NFLX16.access.netflix.com
NFLX17.access.netflix.com
NFLX18.access.netflix.com
NFLX19.access.netflix.com
NFLX20.access.netflix.com
NFLX21.access.netflix.com
NFLX22.access.netflix.com
```

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).



```
vishmi㉿kali:~$ nuclei -u www.netflix.com
vishmi㉿kali:~$ 
[INFO] Current nuclei version: v3.4.2 (latest)
[INFO] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 64
[INFO] Templates loaded for current scan: 7862
[INFO] Current nuclei version: v3.4.2 (latest)
[INFO] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 64
[INFO] Templates loaded for current scan: 7862
[INFO] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[INFO] Targets loaded for current scan: 1
[INFO] Running httpx on input host
[INFO] Found 1 URL from httpx
[INFO] Templates clustered: 1717 (Reduced 1614 Requests)
[INFO] Using Interactsh Server: oast.me
[tls-version] [ssl] [info] www.netflix.com:443 ["tls10"]
[deprecated-tls:tls-1.1] [ssl] [info] www.netflix.com:443 ["tls11"]
[weak-cipher-suites:tls-1.0] [ssl] [low] www.netflix.com:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]
[deprecated-tls:tls-1.0] [ssl] [info] www.netflix.com:443 ["tls10"]
[tls-version] [ssl] [info] www.netflix.com:443 ["tls11"]
[weak-cipher-suites:tls-1.0] [ssl] [low] www.netflix.com:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]
[tls-version] [ssl] [info] www.netflix.com:443 ["tls12"]
[tls-version] [ssl] [info] www.netflix.com:443 ["tls13"]
[xss-deprecated-header] [http] [info] https://www.netflix.com ["1; mode=block; report=https://www.netflix.com/ichnaea/log/freeform/xssreport"]
[security-txt] [http] [info] https://www.netflix.com/.well-known/security.txt ["https://hackerone.com/netflix"]
[dns-saaa-service-detection] [dns] [info] www.netflix.com ["www.dradis.netflix.com"]
[caa-fingerprint] [dns] [info] www.netflix.com
[vishmi㉿kali:~$ ]
```

Vulnerable Title	Description	Risk
<b>Deprecated TLS: TLS 1.1</b>	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
<b>Weak Cipher Suites: TLS 1.0</b>	The server is vulnerable to cryptographic attacks like BEAST and POODLE since it uses TLS 1.0 and weak encryption techniques.	Low
<b>Deprecated TLS: TLS 1.0</b>	Because TLS 1.0 has known weaknesses, it should no longer be maintained as it is an antiquated and unsafe protocol.	Low
<b>Weak Cipher Suites: TLS 1.1</b>	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
<b>XSS Deprecated Header</b>	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
<b>Security.txt Missing or Misconfigured</b>	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
<b>DNS SaaS Service Detection</b>	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
<b>CAA Fingerprint Found</b>	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.

```
vishmi㉿kali: ~]$ sqlmap -u www.netflix.com --level 5 --risk 3 --batch
[!] legal disclaimer: Usage of sqlmap for attacking targets without pri
or mutual consent is illegal. It is the end user's responsibility to ob
ey all applicable local, state and federal laws. Developers assume no l
iability and are not responsible for any misuse or damage caused by thi
s program
[*] starting @ 12:35:41 /2025-04-22/
[12:35:41] [INFO] testing connection to the target URL
got a 301 redirect to 'https://www.netflix.com/'. Do you want to follow
? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('nf
vdid=BQFmAAEBEY...f13A%3D%3D;flwssn=38898625-97...733a2fdec3;SecureNet
flixid=v%3D%26mac..5339744352;Netflixid=v%3D%26ct%...0e86RVVKW0.;gsid
=901e9ecd-8b...5e75c3d04b'). Do you want to use those [Y/n] Y
[12:35:46] [INFO] checking if the target is protected by some kind of W
AP/IPS
[12:35:50] [WARNING] reflective value(s) found and filtering out
[12:35:51] [INFO] testing if the target URL content is stable
[12:35:54] [WARNING] parameter 'User-Agent' does not appear to be dynam
ic
[12:35:58] [WARNING] heuristic (basic) test shows that parameter 'User-


vishmi㉿kali: ~]$ sqlmap -h
[!] legal disclaimer: Usage of sqlmap for attacking targets without pri
or mutual consent is illegal. It is the end user's responsibility to ob
ey all applicable local, state and federal laws. Developers assume no l
iability and are not responsible for any misuse or damage caused by thi
s program
[*] starting @ 12:34 /2025-04-22/
[12:34:00] [INFO] testing connection to the target URL
got a 301 redirect to 'https://www.netflix.com/'. Do you want to follow
? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('nf
vdid=BQFmAAEBEY...f13A%3D%3D;flwssn=38898625-97...733a2fdec3;SecureNet
flixid=v%3D%26mac..5339744352;Netflixid=v%3D%26ct%...0e86RVVKW0.;gsid
=901e9ecd-8b...5e75c3d04b'). Do you want to use those [Y/n] Y
[12:34:05] [INFO] checking if the target is protected by some kind of W
AP/IPS
[12:34:09] [WARNING] reflective value(s) found and filtering out
[12:34:10] [INFO] testing if the target URL content is stable
[12:34:13] [WARNING] parameter 'User-Agent' does not appear to be dynam
ic
[12:34:17] [WARNING] heuristic (basic) test shows that parameter 'User-


Usage: python3 sqlmap [options]

Options:
-h,--help           Show basic help message and exit
-hh                Show advanced help message and exit
--version          Show program's version number and exit
-v VERBOSE         Verbosity level: 0-6 (default 1)

Target:
At least one of these options has to be provided to define the
target(s)

-u URL, --url=URL  Target URL (e.g. "http://www.site.com/vuln.php?
id=1")
-g GOOGLEDORK     Process Google dork results as target URLs

Request:
These options can be used to specify how to connect to the target U
RL
```

```
[12:35:46] [INFO] checking if the target is protected by some kind of WAF/IPS
[12:35:50] [WARNING] reflective value(s) found and filtering out
[12:35:51] [INFO] testing if the target URL content is stable
[12:35:54] [WARNING] parameter 'User-Agent' does not appear to be dynamic
ic
[12:35:58] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[12:36:06] [INFO] testing for SQL injection on parameter 'User-Agent'
[12:36:06] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:41:19] [CRITICAL] can't establish SSL connection

[*] ending @ 12:41:19 /2025-04-22/
```

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

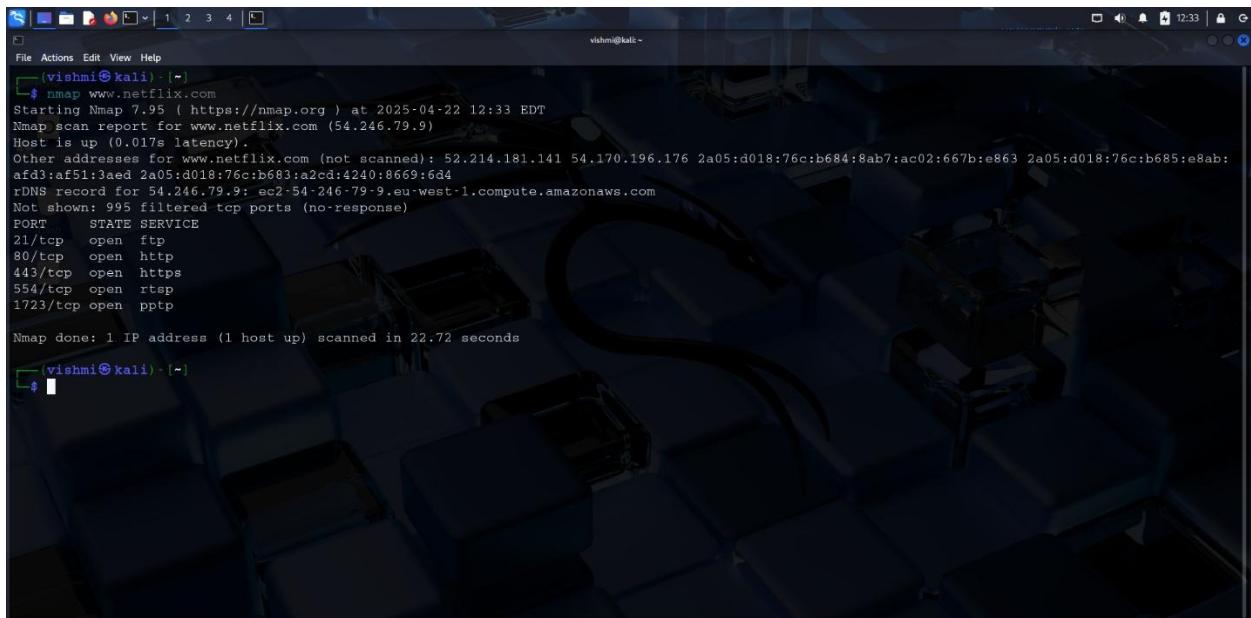
## Detected Information

- \* **[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.



```
vishmi㉿kali: ~]$ nmap www.netflix.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-22 12:33 EDT
Nmap scan report for www.netflix.com (54.246.79.9)
Host is up (0.017s latency).
Other addresses for www.netflix.com (not scanned): 52.214.181.141 54.170.196.176 2a05:d018:76c:b684:8ab7:ac02:667b:e863 2a05:d018:76c:b685:e8ab:a
af03:af51:3aed 2a05:d018:76c:b683:a2cd:4240:8669:6d4
rDNS record for 54.246.79.9: ec2-54-246-79-9.eu-west-1.compute.amazonaws.com
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 22.72 seconds
```

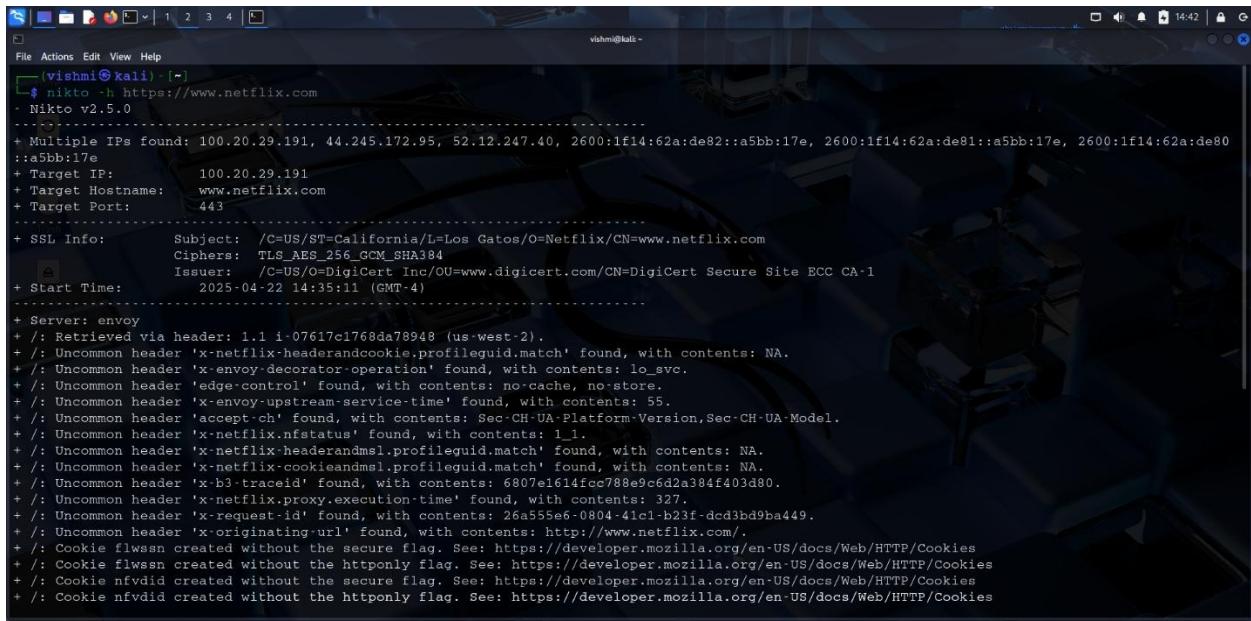
I discovered these details by using Nmap to search [www.netflix.com](http://www.netflix.com).

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

PORT	SERVICE	Vulnerabilities
<b>21/tcp</b>	ftp	Unencrypted credentials are accepted.
<b>80/tcp</b>	http	Transmits plain text data.
<b>443/tcp</b>	https	Deprecated TLS versions are supported.
<b>554/tcp</b>	Rtsp	Usually doesn't have authenticity.
<b>1723/tcp</b>	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.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running the Nikto web scanner against the Netflix website (https://www.netflix.com). The output of the scan is displayed, listing various security findings. Key findings include multiple IPs found (100.20.29.191, 44.245.172.95, 52.12.247.40), SSL info (Subject: /C=US/ST=California/L=Los Gatos/O=Netflix/CN=www.netflix.com, Ciphers: TLS\_AES\_256\_GCM\_SHA384, Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Secure Site ECC CA-1), and a start time of 2025-04-22 14:35:11 (GMT-4). The scan also lists numerous uncommon headers found, such as 'x-envoy-decorator-operation', 'edge-control', and various.netflix.proxy.execution-time' headers, along with cookie findings like 'flwssn' and 'nfvdid'.

```
vishni㉿kali:~$ nikto -h https://www.netflix.com
[Nikto v2.5.0]
-----
+ Multiple IPs found: 100.20.29.191, 44.245.172.95, 52.12.247.40, 2600:1f14:62a:de82::a5bb:17e, 2600:1f14:62a:de81::a5bb:17e, 2600:1f14:62a:de80::a5bb:17e
+ Target IP: 100.20.29.191
+ Target Hostname: www.netflix.com
+ Target Port: 443
-----
+ SSL Info:
  Subject: /C=US/ST=California/L=Los Gatos/O=Netflix/CN=www.netflix.com
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Secure Site ECC CA-1
+ Start Time: 2025-04-22 14:35:11 (GMT-4)
-----
+ Server: envoy
+ /: Retrieved via header: 1.1 i-07617c1768da78948 (us-west-2).
+ /: Uncommon header 'x-netflix-headerandcookie.profileguid.match' found, with contents: NA.
+ /: Uncommon header 'x-envoy-decorator-operation' found, with contents: lo_svc.
+ /: Uncommon header 'edge-control' found, with contents: no-cache, no-store.
+ /: Uncommon header 'x-envoy-upstream-service-time' found, with contents: 55.
+ /: Uncommon header 'accept-ch' found, with contents: Sec-CH-UA-Platform-Version,Sec-CH-UA-Model.
+ /: Uncommon header 'x-netflix.nfstatus' found, with contents: 1_1.
+ /: Uncommon header 'x-netflix-headerandms1.profileguid.match' found, with contents: NA.
+ /: Uncommon header 'x-netflix-cookieandms1.profileguid.match' found, with contents: NA.
+ /: Uncommon header 'x-b3-traceid' found, with contents: 6807e1614fcc788e9cd62a384f403d80.
+ /: Uncommon header 'x-netflix.proxy.execution-time' found, with contents: 327.
+ /: Uncommon header 'x-request-id' found, with contents: 26a555e6-0804-41c1-b23f-dcd3dd9ba449.
+ /: Uncommon header 'x-originating-url' found, with contents: http://www.netflix.com/.
+ /: Cookie flwssn created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie flwssn created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie nfvdid created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie nfvdid created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
```

Security issues found on [https://netiflix.com's](https://netiflix.com) 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.

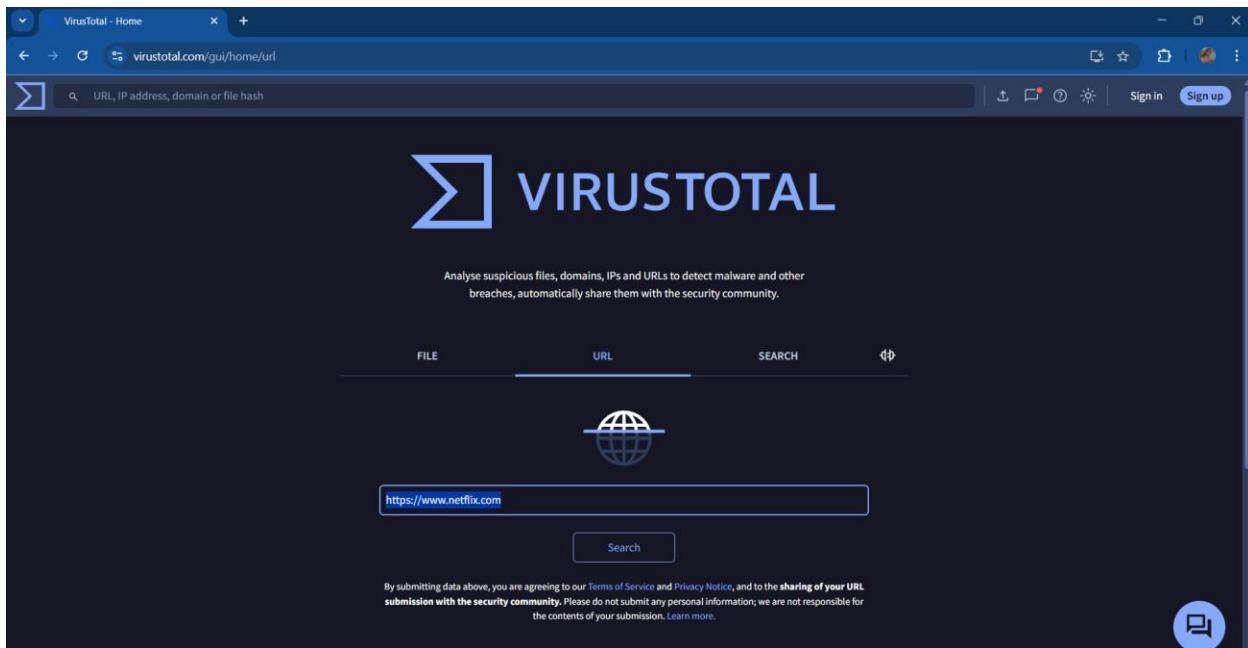
\*Cookie 'flwssn' created without the HTTPOnly and Secure flag.

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

## Virustotal

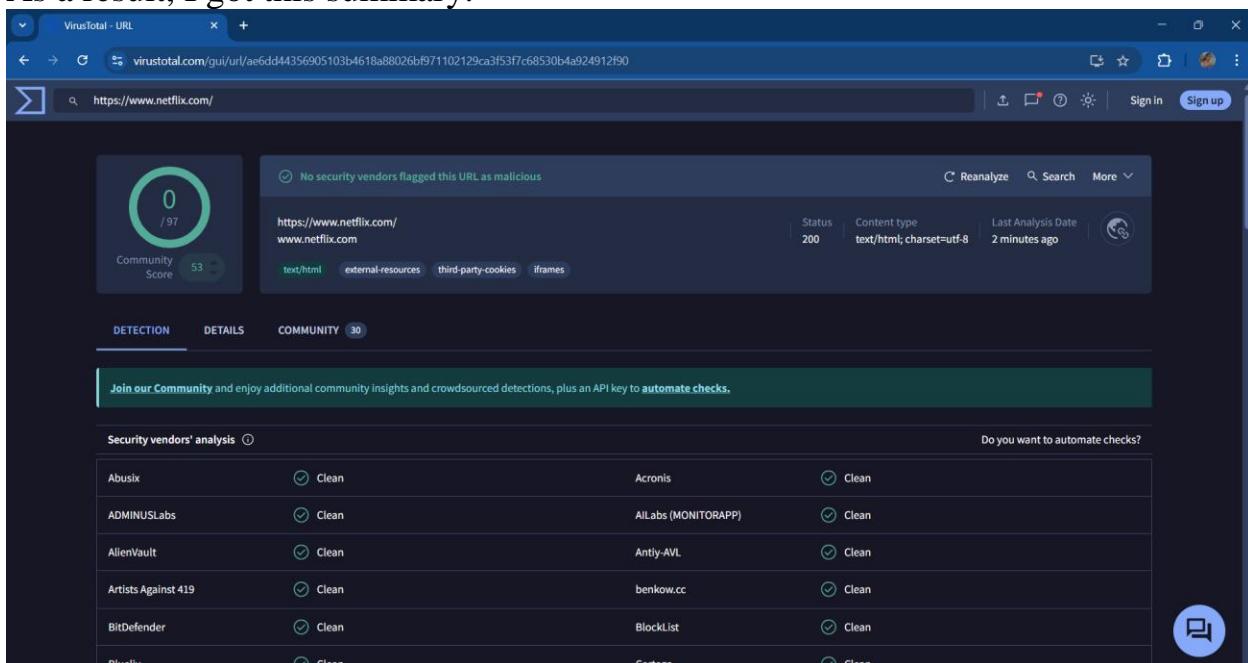
Virustotal is a free web service called VirusTotal employs 70 antivirus engines and URL blocklisting services to scan files and URLs for malware, adware, and other malicious content.

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



The screenshot shows the VirusTotal homepage. At the top, there's a search bar with the placeholder "URL, IP address, domain or file hash". Below it is a large logo consisting of a stylized 'Σ' symbol followed by the word "VIRUSTOTAL". A sub-instruction below the logo reads: "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community." There are three tabs at the top: "FILE", "URL" (which is selected), and "SEARCH". Below the tabs is a globe icon. A text input field contains the URL "https://www.netflix.com". To the right of the input field is a "Search" button. At the bottom of the page, a note states: "By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Notice](#), and to the [sharing of your URL submission with the security community](#). Please do not submit any personal information; we are not responsible for the contents of your submission. [Learn more](#)".

As a result, I got this summary.



The screenshot shows the detailed analysis summary for the URL "https://www.netflix.com". The summary includes:

- A large green circle icon with a '0' and "/97" indicating no malicious detections.
- The URL "https://www.netflix.com/" and its full domain "www.netflix.com".
- Status code "200" and Content type "text/html; charset=utf-8".
- Last Analysis Date "2 minutes ago".
- Community Score "53".
- Reanalyze, Search, and More buttons.
- Detected technologies: text/html, external-resources, third-party-cookies, iframes.
- Community section showing 30 members.
- A message encouraging users to "Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks."
- Security vendors' analysis table:

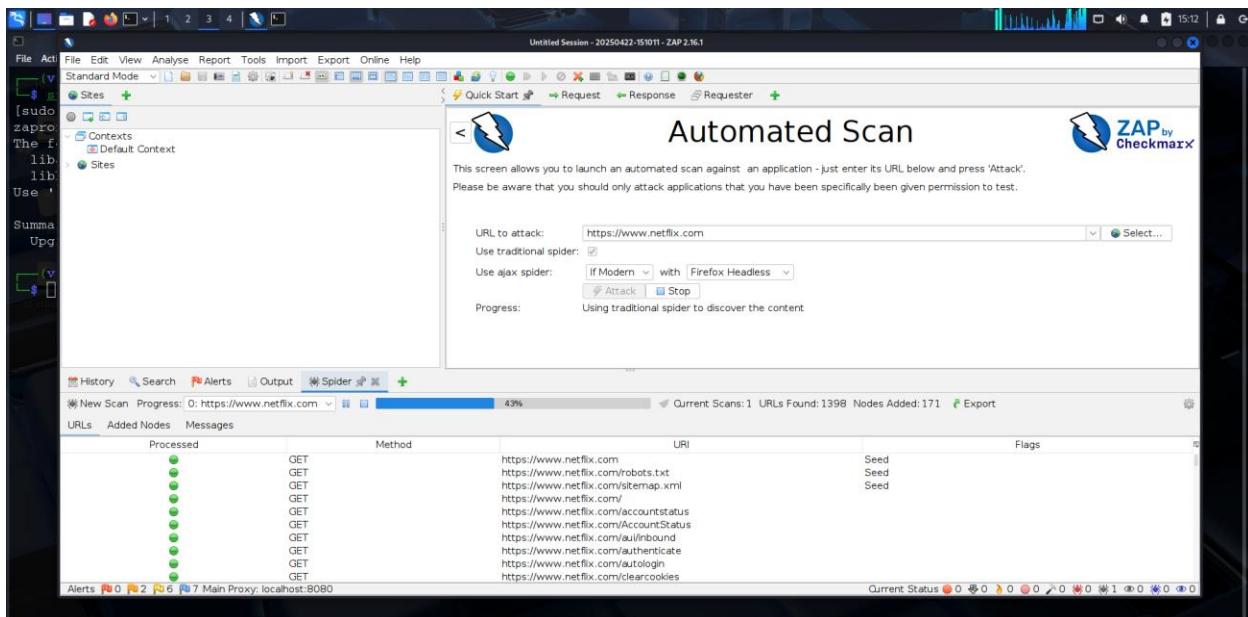
VirusTotal	Clean	Acronis	Clean
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	Allabs (MONITORAPP)	Clean
AlienVault	Clean	Anti-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Certego	Clean

- An "Automate Checks" button.

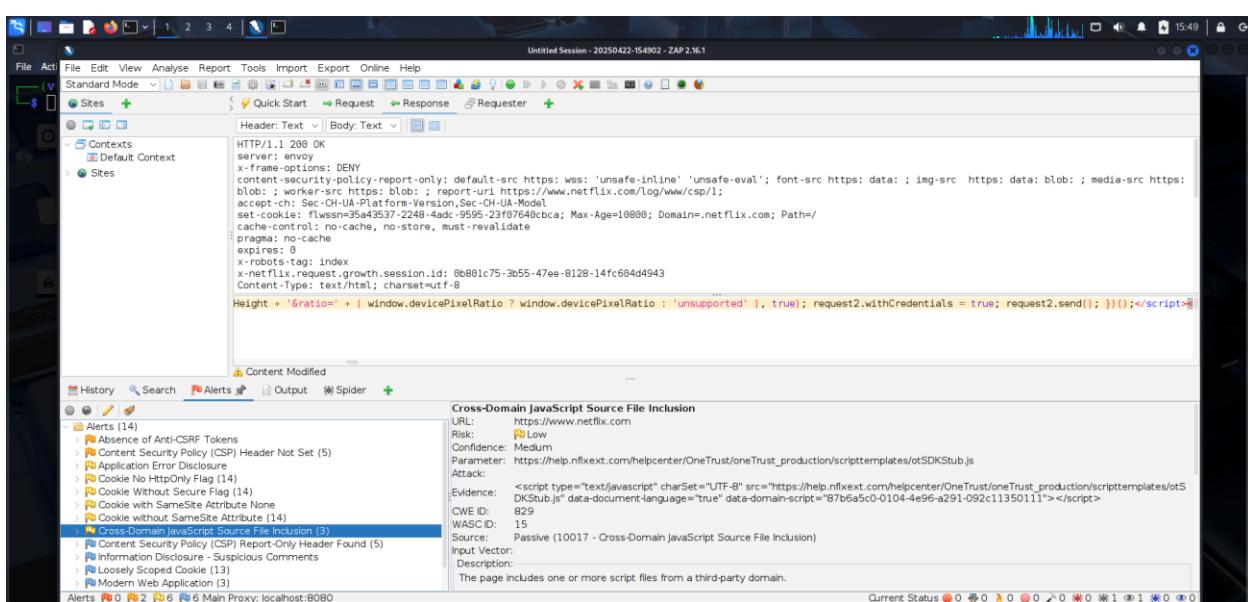
# OWASP ZAP

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](#) ]

The screenshot shows a web browser window with the title 'ZAP by Checkmark Scanning' and the URL 'file:///home/vishmi/2025-04-19-ZAP-Report-.html'. The browser has several tabs open, including 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit.DB', 'Google Hacking DB', and 'OffSec'. The main content area displays two tables from the report.

**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.)

Risk	User Confirmed	Confidence				Total
		High	Medium	Low		
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.)

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

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

## Vulnerabilities

<b>a.Vulnerability Title</b>	<b>Cross-Domain JavaScript Source File Inclusion</b>
<b>b.Vulnerability Description</b>	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.
<b>c.Affected Components</b>	Cross-domain JavaScript file sources in the HTTP response
<b>d.Impact Assessment</b>	This might be used by attackers to run malicious JavaScript, which could result in phishing, data negotiate, or illegal access.
<b>e.Steps to Reproduce</b>	<ol style="list-style-type: none"><li>1. The HTTP response body and headers with development tools or a proxy.</li><li>2. If any JavaScript source files are being loaded from outside domains, note them down.</li><li>3. To verify these files' vulnerability to malicious injections, try altering or intercepting them.</li></ol>
<b>f.Proof of Concept (if applicable)</b>	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.
<b>g.Proposed Mitigation or Fix</b>	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*

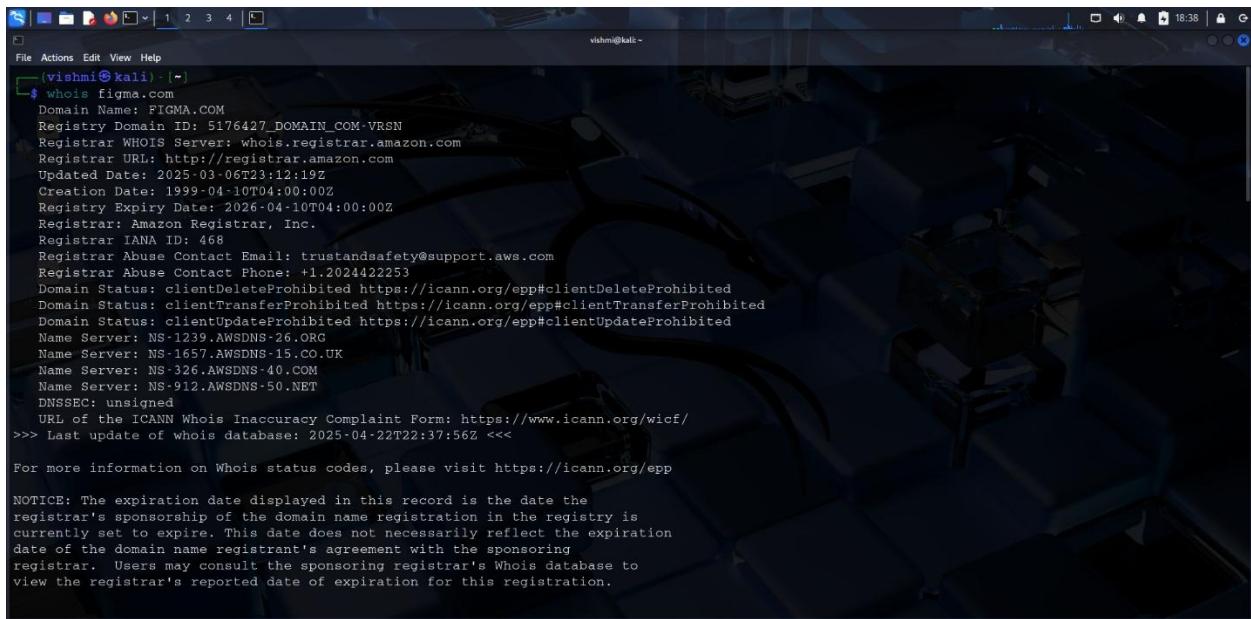
**Domain** = *figma.com*

**Sub-domain** = *go.figma.com*

**URL** = *https://www.figma.com*

# Target Reconnaissance

## Introduction to Figma and Audit Scope



```
vishmi@kali: ~]$ whois figma.com
Domain Name: FIGMA.COM
Registry Domain ID: 5176427_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon.com
Registrar URL: http://registrar.amazon.com
Updated Date: 2025-03-06T23:12:09Z
Creation Date: 1999-04-10T04:00:00Z
Registry Expiry Date: 2026-04-10T04:00:00Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: trustandsafety@support.aws.com
Registrar Abuse Contact Phone: +1.2024422253
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS-1239.AWSDNS-26.ORG
Name Server: NS-1657.AWSDNS-15.CO.UK
Name Server: NS-326.AWSDNS-40.COM
Name Server: NS-912.AWSDNS-50.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-22T22:37:56Z <<<
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

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.

The screenshot shows a list of assets under the 'Scope' tab on the HackerOne platform. The search bar is set to 'All scopes', maximum severity is 'Any', and bounty eligibility is 'All'. The table lists the following assets:

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
Figma Atlassian App <a href="https://marketplace.atlassian.com/apps/1217865/figma-for-jira">https://marketplace.atlassian.com/apps/1217865/figma-for-jira</a>	Other	In scope	Critical	Eligible	Sep 30, 2020	1 (1%)
Figma for Microsoft Teams <a href="https://appsource.microsoft.com/en-us/product/office/wa200004521?tab=overview">https://appsource.microsoft.com/en-us/product/office/wa200004521?tab=overview</a>	Other	In scope	Critical	Eligible	Oct 12, 2022	0 (0%)
Figma iOS and Android apps	Other	In scope	Critical	Eligible	Sep 22, 2022	0 (0%)
Figma Slack App	Other	In scope	Critical	Eligible	Oct 12, 2022	0 (0%)

The screenshot shows a list of assets under the 'Scope' tab on the HackerOne platform. The search bar is set to 'All scopes', maximum severity is 'Any', and bounty eligibility is 'All'. The table lists the following assets:

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
Figma Desktop App	Other	In scope	Critical	Eligible	Sep 22, 2022	5 (3%)
api.figma.com	Domain	In scope	Critical	Eligible	Sep 30, 2020	9 (6%)
www.figma.com	Domain	In scope	Critical	Eligible	Sep 30, 2020	135 (85%)
www.designsystems.com	Domain	Out of scope	None	Ineligible	Oct 3, 2020	0 (0%)

## **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.

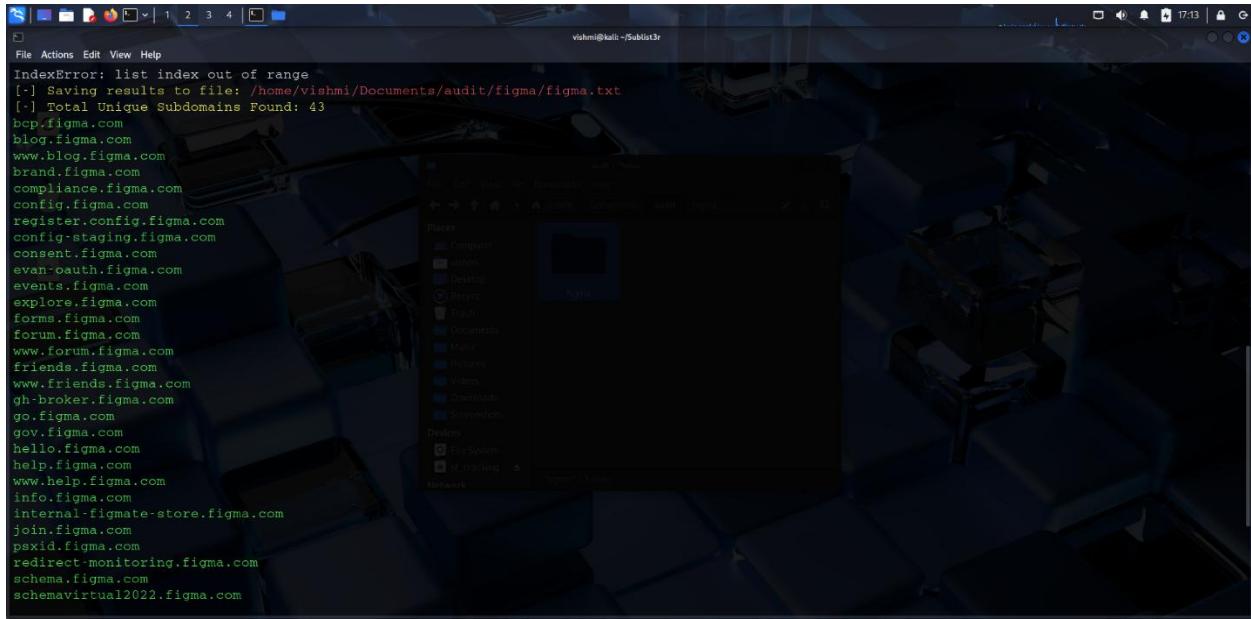
Path to .txt file = **home/vishmi/Documents/audit/figma/figma.txt**

```
vishmi㉿kali:~$ sudo mkdir -p /home/vishmi/Documents/audit/figma
[sudo] password for vishmi:
[vishmi㉿kali:~$ sudo touch /home/vishmi/Documents/audit/figma/figma.txt
[vishmi㉿kali:~$ cd Sublist3r
[vishmi㉿kali:~/Sublist3r]$ sudo python3 sublist3r.py -d figma.com -o /home/vishmi/Documents/audit/figma/figma.txt
[sudo] password for vishmi:
/home/vishmi/Sublist3r/sublist3r.py:78: SyntaxWarning: invalid escape sequence '\_'
    \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_
/home/vishmi/Sublist3r/sublist3r.py:286: SyntaxWarning: invalid escape sequence '\/'
link_regex = re.compile('<cite.*?(&.*?)</cite>')
/home/vishmi/Sublist3r/sublist3r.py:343: SyntaxWarning: invalid escape sequence '\/'
link = re.sub('<(\w/)?b>', "", link)
/home/vishmi/Sublist3r/sublist3r.py:439: SyntaxWarning: invalid escape sequence '\/'
link = re.sub('<(\w/)?strong>|<span.*?>|<br>', '', link)
/home/vishmi/Sublist3r/sublist3r.py:658: SyntaxWarning: invalid escape sequence '\/'
tbl_regex = re.compile('<a name="hostanchor"></a>Host Records.*?<table.*?(&.*?)</table>', re.S)
/home/vishmi/Sublist3r/sublist3r.py:898: SyntaxWarning: invalid escape sequence '\.'
domain_check = re.compile("^(http|https)?:[a-zA-Z0-9]+([-\.\w]{1}[a-zA-Z0-9]+)*\.[a-zA-Z]{2,}$")
```

# Coded By Ahmed Aboul-Ela - @aboul3la

```
[+] Enumerating subdomains now for figma.com
[+] Searching now in Baidu..
[+] Searching now in Yahoo..
[+] Searching now in Google..
[+] Searching now in Bing..
[+] Searching now in Ask..
[+] Searching now in Netcraft..
```

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



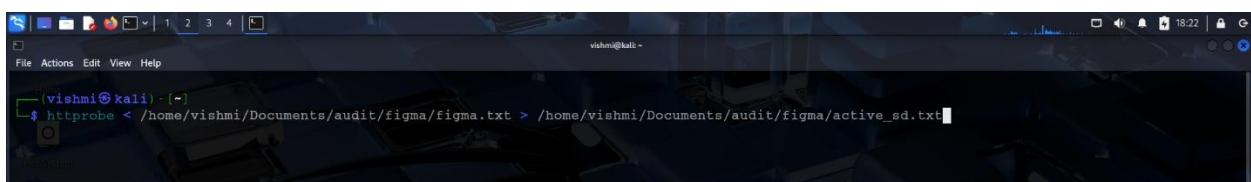
```
vishni@kali:~/Sublist3r
```

```
File Actions Edit View Help
IndexError: list index out of range
[!] Saving results to file: /home/vishni/Documents/audit/figma/figma.txt
[!] Total Unique Subdomains Found: 43
bep.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-auth.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
psnid.figma.com
redirect-monitoring.figma.com
schema.figma.com
schemavirtual2022.figma.com
```

## HTTProbe

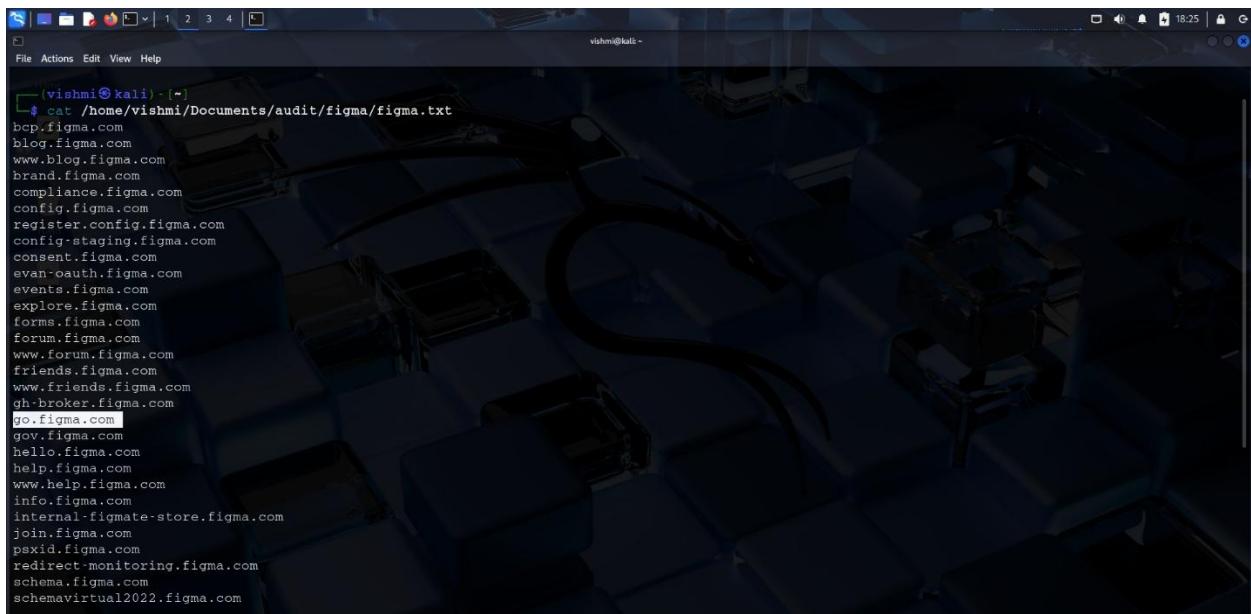
HTTProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing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



```
vishmi@kali:~$ httpprobe </home/vishmi/Documents/audit/figma/figma.txt >/home/vishmi/Documents/audit/figma/active_sd.txt
```

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

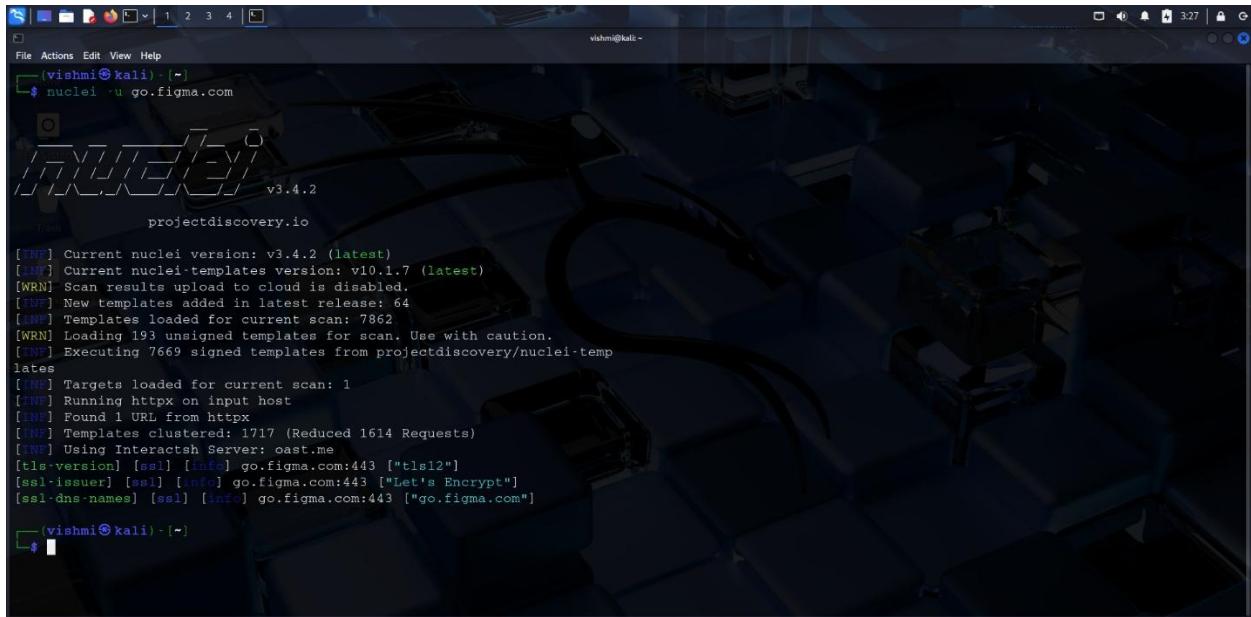


```
vishmi@kali:~$ cat /home/vishmi/Documents/audit/figma/figma.txt
bcp.figma.com
blog.figma.com
www.blog.figma.com
brand.figma.com
compliance.figma.com
config.figma.com
register.config.figma.com
config-staging.figma.com
consent.figma.com
evan-oauth.figma.com
events.figma.com
explore.figma.com
forms.figma.com
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
pxid.figma.com
redirect-monitoring.figma.com
schema.figma.com
schemavirtual2022.figma.com
```

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).



```
vishmi㉿kali:~$ nuclei -u go.figma.com
v3.4.2
projectdiscovery.io

[INFO] Current nuclei version: v3.4.2 (latest)
[INFO] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 64
[INFO] Templates loaded for current scan: 7862
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[INFO] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[INFO] Targets loaded for current scan: 1
[INFO] Running httpx on input host
[INFO] Found 1 URL from httpx
[INFO] Templates clustered: 1717 (Reduced 1614 Requests)
[INFO] Using Interactsh Server: east.me
[tls-version] [ssl] [http] go.figma.com:443 ["tls12"]
[ssl-issuer] [ssl] [info] go.figma.com:443 ["Let's Encrypt"]
[ssl-dns-names] [ssl] [info] go.figma.com:443 ["go.figma.com"]

[vishmi㉿kali:~]$
```

Vulnerable Title	Description	Risk
<b>SSL/TLS Certificate Expiry</b>	SSL/TLS certificate expired for go.figma.com:443.	High
<b>Mismatched SSL Certificate</b>	SSL certificate domain doesn't match the actual domain.	High
<b>Self-Signed SSL Certificate</b>	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.

```
vishni㉿kali: ~]$ sqlmap -h
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 03:34:25 /2025-04-23/
[03:34:25] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('__cf_bm=L4uGd5is8...9qNu8vhj9K'). Do you want to use those [Y/n] Y
[03:34:26] [INFO] checking if the target is protected by some kind of WAF/IPS
[03:34:26] [CRITICAL] WAF/IPS identified as 'CloudFlare'
are you sure that you want to continue with further target testing? [Y/n] Y
[03:34:26] [WARNING] please consider usage of tamper scripts (option '--tamper')
[03:34:26] [INFO] testing if the target URL content is stable
[03:34:26] [INFO] target URL content is stable
[03:34:26] [INFO] testing if parameter 'User-Agent' is dynamic
[03:34:27] [WARNING] parameter 'User-Agent' does not appear to be dynamic
```

<b>Option</b>	<b>Meaning</b>
<b>-u</b>	For basic testing, the target URL is required.
<b>--level5</b>	Increases the number of payloads and tests that are done (maximum is 5).
<b>--risk3</b>	Increase the danger level of the payloads used (maximum is 3)
<b>--batch</b>	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

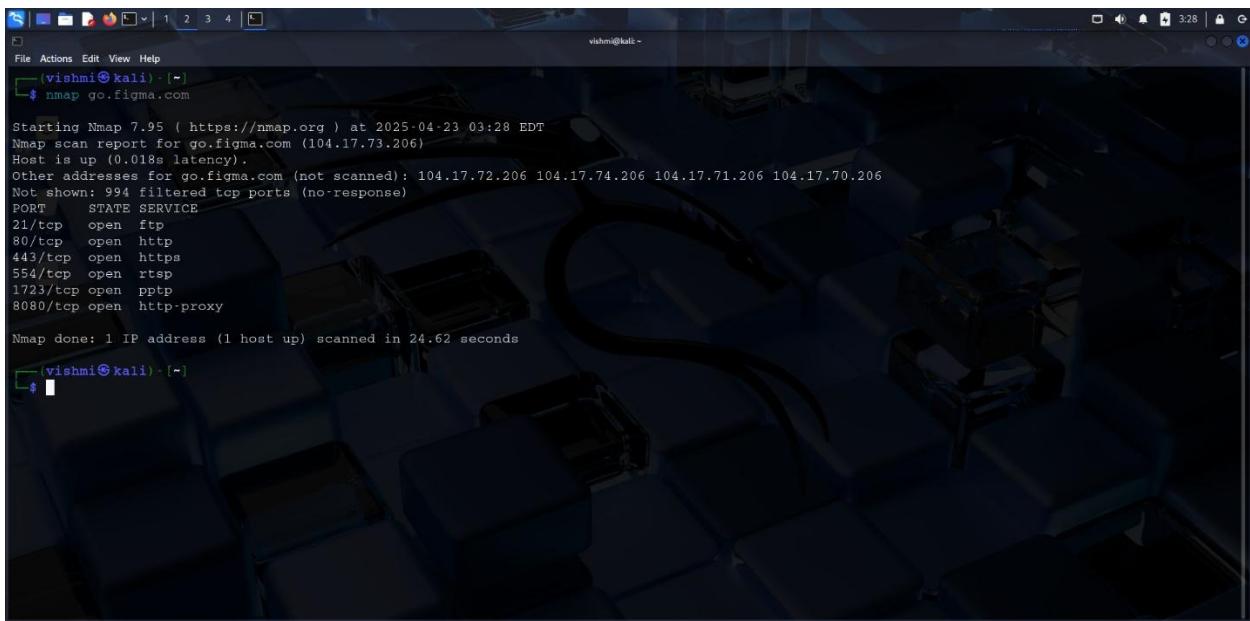
[This is a *potential* vulnerability, but not confirmed.]

\* **[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.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal window title is '(vishmi㉿kali)-[\*]'. The command entered is 'nmap go.figma.com'. The output of the scan is displayed:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 03:28 EDT
Nmap scan report for go.figma.com (104.17.73.206)
Host is up (0.018s latency).
Other addresses for go.figma.com (not scanned): 104.17.72.206 104.17.74.206 104.17.71.206 104.17.70.206
Not shown: 994 filtered tcp ports (no-response)
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

Nmap done: 1 IP address (1 host up) scanned in 24.62 seconds
```

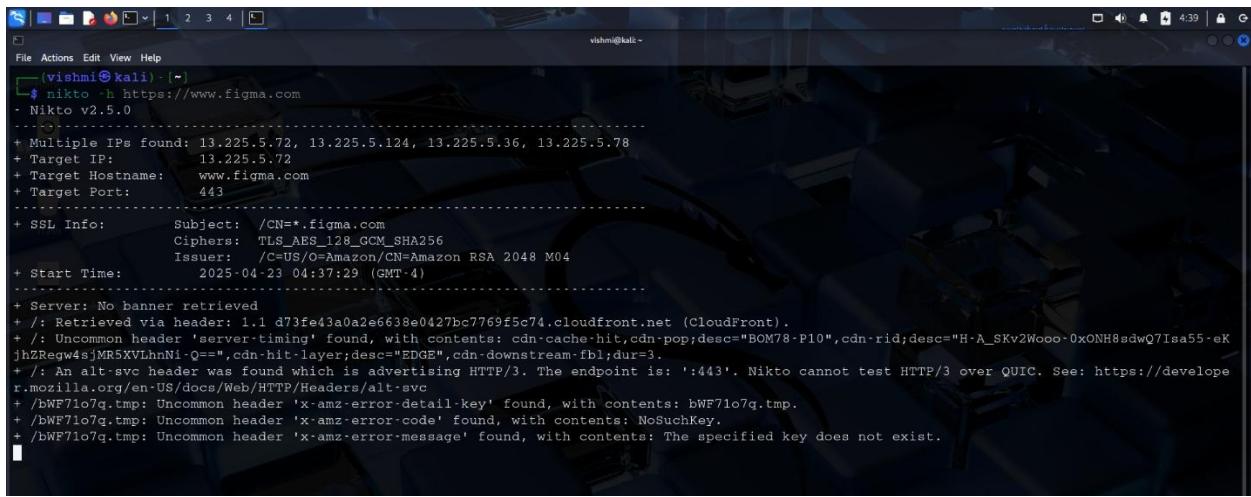
I discovered these details by using Nmap to search *go.figma.com*.

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

<b>PORT</b>	<b>SERVICE</b>	<b>Vulnerabilities</b>
<b>21/tcp</b>	ftp	Unencrypted credentials are accepted.
<b>80/tcp</b>	http	Transmits plain text data.
<b>443/tcp</b>	https	Deprecated TLS versions are supported.
<b>554/tcp</b>	Rtsp	Usually doesn't have authenticity.
<b>1723/tcp</b>	pptp	Makes use of a weak encryption
<b>8080/tcp</b>	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.



```
vishni@kali:~$ nikto -h https://www.figma.com
[Nikto v2.5.0]
-----[Output from Nikto scan against https://www.figma.com]-----
```

The terminal window shows the execution of the command `nikto -h https://www.figma.com`. The output indicates that multiple IPs were found (13.225.5.72, 13.225.5.124, 13.225.5.36, 13.225.5.78), the target IP is 13.225.5.72, the target hostname is www.figma.com, and the target port is 443. The SSL info section details the subject (/CN=\*.figma.com), ciphers (TLS\_AES\_128\_GCM\_SHA256), issuer (C=US/O=Amazon/CN=Amazon RSA 2048 M04), and start time (2025-04-23 04:37:29). The server section notes that no banner was retrieved and lists various headers found, such as 'server-timing' and 'x-amz-error-message'. The output ends with a note about Nikto's inability to test HTTP/3 over QUIC.

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 .

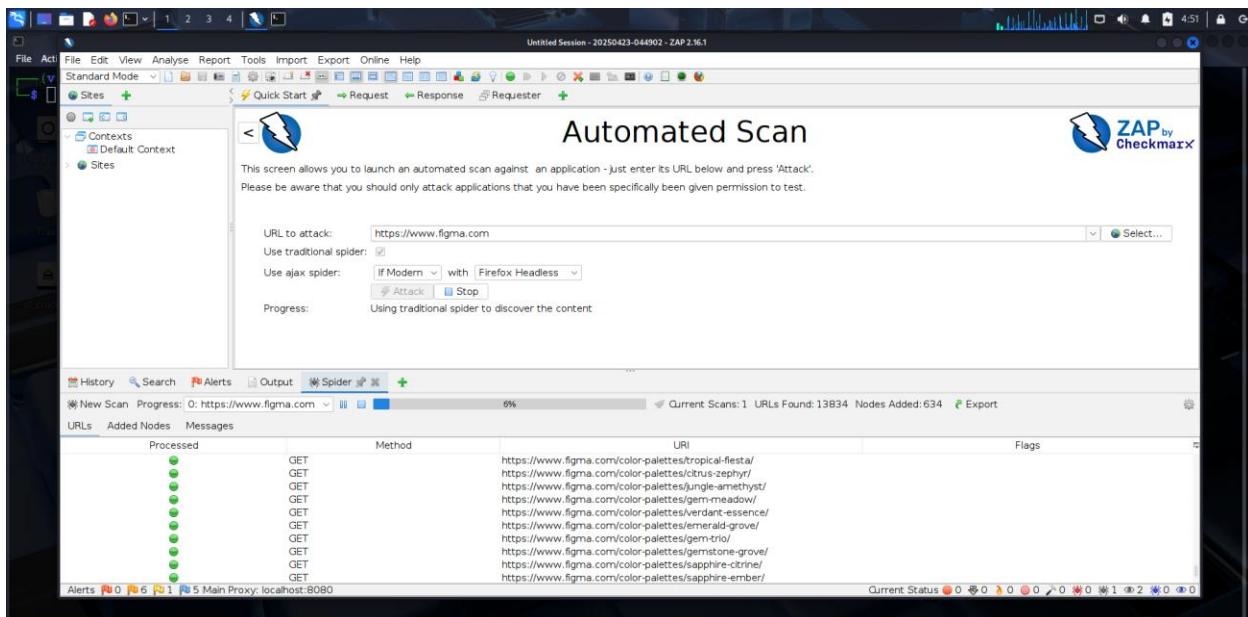


A screenshot of the VirusTotal URL analysis results for the URL "https://www.figma.com". The page shows a "Community Score" of 0 / 97. It states "No security vendors flagged this URL as malicious". The URL is listed as "https://www.figma.com/" and "www.figma.com". The status is 200, the content type is "text/html; charset=utf-8", and the last analysis date is "1 hour ago". Below this, there are tabs for DETECTION, DETAILS, and COMMUNITY (12). A green banner encourages users to "Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.". A table titled "Security vendors' analysis" lists results from various engines: Abusix (Clean), ADMINUSLabs (Clean), AlienVault (Clean), Artists Against 419 (Clean), BitDefender (Clean), Blueliv (Clean), Acronis (Clean), AI Labs (MONITORAPP) (Clean), Anti-AVL (Clean), benkow.cc (Clean), BlockList (Clean), and Certego (Clean). A "Do you want to automate checks?" button is located on the right. A blue speech bubble icon is in the bottom right corner.

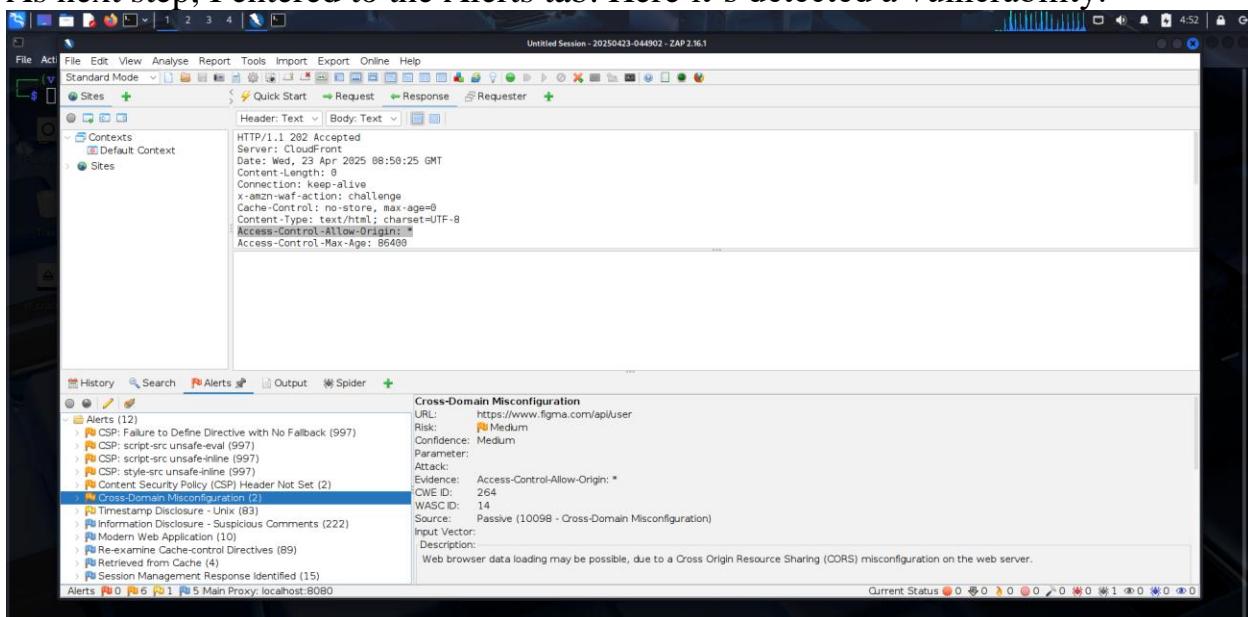
## OWASP ZAP

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](#) ]

The image displays two screenshots of a ZAP report generated on 2025-04-23. The top screenshot shows the 'Summaries' section, specifically the 'Alert counts by risk and confidence' table. The bottom screenshot shows the 'Alert counts by site and risk' table for the domain <https://www.figma.com>.

**Summaries - Alert counts by risk and confidence**

Risk	User Confirmed	Confidence				Total
		High	Medium	Low		
High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	
Medium	0 (0.0%)	5 (41.7%)	1 (8.3%)	0 (0.0%)	6 (50.0%)	
Low	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (8.3%)	1 (8.3%)	
Informational	0 (0.0%)	0 (0.0%)	3 (25.0%)	2 (16.7%)	5 (41.7%)	
Total	0 (0.0%)	5 (41.7%)	4 (33.3%)	3 (25.0%)	12 (100%)	

**Alert counts by site and risk**

Site	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
<a href="https://www.figma.com">https://www.figma.com</a>	0 (0)	6 (6)	1 (7)	5 (12)

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

## Vulnerabilities

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

## **Report-04**

# Web Audit

# *temu.com*

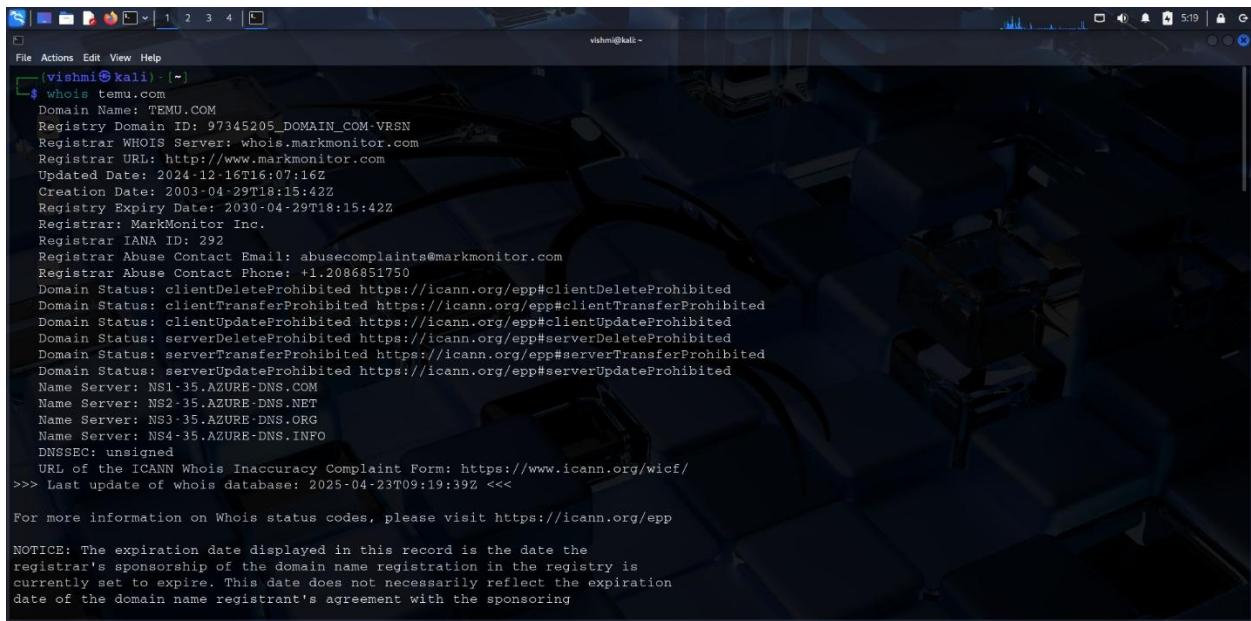
**Domain** = *temu.com*

**Sub-domain** = *ads.temu.com*

**URL** = *https://www.temu.com*

# Target Reconnaissance

## Introduction to Temu and Audit Scope



```
vishni@kali: ~]$ whois temu.com
Domain Name: TEMU.COM
Registry Domain ID: 97345205_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-12-16T16:07:16Z
Creation Date: 2003-04-29T18:15:42Z
Registry Expiry Date: 2030-04-29T18:15:42Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1-35.AZURE-DNS.COM
Name Server: NS2-35.AZURE-DNS.NET
Name Server: NS3-35.AZURE-DNS.ORG
Name Server: NS4-35.AZURE-DNS.INFO
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-23T09:19:39Z <<
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
```

**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.

The screenshot shows the HackerOne interface for the Temu bug bounty program. The left sidebar has a navigation menu with options like Security page, Program guidelines, and Scope (which is currently selected). The main content area is titled "Scope" and includes search and filter fields for "Search", "Scope" (set to "All scopes"), "Maximum severity" (set to "Any"), and "Bounty eligibility" (set to "All"). Below these are download links for "Download Burp Suite Project Configuration File", "Download CSV", and "View changes (Last updated on November 28, 2023) 1-3 of 3". A progress bar indicates "95%" completion. The main table lists three assets:

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
com.einnovation.temu	Android: Play Store	In scope	Critical	Eligible	Nov 22, 2023	2 (11%)
www.temu.com	Domain	In scope	Critical	Eligible	Nov 3, 2023	15 (79%)
1641486558	iOS: App Store	In scope	Critical	Eligible	Nov 22, 2023	1 (5%)

At the bottom, there are links for Opportunities, Security, Leaderboard, Blog, Status, Docs, Support, Disclosure Guidelines, Press, Privacy, and Term.

## **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

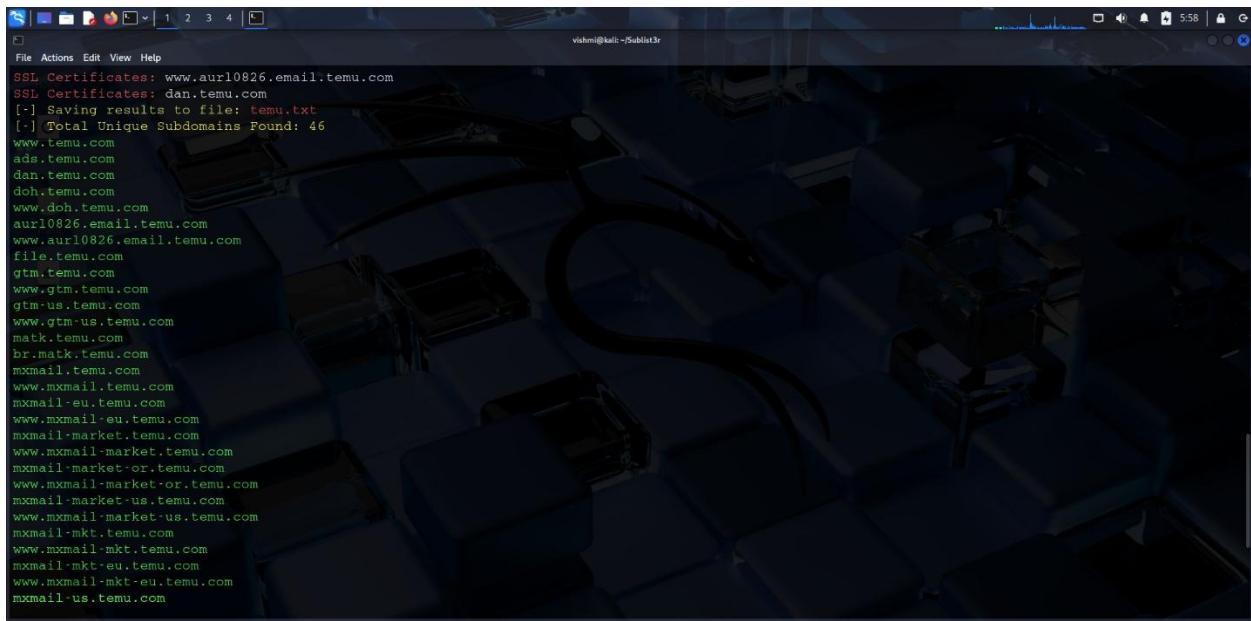
Sublist3r is an open-source Python application that uses OSINT (Open Source Intelligence) techniques to quickly and effectively scan subdomains. Subdomains linked to a target domain can be found by penetration testers, security researchers, and bug bounty hunters using a variety of search engine queries (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***

```
vishmi@kali:~/Sublist3r
[vishmi@kali:~]
$ sudo mkdir -p /home/vishmi/Documents/audit/temu
[sudo] password for vishmi:
[vishmi@kali:~]
$ sudo touch /home/vishmi/Documents/audit/temu/temu.txt
[vishmi@kali:~]
$ cd Sublist3r
[vishmi@kali:~/Sublist3r]
$ [vishmi@kali:~/Sublist3r]
$ python3 sublist3r.py -d temu.com -v > temu.txt
/home/vishmi/Sublist3r/sublist3r.py:78: SyntaxWarning: invalid escape sequence '\'
  \ | | | | | | | | / | | | | | | | | | | | | | | | |
/home/vishmi/Sublist3r/sublist3r.py:286: SyntaxWarning: invalid escape sequence '\'
  link_regex = re.compile('<cite.*?>(.*)</cite>')
/home/vishmi/Sublist3r/sublist3r.py:343: SyntaxWarning: invalid escape sequence '\'
  link = re.sub("<(/)?b>", "", link)
/home/vishmi/Sublist3r/sublist3r.py:439: SyntaxWarning: invalid escape sequence '\'
  link = re.sub('<(/)?strong>|<span.*?>|<|>', '', link)
/home/vishmi/Sublist3r/sublist3r.py:658: SyntaxWarning: invalid escape sequence '\'
  tbl_regex = re.compile('a name="hostanchor"></a>Host Records.*?<table.*?>(.*)</table>', re.S)
/home/vishmi/Sublist3r/sublist3r.py:898: SyntaxWarning: invalid escape sequence '\'
  domain_check = re.compile("^(http|https)?[a-zA-Z0-9]+((\.-\.){1}[a-zA-Z0-9]+)*\.[a-zA-Z]{2,}$")
# Coded By Ahmed Aboul-Ela - @aboul3la
[+] Enumerating subdomains now for temu.com
```

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

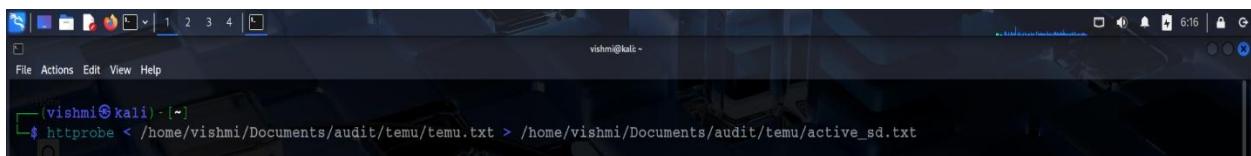


```
vishnu@kali: ~/Sublist3r
File Actions Edit View Help
SSL Certificates: www.aur10826.email.temu.com
SSL Certificates: dan.temu.com
[!] Saving results to file: temu.txt
[!] Total Unique Subdomains Found: 46
www.temu.com
ads.temu.com
dan.temu.com
doh.temu.com
www.doh.temu.com
aur10826.email.temu.com
www.aur10826.email.temu.com
file.temu.com
gtm.temu.com
www.gtm.temu.com
gtm-us.temu.com
www.gtm-us.temu.com
matk.temu.com
br.matk.temu.com
mxmail.temu.com
www.mxmail.temu.com
mxmail-eu.temu.com
www.mxmail-eu.temu.com
mxmail-market.temu.com
www.mxmail-market.temu.com
mxmail-market-or.temu.com
www.mxmail-market-or.temu.com
mxmail-market-us.temu.com
www.mxmail-market-us.temu.com
mxmail-mkt.temu.com
www.mxmail-mkt.temu.com
mxmail-mkt-eu.temu.com
www.mxmail-mkt-eu.temu.com
mxmail-us.temu.com
```

## HTTPProbe

HTTPProbe 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.



```
vishmi@kali:~$ httpprobe </home/vishmi/Documents/audit/temu/temu.txt >/home/vishmi/Documents/audit/temu/active_sd.txt
```

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

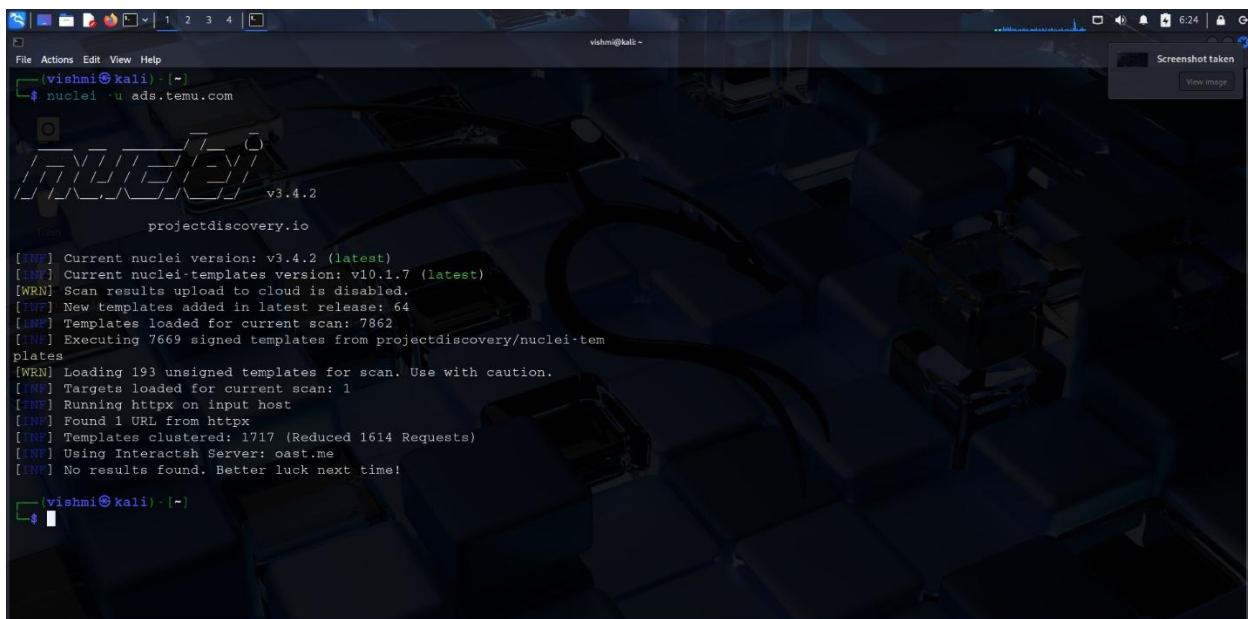


```
vishmi@kali:~$ cat /home/vishmi/Documents/audit/temu/temu.txt
ads.temu.com
dan.temu.com
doh.temu.com
www.doh.temu.com
aur10826.email.temu.com
www.aur10826.email.temu.com
file.temu.com
gtm.temu.com
www.gtm.temu.com
gtm-us.temu.com
www.gtm-us.temu.com
matk.temu.com
br.matk.temu.com
mxmail.temu.com
www.mxmail.temu.com
mxmail.eu.temu.com
www.mxmail-eu.temu.com
mxmail-market.temu.com
www.mxmail-market.temu.com
mxmail-market-or.temu.com
www.mxmail-market-or.temu.com
mxmail-market-us.temu.com
www.mxmail-market-us.temu.com
mxmail-mkt.temu.com
```

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).



```
vishni@kali: ~$ nuclei -u ads.temu.com
[✓] v3.4.2
[✓] projectdiscovery.io

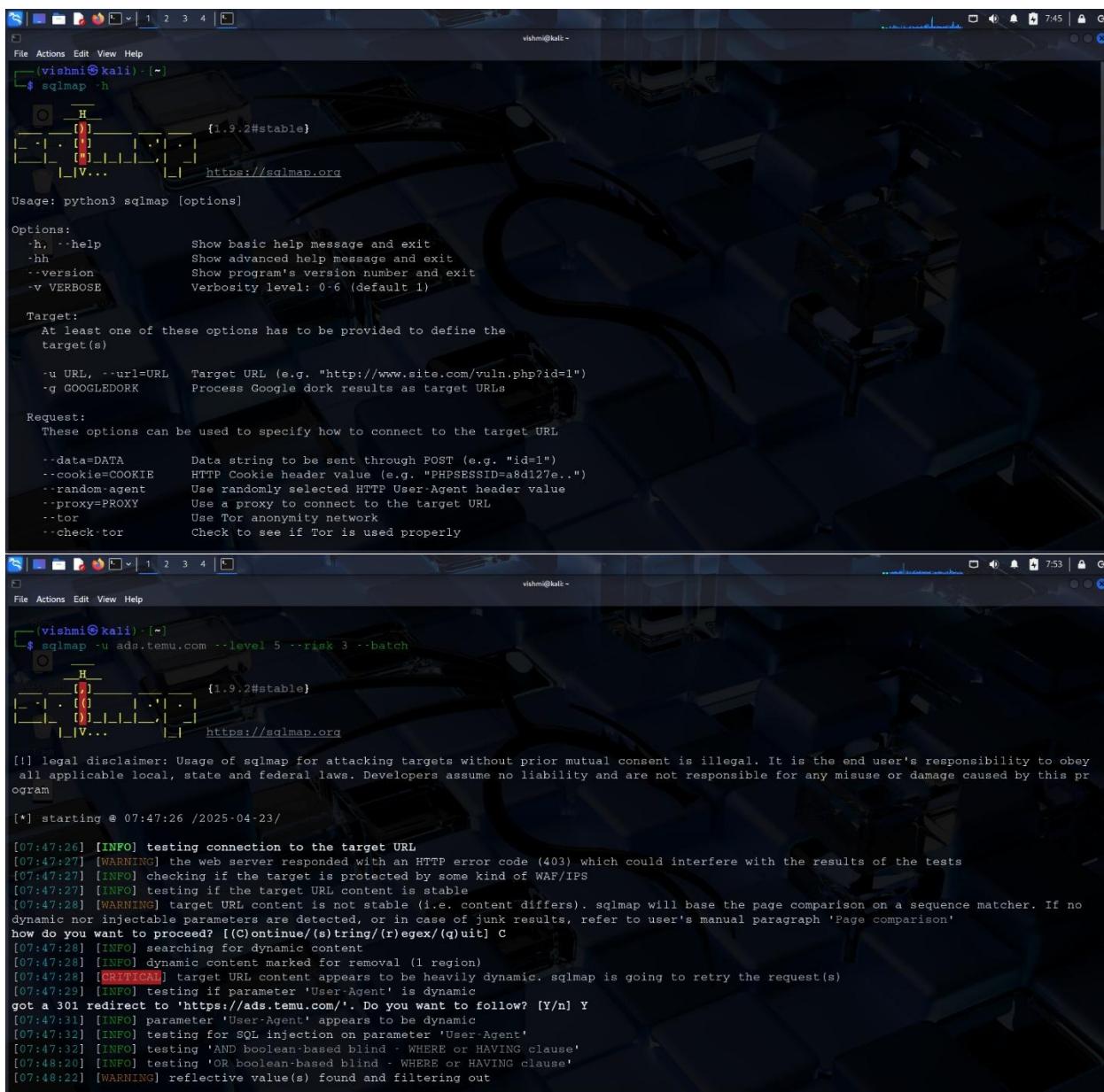
[INF] Current nuclei version: v3.4.2 (latest)
[INF] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 64
[INF] Templates loaded for current scan: 7862
[INF] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1717 (Reduced 1614 Requests)
[INF] Using Interactsh Server: oast.me
[INF] No results found. Better luck next time!

[vishni@kali: ~]$
```

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.



The screenshot shows two terminal windows side-by-side. Both windows are running on a Kali Linux desktop environment, indicated by the desktop icons at the top and the terminal title bar 'vishni@kali:~'.

The left terminal window displays the help documentation for the `sqlmap` command:

```
vishni@kali:~$ sqlmap -h
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

Usage: python3 sqlmap [options]

Options:
-h, --help          Show basic help message and exit
--hh               Show advanced help message and exit
--version          Show program's version number and exit
-v VERBOSE         Verbosity level: 0-6 (default 1)

Target:
At least one of these options has to be provided to define the target(s)

-u URL, --url=URL  Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-g GOOGLEDORK      Process Google dork results as target URLs

Request:
These options can be used to specify how to connect to the target URL

--data=DATA        Data string to be sent through POST (e.g. "id=1")
--cookie=COOKIE    HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
--random-agent     Use randomly selected HTTP User-Agent header value
--proxy=PROXY       Use a proxy to connect to the target URL
--tor              Use Tor anonymity network
--check-tor        Check to see if Tor is used properly
```

The right terminal window shows the execution of `sqlmap` against the target URL `ads.temu.com`:

```
vishni@kali:~$ sqlmap -u ads.temu.com --level 5 --risk 3 --batch
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 07:47:26 /2025-04-23

[07:47:26] [INFO] testing connection to the target URL
[07:47:27] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
[07:47:27] [INFO] checking if the target is protected by some kind of WAF/IPS
[07:47:27] [INFO] testing if the target URL content is stable
[07:47:28] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison' how do you want to proceed? [(C)ontinue/(S)tring/(R)eexec/(Q)uit] C
[07:47:28] [INFO] searching for dynamic content
[07:47:28] [INFO] dynamic content marked for removal (1 region)
[07:47:28] [CRITICAL] target URL content appears to be heavily dynamic. sqlmap is going to retry the request(s)
[07:47:29] [INFO] testing if parameter 'User-Agent' is dynamic
got a 301 redirect to 'https://ads.temu.com/'. Do you want to follow? [Y/n] Y
[07:47:31] [INFO] parameter 'User-Agent' appears to be dynamic
[07:47:32] [INFO] testing for SQL injection on parameter 'User-Agent'
[07:47:32] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:48:20] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[07:48:22] [WARNING] reflective value(s) found and filtering out
```

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

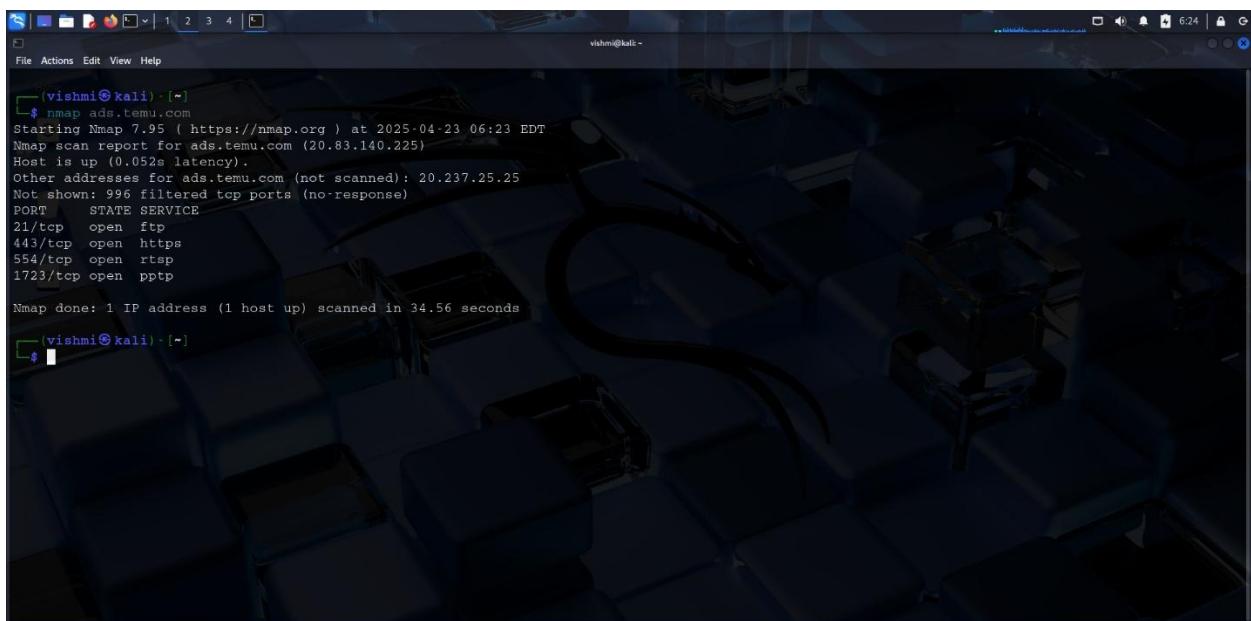
## **Detected Information**

- \* **[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.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running the command `nmap ads.temu.com`. The output of the scan is displayed, showing the host is up with 0.052s latency. It lists open ports: 21/tcp (FTP), 443/tcp (HTTPS), 554/tcp (RTSP), and 1723/tcp (PPTP). Other addresses for ads.temu.com (not scanned) are listed as 20.237.25.25. The scan took 34.56 seconds. The terminal prompt ends with a dollar sign.

```
vishmi㉿kali:~$ nmap ads.temu.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 06:23 EDT
Nmap scan report for ads.temu.com (20.83.140.225)
Host is up (0.052s latency).
Other addresses for ads.temu.com (not scanned): 20.237.25.25
Not shown: 996 filtered top ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 34.56 seconds
vishmi㉿kali:~$
```

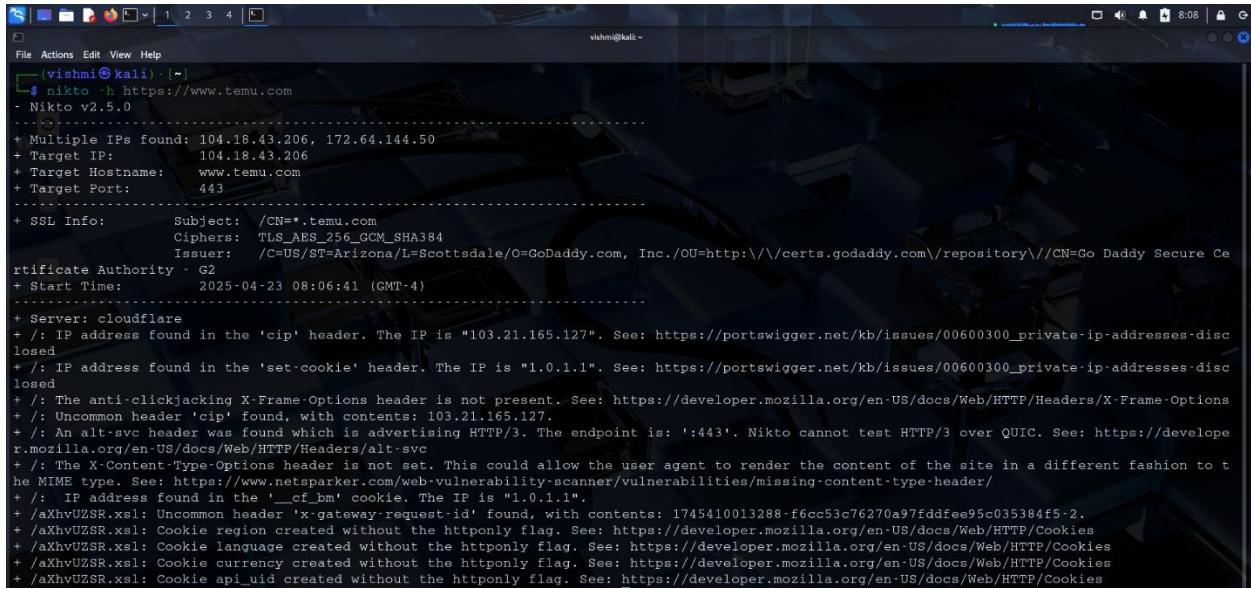
I discovered these details by using Nmap to search *ads.temu.org*.

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.



```
vishni@kali:~$ nikto -h https://www.temu.com
- Nikto v2.5.0
-----
+ Multiple IPs found: 104.18.43.206, 172.64.144.50
+ Target IP: 104.18.43.206
+ Target Hostname: www.temu.com
+ Target Port: 443
-----
+ SSL Info: Subject: /CN=*.temu.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Ce
rtificate Authority - G2
+ Start Time: 2025-04-23 08:06:41 (GMT-4)
-----
+ Server: cloudflare
+/: IP address found in the 'cip' header. The IP is "103.21.165.127". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+/: IP address found in the 'set-cookie' header. The IP is "1.0.1.1". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+/: Uncommon header 'cip' found, with contents: 103.21.165.127.
+/: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+/: IP address found in the '__cf_bm' cookie. The IP is "1.0.1.1".
+ /xhvUZSR.xsl: Uncommon header 'x-gateway-request-id' found, with contents: 1745410013288-f6cc53c76270a97fddfee95c035384f5-2.
+ /xhvUZSR.xsl: Cookie region created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /xhvUZSR.xsl: Cookie language created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /xhvUZSR.xsl: Cookie currency created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /xhvUZSR.xsl: Cookie api_uid created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
```

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 .

The screenshot shows two consecutive screenshots of the VirusTotal URL analysis interface. Both screenshots are from a dark-themed browser window with a blue header bar containing the address bar and navigation buttons.

**Screenshot 1 (Top):** The title bar says "VirusTotal - Home". The address bar shows "virustotal.com/gui/home/url". Below the address bar is a search bar with the placeholder "URL, IP address, domain or file hash". The main heading is "Σ VIRUSTOTAL". A sub-instruction reads "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community." Below this are three tabs: "FILE", "URL" (which is selected), and "SEARCH". In the center is a globe icon. Below the globe is a text input field containing "https://www.temu.com". Below the input field is a "Search" button. At the bottom of the page, a note states: "By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Notice](#), and to the **sharing of your URL submission with the security community**. Please do not submit any personal information; we are not responsible for the contents of your submission. [Learn more](#)".

**Screenshot 2 (Bottom):** The title bar says "VirusTotal - URL". The address bar shows "virustotal.com/gui/url/23b5a1361e0b7ed42a98129f15ba1444c8f3836fdb5d45784aebe99d505a515". Below the address bar is a search bar with the placeholder "https://www.temu.com/". The main heading is "Σ VIRUSTOTAL". On the left is a circular "Community Score" icon with a green border and a white center, showing "0 / 97". Below it is a "Community Score" button with the number "1". To the right of the score are buttons for "Rerunalyze", "Search", and "More". Below the score area is a table with the following data:

https://www.temu.com/	www.temu.com	Status	Content type	Last Analysis Date
text/html	external-resources	200	text/html; charset=UTF-8	31 minutes ago

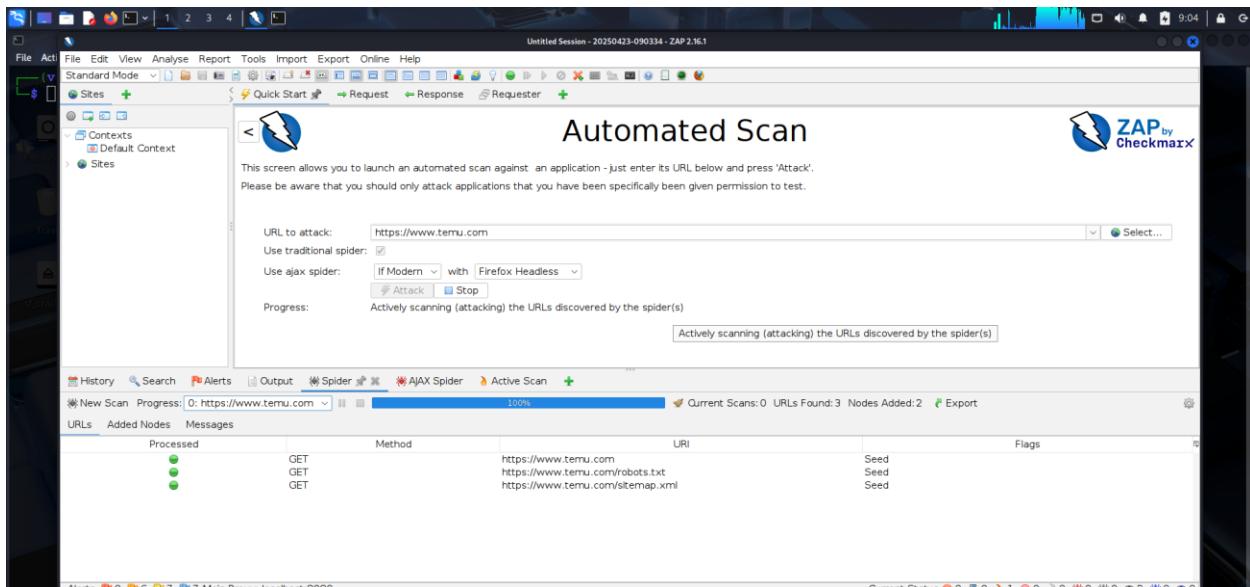
Below the table are three tabs: "DETECTION" (selected), "DETAILS", and "COMMUNITY" (with a count of 9). A green banner at the bottom encourages users to "Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).". At the very bottom, there is a table titled "Security vendors' analysis" with columns for vendor name, detection status (Clean), and a "Do you want to automate checks?" checkbox. The table lists the following vendors:

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AI Labs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean
BitDefender	Clean	BlockList	Clean

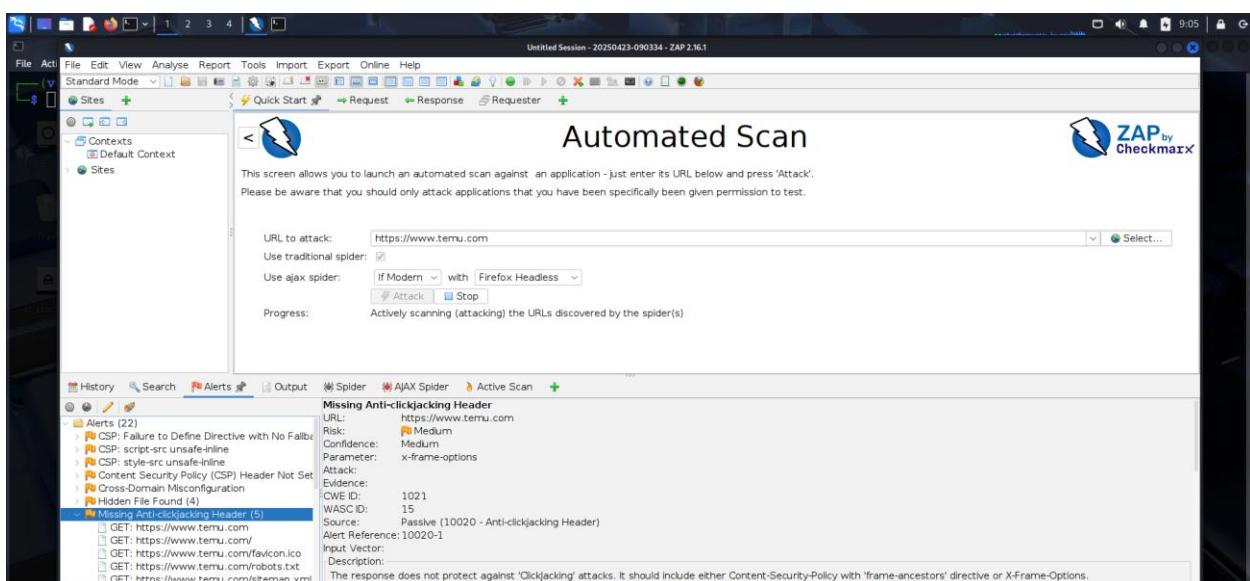
# OWASP ZAP

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.)

Risk	User Confirmed	Confidence				Total
		High	Medium	Low		
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.)

Site	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informati onal)
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 Checkmark Scanning + file:///home/vishnu/2025-04-23-ZAP-Report-.html

Kali Linux Kali Tools Kali Docs Kali Forums 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
<a href="#">CSP: Failure to Define Directive with No Fallback</a>	Medium	1 (4.5%)
<a href="#">CSP: script-src unsafe-inline</a>	Medium	1 (4.5%)
<a href="#">CSP: style-src unsafe-inline</a>	Medium	1 (4.5%)
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	5 (22.7%)
<a href="#">Cross-Domain Misconfiguration</a>	Medium	1 (4.5%)
<a href="#">Hidden File Found</a>	Medium	4 (18.2%)
<a href="#">Missing Anti-clickjacking Header</a>	Medium	5 (22.7%)
<a href="#">Timestamp Disclosure - Unix</a>	Low	6 (27.3%)
<a href="#">X-Content-Type-Options Header Missing</a>	Low	5 (22.7%)
<a href="#">Content Security Policy (CSP) Report-Only Header Found</a>	Informational	1 (4.5%)
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	3 (13.6%)
<a href="#">Loosely Scoped Cookie</a>	Informational	6 (27.3%)
<a href="#">Modern Web Application</a>	Informational	7 (31.8%)
<a href="#">Re-examine Cache-control Directives</a>	Informational	4 (18.2%)
<a href="#">Retrieved from Cache</a>	Informational	1 (4.5%)
<a href="#">Session Management Response Identified</a>	Informational	6 (27.3%)
<a href="#">User Agent Fuzzer</a>	Informational	55 (250.0%)
Total		22

# Vulnerabilities

<b>a.Vulnerability Title</b>	<b>Missing Anti-Clickjacking Header</b>
<b>b.Vulnerability Description</b>	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.
<b>c.Affected Components</b>	The target domain's server configuration and response headers.
<b>d.Impact Assessment</b>	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.
<b>e.Steps to Reproduce</b>	<ol style="list-style-type: none"><li>1.Create a simple HTML page embedding the target site in an iframe: <pre>html=&lt;iframe src="http://target-site.com" style="width:100%; height:100%;"&gt;&lt;/iframe&gt;</pre></li><li>2.Load the HTML page in a browser.</li><li>3.Verify that the embedded site loads successfully within the iframe, confirming the absence of an anti-clickjacking mechanism.</li></ol>
<b>f.Proof of Concept (if applicable)</b>	Include a screenshot showing the site successfully embedded within an iframe, demonstrating its vulnerability to clickjacking.
<b>g.Proposed Mitigation or Fix</b>	Add the <b>X-Frame-Options</b> header to HTTP responses to prevent embedding

## **Report-05**

# **Web Audit**

# ***ring.com***

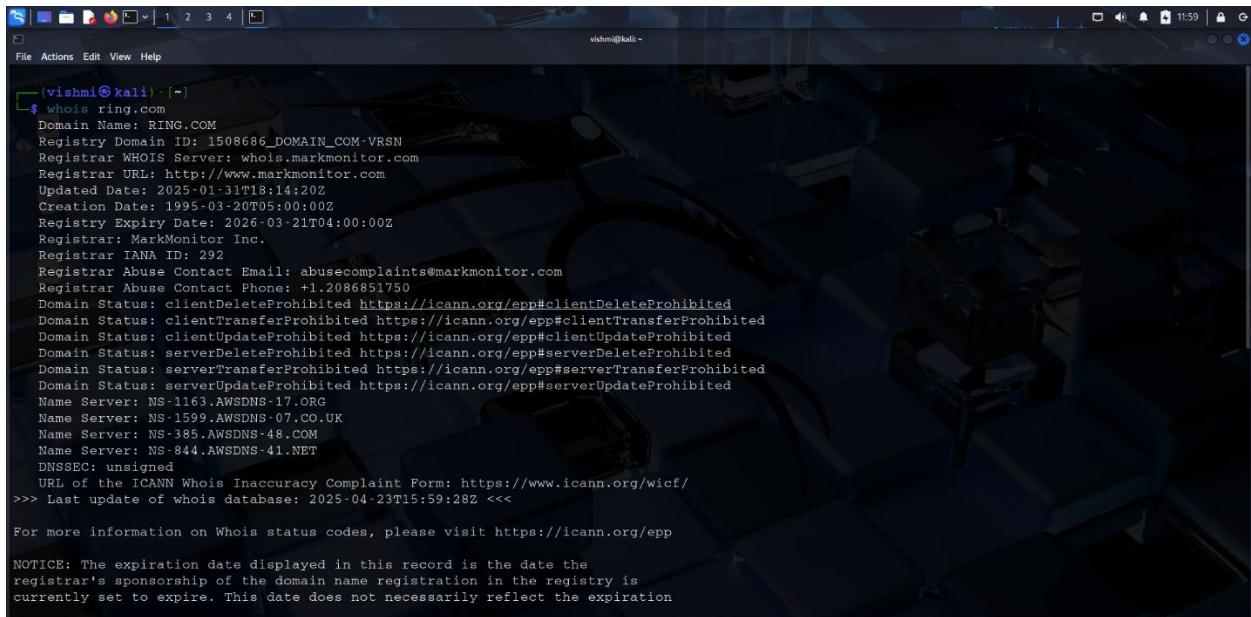
**Domain = *ring.com***

**Sub-domain = *admin.ring.com***

**URL = *https://www.ring.com***

# Target Reconnaissance

Introduction to Sony and Audit Scope



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running a WHOIS query for the domain 'ring.com'. The output provides detailed information about the domain's registration, including the registrar (MarkMonitor Inc.), creation date (1995-03-20T05:00:00Z), and expiration date (2026-03-21T04:00:00Z). It also lists several name servers (NS-1163.AWSDNS-17.ORG, NS-1599.AWSDNS-07.CO.UK, NS-385.AWSDNS-48.COM, NS-844.AWSDNS-41.NET) and notes that DNSSEC is unsigned. A notice at the bottom states that the expiration date is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire.

```
vishmi㉿kali:~$ whois ring.com
Domain Name: RING.COM
Registry Domain ID: 1508686_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2025-01-31T18:14:20Z
Creation Date: 1995-03-20T05:00:00Z
Registry Expiry Date: 2026-03-21T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS-1163.AWSDNS-17.ORG
Name Server: NS-1599.AWSDNS-07.CO.UK
Name Server: NS-385.AWSDNS-48.COM
Name Server: NS-844.AWSDNS-41.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-23T15:59:28Z <<<
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
```

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

The screenshots show the 'Scope' section of the Ring bug bounty program configuration page on the HackerOne platform. Both pages display a table of assets with columns for Asset name, Type, Coverage, Max. severity, Bounty, Last update, and Resolved Reports.

**Screenshot 1 (Top):** This screenshot shows three assets in the 'In scope' category:

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
https://fw.ring.com/*	Other	In scope	Critical	Eligible	Jan 16, 2024	0 (0%)
Video Doorbell 2nd Gen, 3 & 3 Plus, ASINs: B0849J7W5X, B08N5NQ869, B07WLP395R	Hardware/IoT	In scope	Critical	Eligible	Jan 16, 2024	0 (0%)
Chime Gen 2 and 2 Pro, ASIN: B07WML2XTD, B07WML1QM4	Hardware/IoT	In scope	Critical	Eligible	Jan 16, 2024	0 (0%)
Ring Alarm Gen 2, ASIN: B07ZPMCW64	Hardware/IoT	In scope	Critical	Eligible	Jan 16, 2024	0 (0%)

**Screenshot 2 (Bottom):** This screenshot shows four assets, with the last one being 'Anything not in scope' which is listed as 'Out of scope' and 'Ineligible'.

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
https://nw.ring.com/*	Other	In scope	Critical	Eligible	Jan 16, 2024	0 (0%)
Devices Placeholder for the Rewards modal	Other	Out of scope	None	Ineligible	Jan 16, 2024	0 (0%)
Services, Apps, Mobile Placeholder for the Rewards modal	Other	Out of scope	None	Ineligible	Jan 16, 2024	0 (0%)
Anything not in scope	Other	Out of scope	None	Ineligible	Jan 16, 2024	0 (0%)

## **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

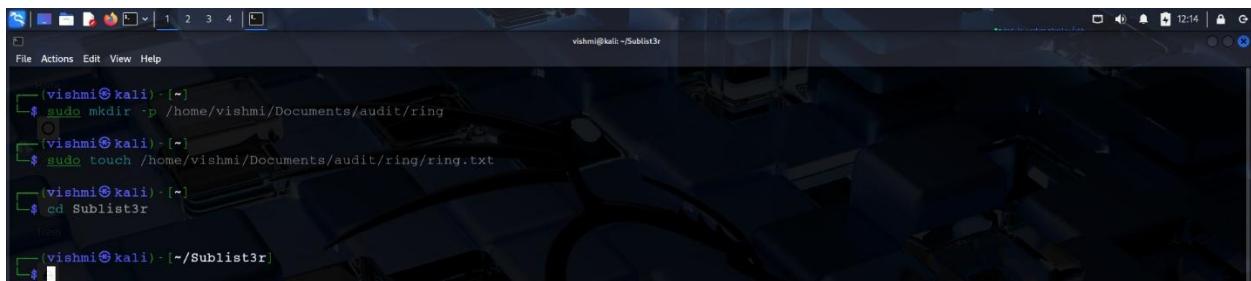
# Finding active subdomains and their states

## Sublist3r

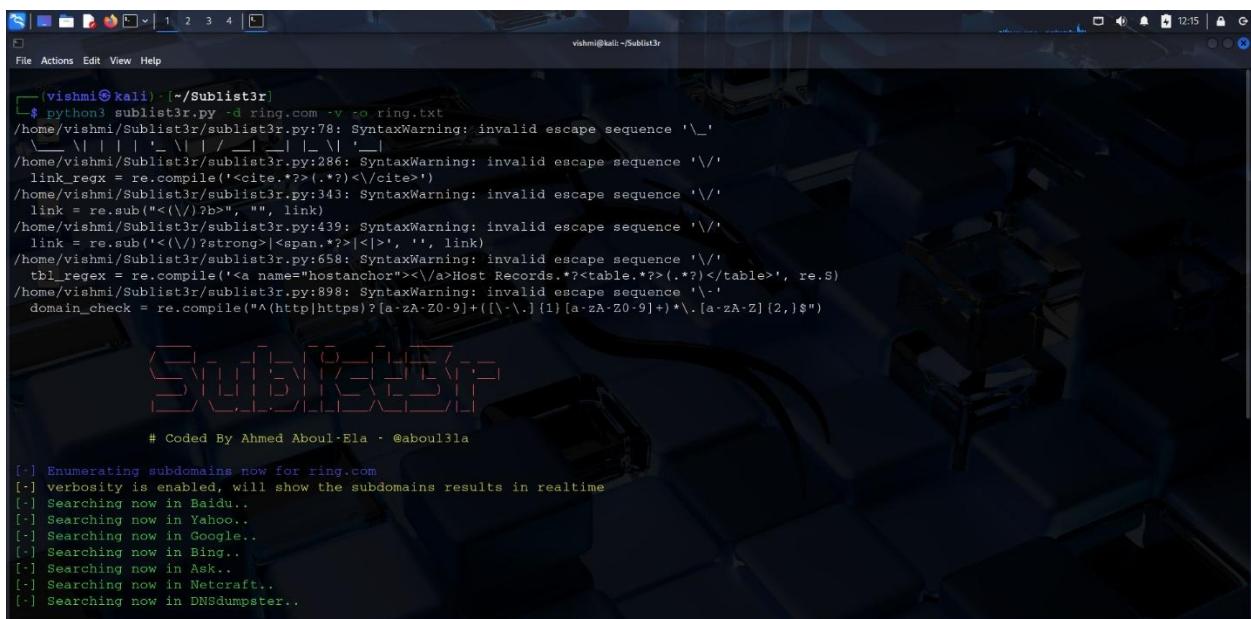
Sublist3r is an open-source Python application that uses OSINT (Open Source Intelligence) techniques to quickly and effectively scan subdomains. Subdomains linked to a target domain can be found by penetration testers, security researchers, and bug bounty hunters using a variety of search engine queries (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*



```
vishmi@kali: ~
$ sudo mkdir -p /home/vishmi/Documents/audit/ring
[vishmi@kali: ~]
$ sudo touch /home/vishmi/Documents/audit/ring/ring.txt
[vishmi@kali: ~]
$ cd Sublist3r
[vishmi@kali: ~]
$ ./sublist3r.py -d ring.com -o ring.txt
[vishmi@kali: ~/Sublist3r]
```

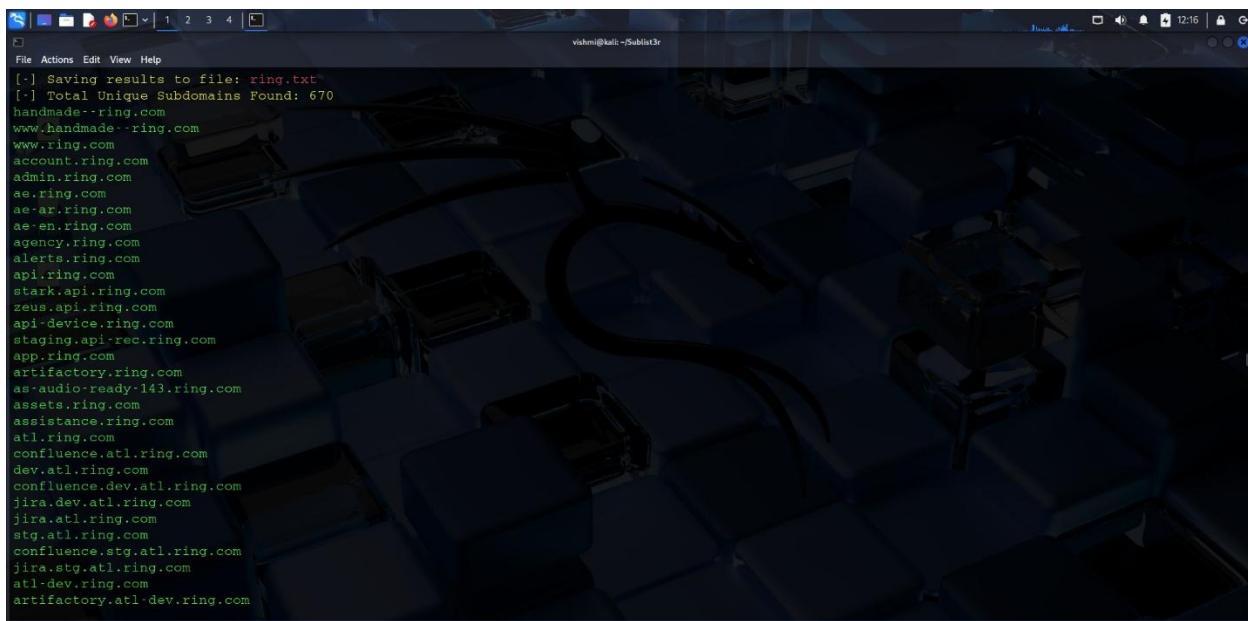


```
vishmi@kali: ~/Sublist3r
$ python3 sublist3r.py -d ring.com -o ring.txt
/home/vishmi/Sublist3r/sublist3r.py:78: SyntaxWarning: invalid escape sequence '\_'
    \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_
/home/vishmi/Sublist3r/sublist3r.py:286: SyntaxWarning: invalid escape sequence '\\'
    link_regex = re.compile('<cite.*?>(.*)?</cite>')
/home/vishmi/Sublist3r/sublist3r.py:343: SyntaxWarning: invalid escape sequence '\\'
    link = re.sub('<((\?)?b>', "", link)
/home/vishmi/Sublist3r/sublist3r.py:439: SyntaxWarning: invalid escape sequence '\\'
    link = re.sub('<(\?)?strong>|<span.*?>|<[^>]', '', link)
/home/vishmi/Sublist3r/sublist3r.py:658: SyntaxWarning: invalid escape sequence '\\'
    tbl_regex = re.compile('<a name="hostanchor"></a>Host Records.*?<table.*?(>.*?</table>', re.S)
/home/vishmi/Sublist3r/sublist3r.py:898: SyntaxWarning: invalid escape sequence '\_'
    domain_check = re.compile("^(http|https)?[a-zA-Z0-9]+([\\_.][a-zA-Z0-9]+)*.[a-zA-Z]{2,}$")
```

# Coded By Ahmed Aboul-Ela - @aboul3la

```
[+] Enumerating subdomains now for ring.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..
```

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

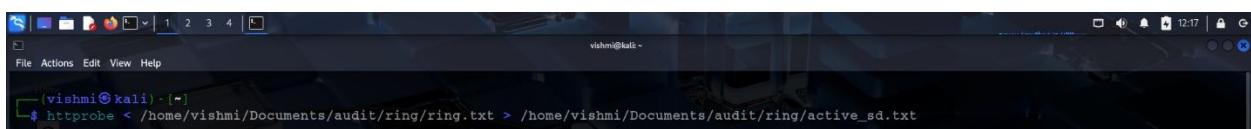


```
vishnu@kali:~/Sublist3r
File Actions Edit View Help
[-] Saving results to file: ring.txt
[-] Total Unique Subdomains Found: 670
handmade--ring.com
www.handmade--ring.com
www.ring.com
account.ring.com
admin.ring.com
as.ring.com
ae-ar.ring.com
ae-en.ring.com
agency.ring.com
alerts.ring.com
api.ring.com
stark.api.ring.com
zeus.api.ring.com
api-device.ring.com
staging.api-rec.ring.com
app.ring.com
artifactory.ring.com
as-audio-ready-143.ring.com
assets.ring.com
assistance.ring.com
atl.ring.com
confluence.atl.ring.com
dev.atl.ring.com
confluence.dev.atl.ring.com
jira.dev.atl.ring.com
jira.atl.ring.com
stg.atl.ring.com
confluence.stg.atl.ring.com
jira.stg.atl.ring.com
atl-dev.ring.com
artifactory.atl-dev.ring.com
```

## HTTPProbe

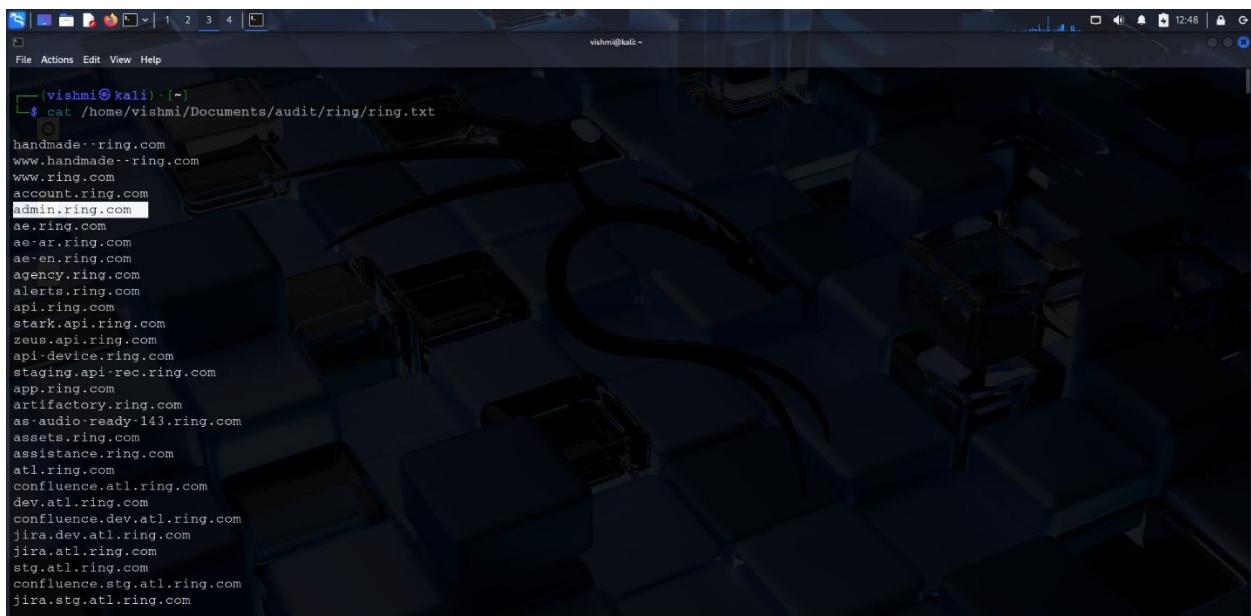
HTTPProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing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



```
vishmi@kali:~$ httpprobe < /home/vishmi/Documents/audit/ring/ring.txt > /home/vishmi/Documents/audit/ring/active_sd.txt
```

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



```
vishmi@kali:~$ cat /home/vishmi/Documents/audit/ring/ring.txt
handmade--ring.com
www.handmade--ring.com
www.ring.com
account.ring.com
admin.ring.com
ae.ring.com
ae-ar.ring.com
ae-en.ring.com
agency.ring.com
alerts.ring.com
api.ring.com
stark.api.ring.com
zeus.api.ring.com
api-device.ring.com
staging.api-rec.ring.com
app.ring.com
artifactory.ring.com
as-audio-ready-143.ring.com
assets.ring.com
assistance.ring.com
atl.ring.com
confluence.atl.ring.com
dev.atl.ring.com
confluence.dev.atl.ring.com
jira.dev.atl.ring.com
jira.atl.ring.com
stg.atl.ring.com
confluence.stg.atl.ring.com
jira.stg.atl.ring.com
```

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

## Nuclei

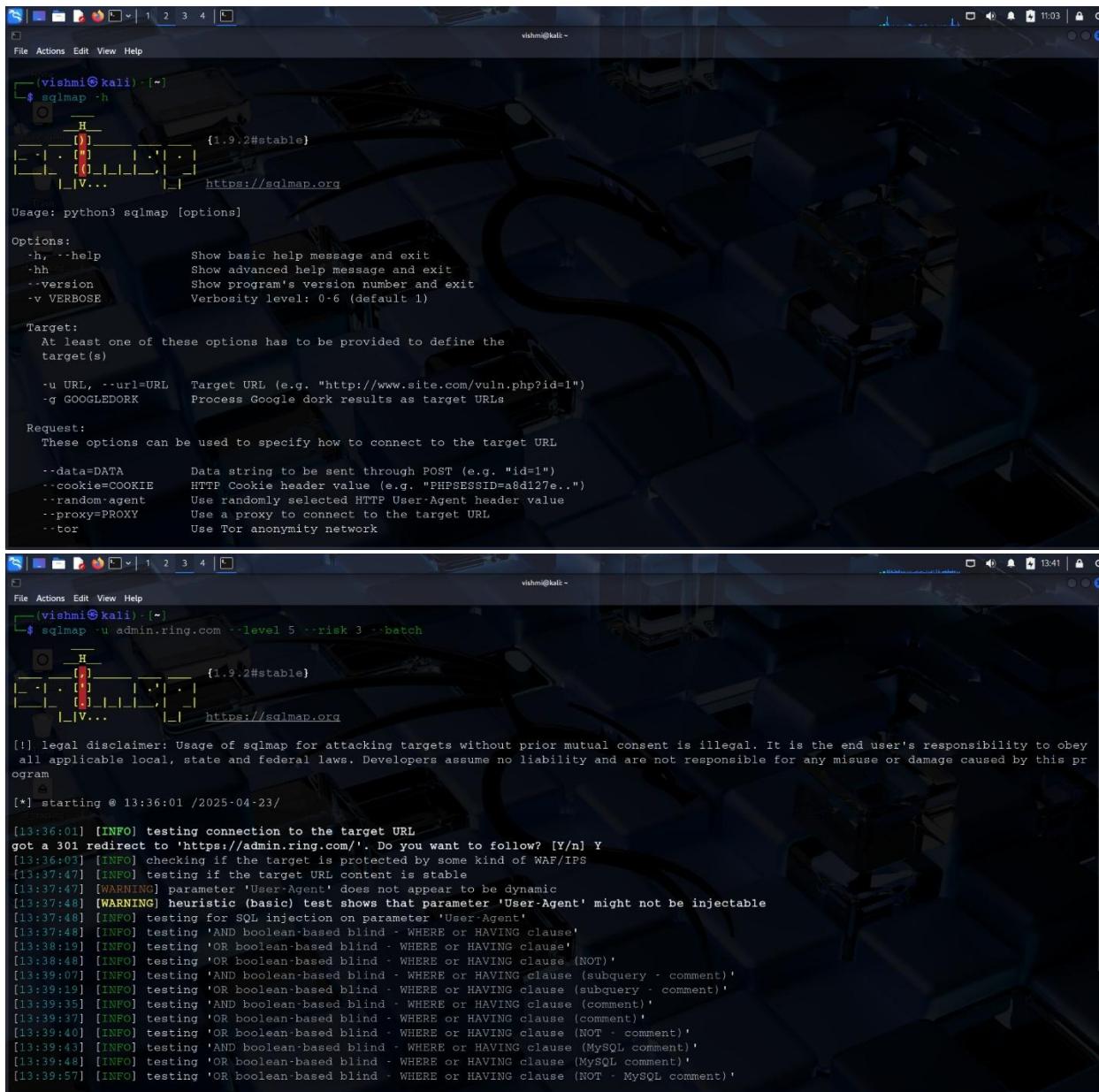
Nuclei is an open-source vulnerability scanner developed by ProjectDiscovery for security professionals, penetration testers, and bug bounty hunters. It uses customizable YAML("Yet Another Markup Language") -based templates to identify vulnerabilities such as misconfigurations, outdated software, and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

```
vishmi㉿kali:~$ nuclei -u admin.ring.com
v3.4.2
projectdiscovery.io
[INFO] Current nuclei version: v3.4.2 (latest)
[INFO] Current nuclei-templates version: v10.1.7 (latest)
[NRGN] Scan results upload to cloud is disabled.
[NRGN] New templates added in latest release: 64
[INFO] Templates loaded for current scan: 7862
[INFO] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[NRGN] Loading 193 unsigned templates for scan. Use with caution.
[INFO] Targets loaded for current scan: 1
[INFO] Running httpx on input host
[INFO] Found 1 URL from httpx
[INFO] Templates clustered: 1717 (Reduced 1614 Requests)
[INFO] Using Interactsh Server: oast.fun
[INFO] No results found. Better luck next time!
[vishmi㉿kali:~$ ]
```

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.



The screenshot shows two terminal windows side-by-side, both running on a Kali Linux desktop environment. Both windows have the title '(vishmi㉿kali) - [~]' and show the command \$ sqlmap -h being run. The output is identical in both windows, displaying the help menu for SQLmap. The help menu includes sections for Options, Target, Request, and Response, along with detailed descriptions of each option. The terminal window has a dark blue background with a futuristic cityscape graphic.

```
vishmi㉿kali: ~]$ sqlmap -h
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:36:01 /2025-04-23

[13:36:01] [INFO] testing connection to the target URL
got a 301 redirect to 'https://admin.ring.com/'. Do you want to follow? [Y/n] Y
[13:36:03] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:37:47] [INFO] testing if the target URL content is stable
[13:37:47] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[13:37:48] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[13:37:48] [INFO] testing for SQL injection on parameter 'User-Agent'
[13:37:48] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:38:19] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[13:38:48] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[13:39:07] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[13:39:19] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[13:39:35] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[13:39:37] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[13:39:40] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[13:39:43] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[13:39:48] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[13:39:57] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)',
```

Option	Meaning
<b>-u</b>	For basic testing, the target URL is required.
<b>--level5</b>	Increases the number of payloads and tests that are done (maximum is 5).
<b>--risk3</b>	Increase the danger level of the payloads used (maximum is 3)
<b>--batch</b>	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.]

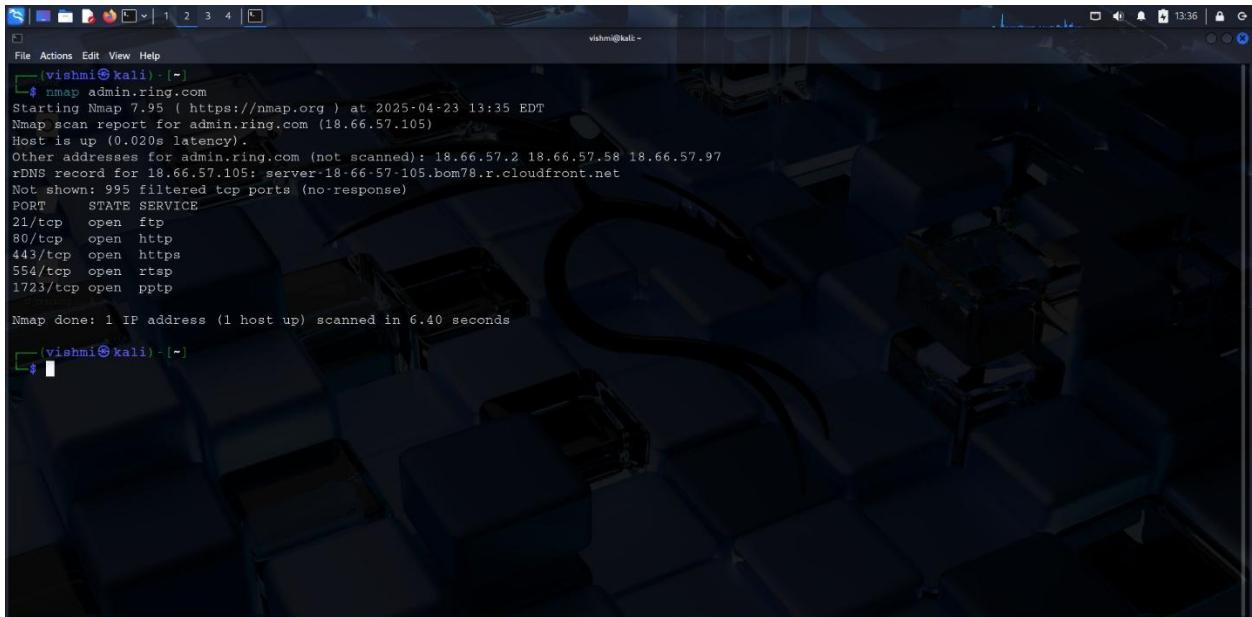
\* **[INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'**

[ 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.

A screenshot of a terminal window on a Kali Linux desktop. The terminal shows the output of an Nmap scan against the host admin.ring.com. The output includes the version of Nmap, the target IP, host status, and a table of open ports with their corresponding services.

```
vishmi㉿kali: ~]$ nmap admin.ring.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 13:35 EDT
Nmap scan report for admin.ring.com (18.66.57.105)
Host is up (0.020s latency).
Other addresses for admin.ring.com (not scanned): 18.66.57.2 18.66.57.58 18.66.57.97
rDNS record for 18.66.57.105: server-18-66-57-105.bom78.r.cloudfront.net
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 6.40 seconds
```

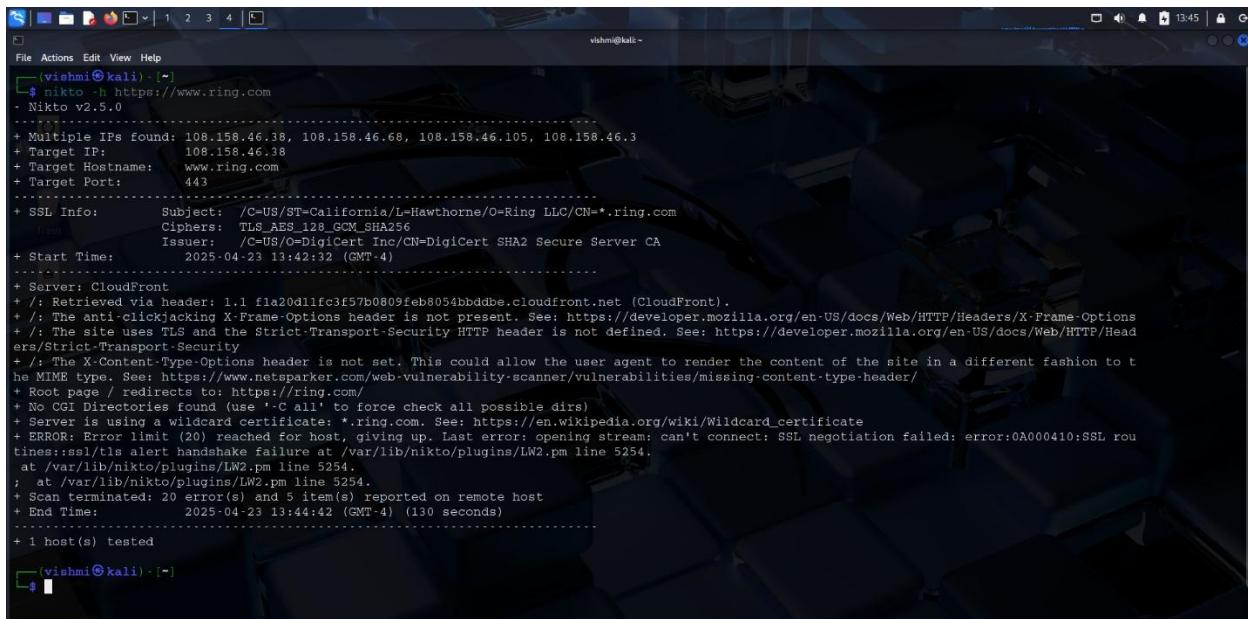
I discovered these details by using Nmap to search *admin.ring.com*.

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.



```
vishni㉿kali ~ [~]
$ nikto -h https://www.ring.com
- Nikto v2.5.0
...
+ Multiple IPs found: 108.158.46.38, 108.158.46.68, 108.158.46.105, 108.158.46.3
+ Target IP: 108.158.46.38
+ Target Hostname: www.ring.com
+ Target Port: 443
...
+ SSL Info: Subject: /C=US/ST=California/L=Hawthorne/O=Ring LLC/CN=*.ring.com
  Ciphers: TLS_AES_128_GCM_SHA256
  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
+ Start Time: 2025-04-23 13:42:32 (GMT-4)
...
+ Server: CloudFront
+ /: Retrieved via header: 1.1 f1a20d11fcf57b0809feb8054bbddbe.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to its MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://ring.com/
+ No CGI Directories Found (use '-C all' to force check all possible dirs)
+ Server is using a wildcard certificate: *.ring.com. See: https://en.wikipedia.org/wiki/Wildcard_certificate
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed; error:0A000410:SSL routines::ssl/tls alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
  at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
+ End Time: 2025-04-23 13:44:42 (GMT-4) (130 seconds)
...
+ 1 host(s) tested
vishni㉿kali ~ [~]
```

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.

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE URL SEARCH

https://www.ring.com

Search

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Notice](#), and to the [sharing of your URL submission with the security community](#). Please do not submit any personal information; we are not responsible for the contents of your submission. [Learn more](#).

Community Score 0 / 97

No security vendors flagged this URL as malicious

https://www.ring.com/  
www.ring.com

Status 200 Content type text/html; charset=utf-8 Last Analysis Date 4 days ago

text/html trackers iframes external-resources

DETECTION DETAILS COMMUNITY

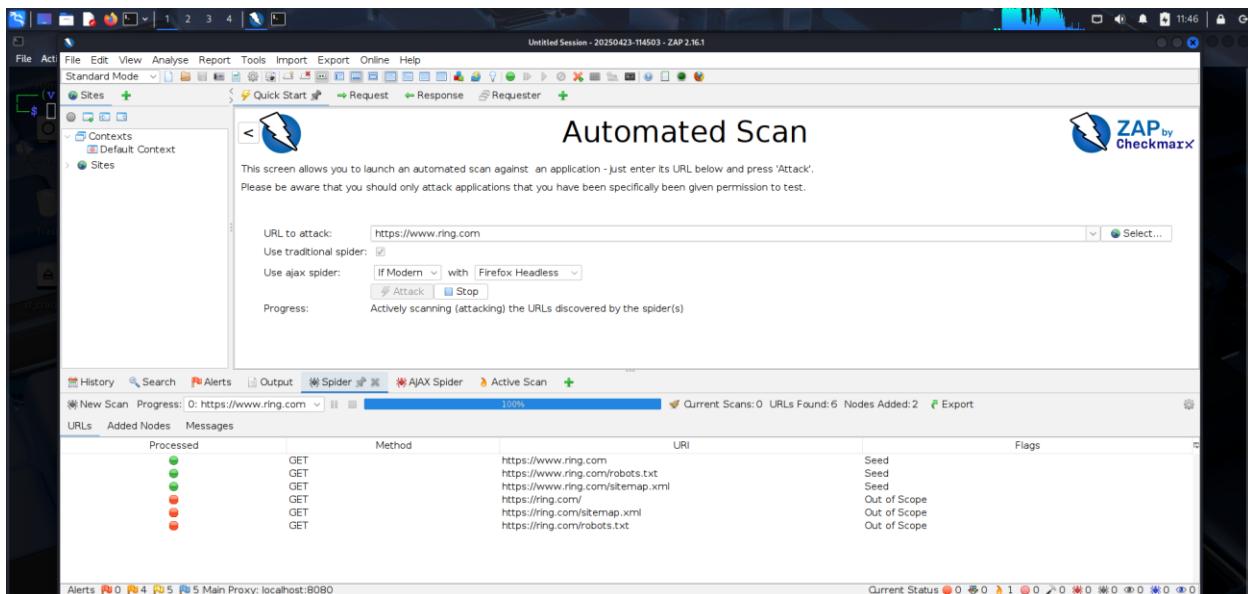
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis		Do you want to automate checks?	
Abusix	<input checked="" type="checkbox"/> Clean	Acronis	<input checked="" type="checkbox"/> Clean
ADMINUSLabs	<input checked="" type="checkbox"/> Clean	AllLabs (MONITORAPP)	<input checked="" type="checkbox"/> Clean
AlienVault	<input checked="" type="checkbox"/> Clean	Antly-AVL	<input checked="" type="checkbox"/> Clean
Artists Against 419	<input checked="" type="checkbox"/> Clean	benkow.cc	<input checked="" type="checkbox"/> Clean
BitDefender	<input checked="" type="checkbox"/> Clean	BlockList	<input checked="" type="checkbox"/> Clean
Blueliv	<input checked="" type="checkbox"/> Clean	Certego	<input checked="" type="checkbox"/> Clean

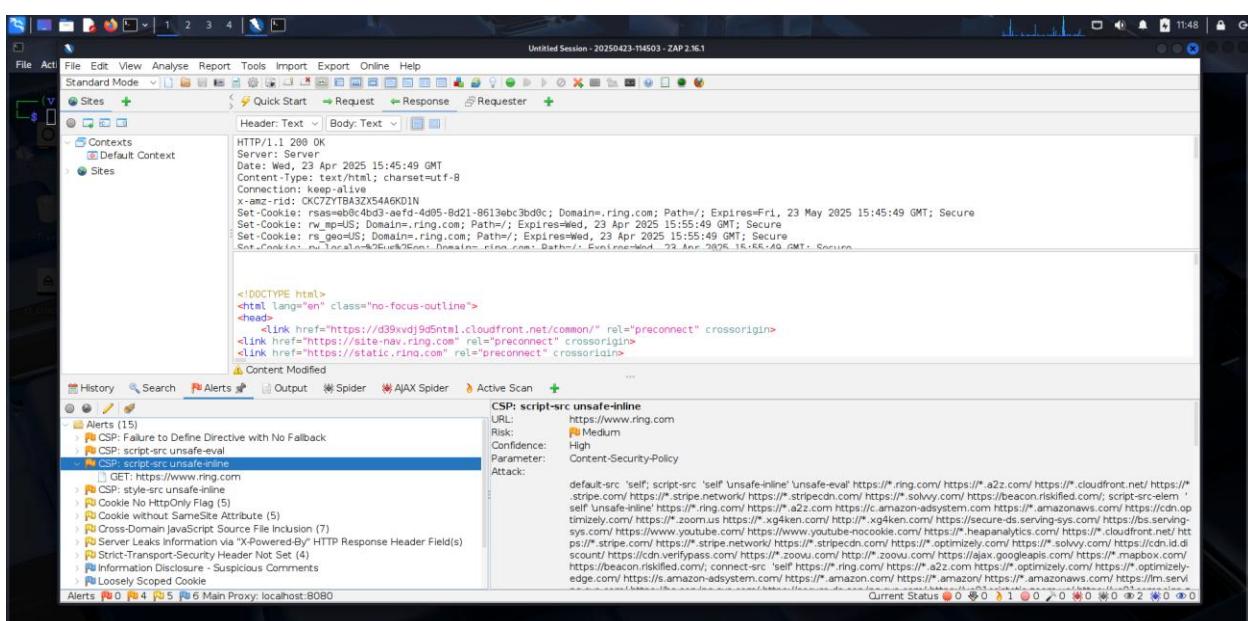
# OWASP ZAP

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](#) ]

The image displays two screenshots of a ZAP report generated by Checkmarx Scanning. The top screenshot shows the 'Summaries' section, specifically the 'Alert counts by risk and confidence' table. The bottom screenshot shows the 'Alert counts by site and risk' table for the domain <https://www.ring.com>.

**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.)

Risk	User Confirmed	Confidence				Total
		High	Medium	Low		
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.)

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

ZAP by Checkmark Scanning + file:///home/vishnu/2025-04-23-ZAP-Report-.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**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
<a href="#">CSP: Failure to Define Directive with No Fallback</a>	Medium	1 (6.7%)
<a href="#">CSP: script-src unsafe-eval</a>	Medium	1 (6.7%)
<a href="#">CSP: script-src unsafe-inline</a>	Medium	1 (6.7%)
<a href="#">CSP: style-src unsafe-inline</a>	Medium	1 (6.7%)
<a href="#">Cookie No HttpOnly Flag</a>	Low	5 (33.3%)
<a href="#">Cookie without SameSite Attribute</a>	Low	5 (33.3%)
<a href="#">Cross-Domain JavaScript Source File Inclusion</a>	Low	7 (46.7%)
<a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a>	Low	1 (6.7%)
<a href="#">Strict-Transport-Security Header Not Set</a>	Low	4 (26.7%)
<a href="#">Cookie without SameSite Attribute</a>	Low	5 (33.3%)
<a href="#">Cross-Domain JavaScript Source File Inclusion</a>	Low	7 (46.7%)
<a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a>	Low	1 (6.7%)
<a href="#">Strict-Transport-Security Header Not Set</a>	Low	4 (26.7%)
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	1 (6.7%)
<a href="#">Loosely Scoped Cookie</a>	Informational	1 (6.7%)
<a href="#">Modern Web Application</a>	Informational	1 (6.7%)
<a href="#">Re-examine Cache-control Directives</a>	Informational	1 (6.7%)
<a href="#">Session Management Response Identified</a>	Informational	1 (6.7%)
<a href="#">User Agent Fuzzer</a>	Informational	34 (226.7%)
Total		15

Screenshot taken View image

file:///home/vishnu/2025-04-23-ZAP-Report-.html#alert-type-7

## Vulnerabilities

<b>a.Vulnerability Title</b>	<b>CSP:script-src unsafe-inline</b>
<b>b.Vulnerability Description</b>	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.
<b>c.Affected Components</b>	HTTP response headers containing the CSP configuration.
<b>d.Impact Assessment</b>	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.
<b>e.Steps to Reproduce</b>	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>
<b>f.Proof of Concept (if applicable)</b>	Provide a screenshot showing the effective execution of an inline script and the CSP directive in the HTTP response headers.
<b>g.Proposed Mitigation or Fix</b>	1.Use http; [Content-Security-Policy: script-src 'self' 'nonce- <random-value>';] 2.Avoid using <i>unsafe-inline</i> entirely to ensure robust protection against XSS.

## **Report-06**

# **Web Audit**

# ***tiktok.com***

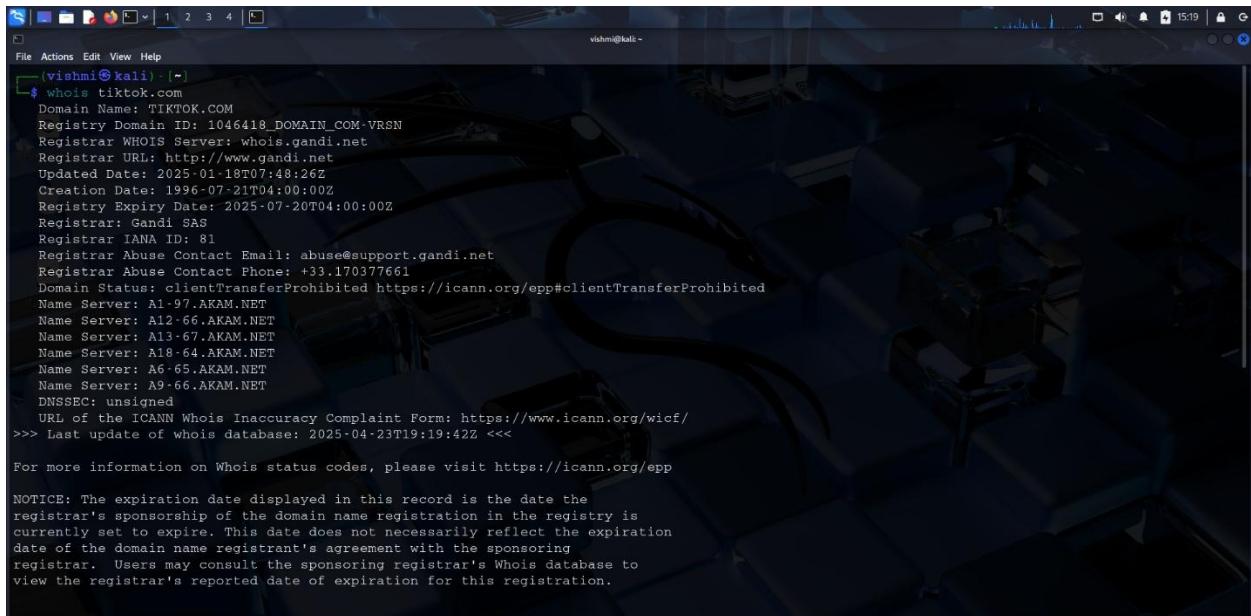
**Domain** = *tiktok.com*

**Sub-domain** = *in.tiktok.com*

**URL** = *https://www.tiktok.com*

# Target Reconnaissance

## Introduction to Tiktok and Audit Scope



```
vishni@kali:~$ whois tiktok.com
Domain Name: TIKTOK.COM
Registry Domain ID: 1046418_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2025-01-18T07:48:26Z
Creation Date: 1996-07-21T04:00:00Z
Registry Expiry Date: 2025-07-20T04:00:00Z
Registrar: Gandi SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: A1-97.AKAM.NET
Name Server: A12-66.AKAM.NET
Name Server: A13-67.AKAM.NET
Name Server: A18-64.AKAM.NET
Name Server: A6-65.AKAM.NET
Name Server: A9-66.AKAM.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-23T19:19:42Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

**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.

The screenshot displays two tables of data from the HackerOne platform, specifically for the TikTok bug bounty program. The left sidebar shows navigation links: Security page, Program guidelines, Scope (selected), Hacktivity, Thanks, Updates, and Collaborators. The top right corner shows a profile icon, a progress bar at 65%, and a download button for a Burp Suite Project Configuration File.

**Table 1 (Top):**

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
com.zhiliaomusically.livewallpaper	Android: Play Store	In scope	Critical	Eligible	Mar 2, 2023	0 (0%)
fp-sg.tiktokv.com	Domain	In scope	Critical	Eligible	Jan 15, 2024	1 (0%)
com.tiktok.tv TikTok TV app	Android: Play Store	In scope	Critical	Eligible	Mar 2, 2023	0 (0%)
effecthouse.tiktok.com	Domain	In scope	Critical	Eligible	Jan 23, 2023	6 (0%)
academy-outbound-ads.tiktok.com	Domain	In scope	Critical	Eligible	Oct 2, 2023	2 (0%)

**Table 2 (Bottom):**

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
com.zhiliaoapp.musically Play Store Download	Android: Play Store	In scope	Critical	Eligible	Jan 23, 2023	82 (6%)
com.ss.android.ugc.now Play Store Download.	Android: Play Store	In scope	Critical	Eligible	Jan 23, 2023	8 (1%)
*.tiktok.com	Other	In scope	Critical	Eligible for bounty	Jan 23, 2023	322 (24%)
www.pangleglobal.com	Domain	In scope	Critical	Eligible	Oct 2, 2023	27 (2%)
ads.tiktok.com	Domain	In scope	Critical	Eligible	Jan 23, 2023	389 (29%)
*.tiktokv.com	Other	In scope	Critical	Eligible	Jan 23, 2023	146 (11%)

## **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

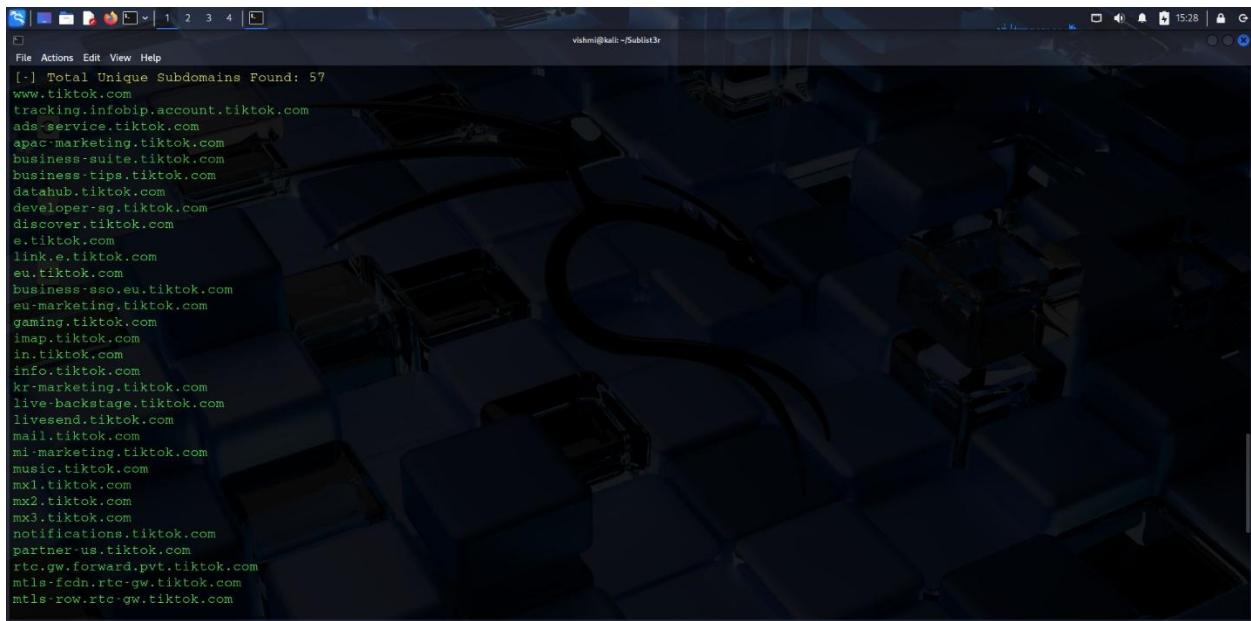
## Sublist3r

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.

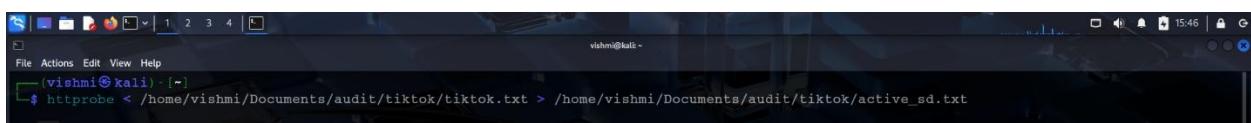


```
vishnu@kali:~/Sublist3r
File Actions Edit View Help
[+] Total Unique Subdomains Found: 57
www.tiktok.com
tracking.infobip.account.tiktok.com
ads-service.tiktok.com
apac-marketing.tiktok.com
business-suite.tiktok.com
business-tips.tiktok.com
datahub.tiktok.com
developer-sg.tiktok.com
discover.tiktok.com
e.tiktok.com
link.e.tiktok.com
eu.tiktok.com
business-sso.eu.tiktok.com
eu-marketing.tiktok.com
gaming.tiktok.com
imap.tiktok.com
in.tiktok.com
info.tiktok.com
kr-marketing.tiktok.com
live-backstage.tiktok.com
livesend.tiktok.com
mail.tiktok.com
mi-marketing.tiktok.com
music.tiktok.com
mx1.tiktok.com
mx2.tiktok.com
mx3.tiktok.com
notifications.tiktok.com
partner-us.tiktok.com
rtc-gw.forward.pvt.tiktok.com
mtls-fcdn rtc-gw.tiktok.com
mtls-row rtc-gw.tiktok.com
```

## HTTPProbe

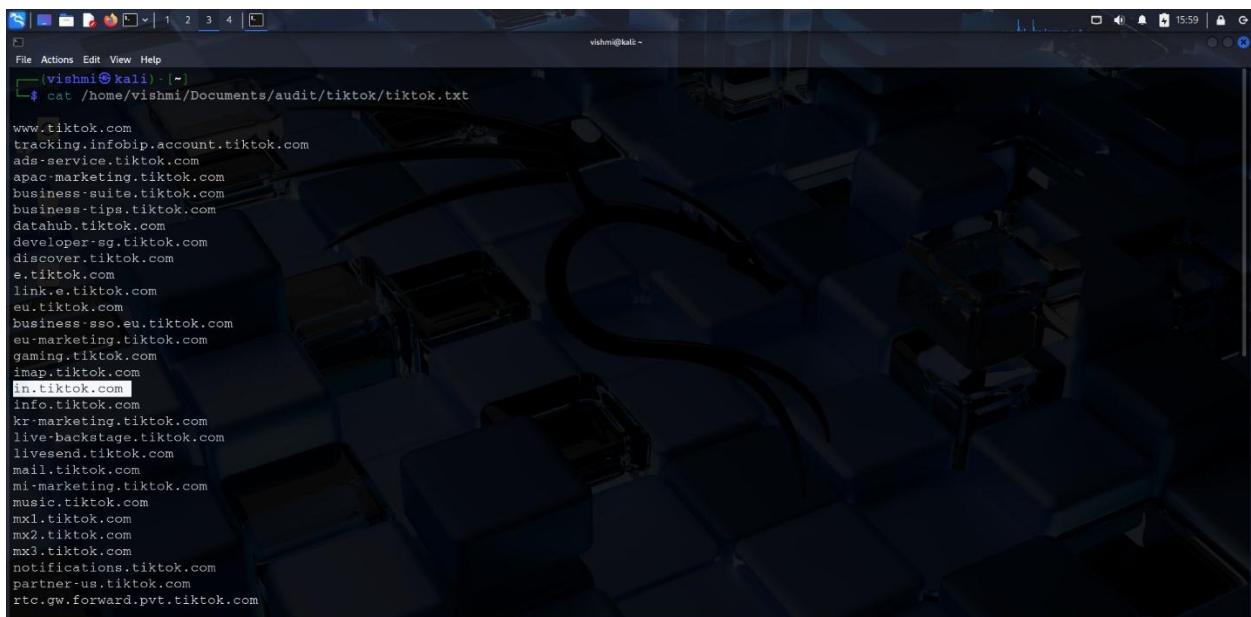
HTTPProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing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



```
vishmi@kali:~$ httpprobe < /home/vishmi/Documents/audit/tiktok/tiktok.txt > /home/vishmi/Documents/audit/tiktok/active_sd.txt
```

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

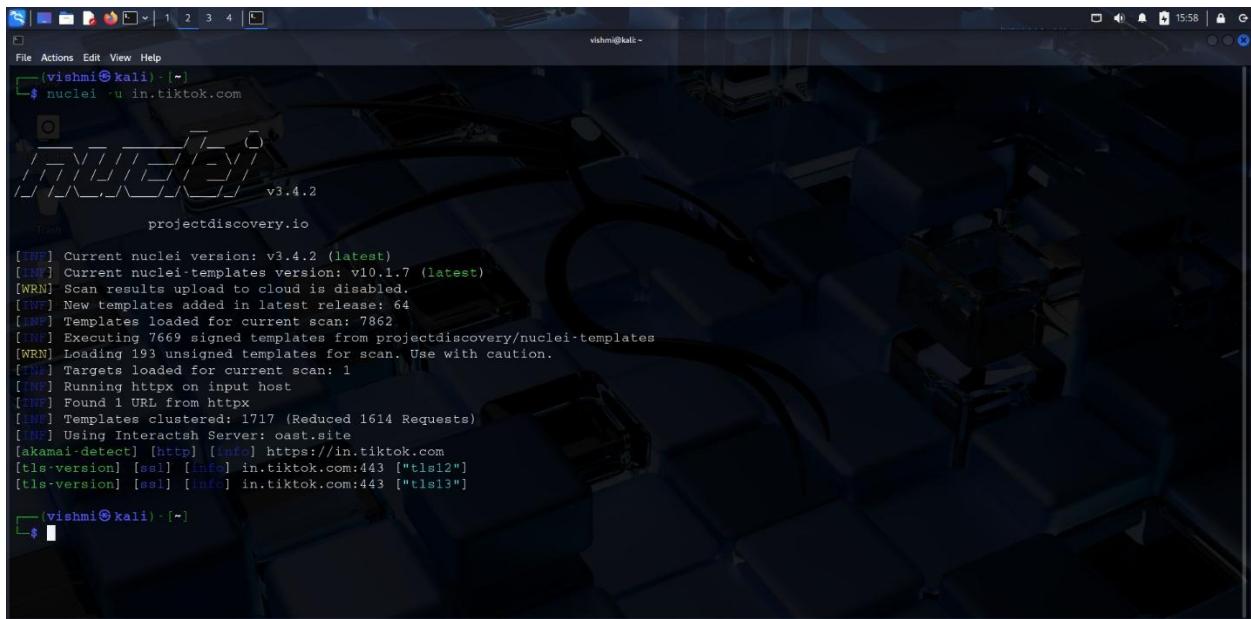


```
vishmi@kali:~$ cat /home/vishmi/Documents/audit/tiktok/tiktok.txt
www.tiktok.com
tracking.infobip.account.tiktok.com
ads-service.tiktok.com
apac-marketing.tiktok.com
business-suite.tiktok.com
business-tips.tiktok.com
datahub.tiktok.com
developer-sg.tiktok.com
discover.tiktok.com
e.tiktok.com
link-e.tiktok.com
eu.tiktok.com
business-sso.eu.tiktok.com
eu-marketing.tiktok.com
gaming.tiktok.com
imap.tiktok.com
in.tiktok.com
info.tiktok.com
kr-marketing.tiktok.com
live-backstage.tiktok.com
livesend.tiktok.com
mail.tiktok.com
mi-marketing.tiktok.com
music.tiktok.com
mx1.tiktok.com
mx2.tiktok.com
mx3.tiktok.com
notifications.tiktok.com
partner-us.tiktok.com
rtc.gw.forward.pvt.tiktok.com
```

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).



```
vishmi㉿kali: ~$ nuclei -u in.tiktok.com
v3.4.2
projectdiscovery.io

[INFO] Current nuclei version: v3.4.2 (latest)
[INFO] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 64
[INFO] Templates loaded for current scan: 7862
[INFO] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[INFO] Targets loaded for current scan: 1
[INFO] Running httpx on input host
[INFO] Found 1 URL from httpx
[INFO] Templates clustered: 1717 (Reduced 1614 Requests)
[INFO] Using Interceptsh Server: oast.site
[akamai-detect] [http] [info] https://in.tiktok.com
[tls-version] [ssl] [https] in.tiktok.com:443 ["tls12"]
[tls-version] [ssl] [info] in.tiktok.com:443 ["tls13"]

(vishmi㉿kali: ~$
```

Vulnerability Type	Description	Risk
<b>akamai-detect</b>	Just verifies that the destination website has Akamai protection.	Not a vulnerability; [Information detect]
<b>SSL/TLS Exposure</b>	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.

```
vishmi㉿kali:~$ sqlmap -u in.tiktok.com --level 5 --risk 3 --batch
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 16:02:15 /2025-04-23/
[16:02:15] [INFO] testing connection to the target URL
[16:02:15] [CRITICAL] WAF/IPS identified as 'Kona Site Defender (Akamai Technologies)'
[16:02:15] [WARNING] potential permission problems detected ('Access Denied')
[16:02:15] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
[16:02:15] [INFO] checking if the target is protected by some kind of WAF/IPS
[16:02:15] [INFO] testing if the target URL content is stable
[16:02:16] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison' how do you want to proceed? [(C)ontinue/(S)tring/(R)eject/(Q)uit] C
[16:02:16] [INFO] searching for dynamic content
[16:02:16] [INFO] dynamic content marked for removal (1 region)
[16:02:16] [INFO] testing if parameter 'User-Agent' is dynamic
got a 301 redirect to 'https://in.tiktok.com/'. Do you want to follow? [Y/n] Y
[16:02:18] [WARNING] it appears that you have been blocked by the target server
[16:02:18] [INFO] parameter 'User-Agent' appears to be dynamic
[16:02:18] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[16:02:18] [INFO] testing for SQL injection on parameter 'User-Agent'

vishmi㉿kali:~$ sqlmap -h
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 16:02:15 /2025-04-23/
[16:02:15] [INFO] testing connection to the target URL
[16:02:15] [CRITICAL] WAF/IPS identified as 'Kona Site Defender (Akamai Technologies)'
[16:02:15] [WARNING] potential permission problems detected ('Access Denied')
[16:02:15] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
[16:02:15] [INFO] checking if the target is protected by some kind of WAF/IPS
[16:02:15] [INFO] testing if the target URL content is stable
[16:02:16] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison' how do you want to proceed? [(C)ontinue/(S)tring/(R)eject/(Q)uit] C
[16:02:16] [INFO] searching for dynamic content
[16:02:16] [INFO] dynamic content marked for removal (1 region)
[16:02:16] [INFO] testing if parameter 'User-Agent' is dynamic
got a 301 redirect to 'https://in.tiktok.com/'. Do you want to follow? [Y/n] Y
[16:02:18] [WARNING] it appears that you have been blocked by the target server
[16:02:18] [INFO] parameter 'User-Agent' appears to be dynamic
[16:02:18] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[16:02:18] [INFO] testing for SQL injection on parameter 'User-Agent'

Usage: python3 sqlmap [options]

Options:
-h, --help          Show basic help message and exit
-hh                Show advanced help message and exit
--version          Show program's version number and exit
-v VERBOSE         Verbosity level: 0-6 (default 1)

Target:
At least one of these options has to be provided to define the target(s)

-u URL, --url=URL  Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-g GOOGLEDORK      Process Google dork results as target URLs

Request:
These options can be used to specify how to connect to the target URL

--data=DATA        Data string to be sent through POST (e.g. "id=1")
--cookie=COOKIE    HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
--random-agent     Use randomly selected HTTP User-Agent header value
--proxy=PROXY       Use a proxy to connect to the target URL
--tor              Use Tor anonymity network
```

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

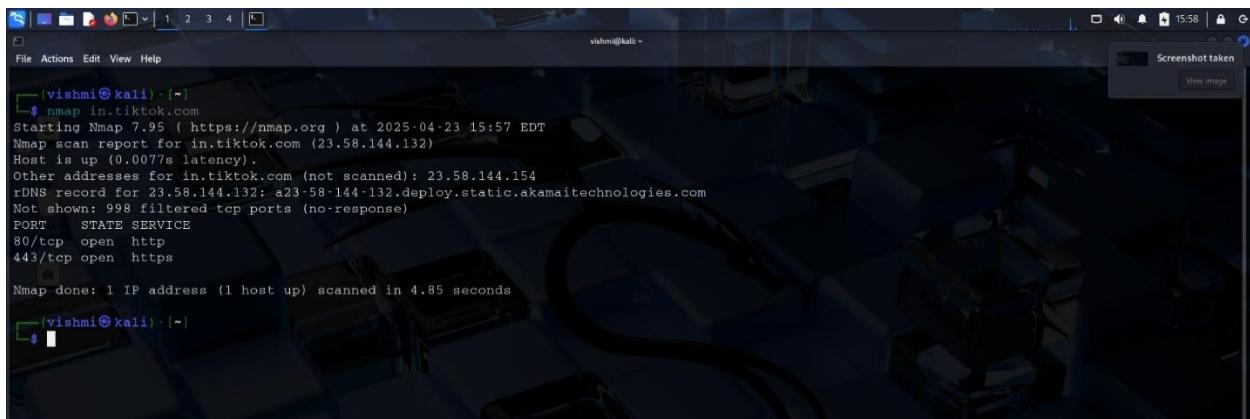
## Detected Information

- \* **[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.



A screenshot of a terminal window titled 'vishmi@kali'. The command '\$ nmap in.tiktok.com' is run, and the output shows the following details:

```
vishmi@kali: ~]$ nmap in.tiktok.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 15:57 EDT
Nmap scan report for in.tiktok.com (23.58.144.132)
Host is up (0.0077s latency).
Other addresses for in.tiktok.com (not scanned): 23.58.144.154
rDNS record for 23.58.144.132: a23-58-144-132.deploy.static.akamaitechnologies.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.85 seconds
```

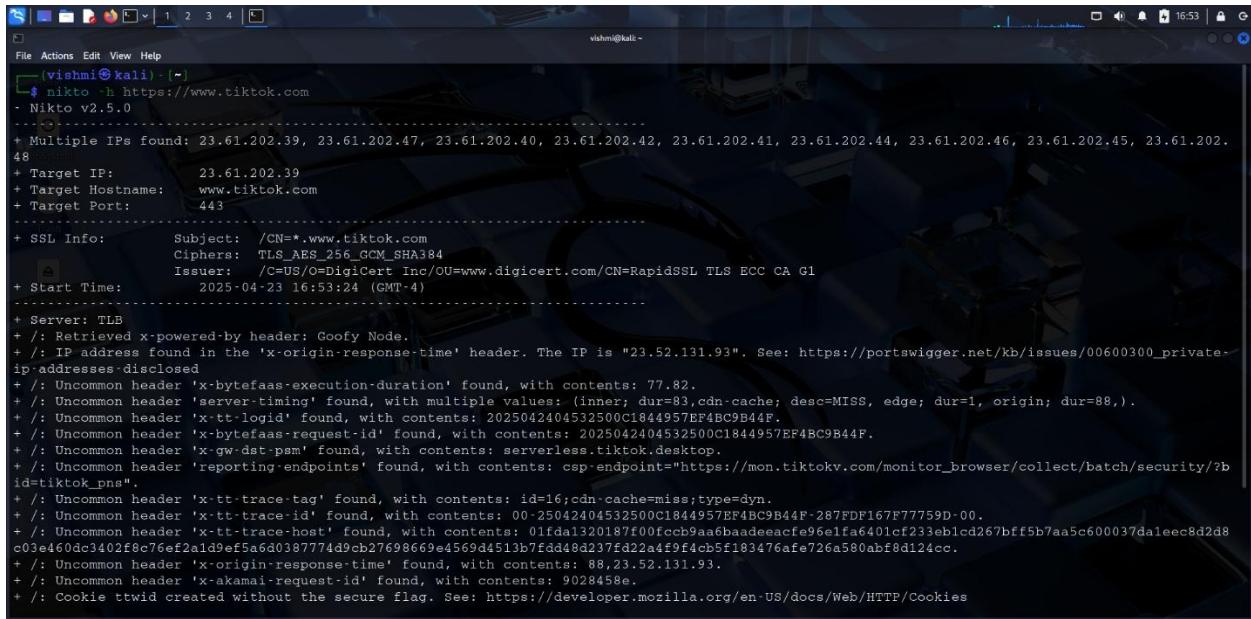
I discovered these details by using Nmap to search *in.tiktok.com*.

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.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running the Nikto web scanner against the URL <https://www.tiktok.com>. The output of the scan is displayed, detailing various security findings. Key findings include multiple IP addresses found (23.61.202.39, 23.61.202.47, 23.61.202.40, 23.61.202.42, 23.61.202.41, 23.61.202.44, 23.61.202.46, 23.61.202.45, 23.61.202.48), target IP (23.61.202.39), target hostname (www.tiktok.com), and target port (443). SSL information is also provided, including the subject (/CN=\*.www.tiktok.com), ciphers (TLS\_AES\_256\_GCM\_SHA384), and issuer (C=US/O=DigiCert Inc/OU=www.digicert.com/CN=RapidSSL TLS ECC CA G1). The start time of the scan is listed as 2025-04-23 16:53:24 (GMT-4). The server is identified as TLB. Numerous uncommon headers are listed, such as 'x-bytefaas-execution-duration' (contents: 77.82), 'x-tt-logid' (contents: 2025042404532500C1844957EF4BC9B44F), 'x-gw-dst-psm' (contents: serverless.tiktok.desktop), and 'reporting-endpoints' (contents: csp-endpoint="https://mon.tiktokv.com/monitor\_browser/collect/batch/security/?bid=tiktok\_pns"). Other findings include 'x-tt-trace-tag' (contents: id=16;cdn-cache=miss;type=dyn), 'x-tt-trace-id' (contents: 0025042404532500C1844957EF4BC9B44F-287FDF167F77759D-00), 'x-tt-trace-host' (contents: 01fdal320187f00fc9aa6baadeeacfe96e1fa6401cf233eb1cd267bfff5b7aa5c600037daleec8d2d8c03e460dc3402f8c76ef2a1d9ef5a6d0387774d9cb27698669e4569d4513b7fdd48d237fd22a4f9f4cb5f103476afe726a580abf8d124cc), 'x-origin-response-time' (contents: 88,23,52,131,93), 'x-akamai-request-id' (contents: 9028458e), and a cookie 'ttwid' created without the secure flag (contents: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies).

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 .

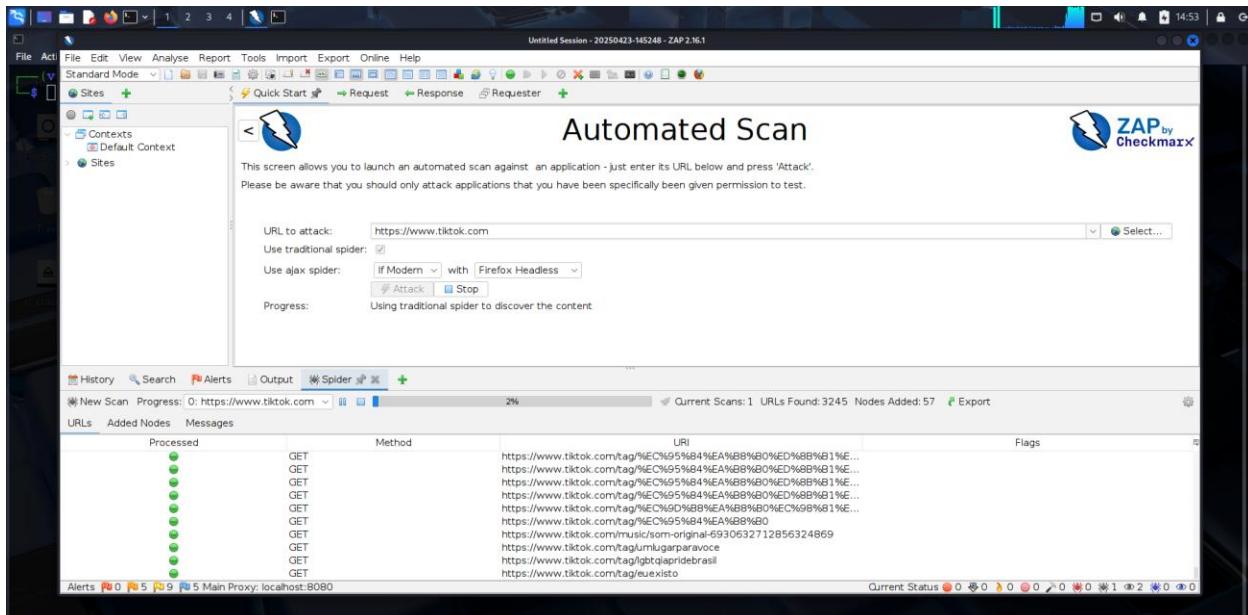
The screenshot shows two browser windows for Virustotal. The top window is the homepage with a search bar for 'URL, IP address, domain or file hash'. The bottom window shows the analysis results for the URL <https://www.tiktok.com>. The results table lists 12 security vendors, all of which found the URL to be 'Clean'.

Security vendor	Result
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Artists Against 419	Clean
BitDefender	Clean
Blueliv	Clean
Acronis	Clean
AI Labs (MONITORAPP)	Clean
Antiy-AVL	Clean
benkow.cc	Clean
BlockList	Clean
Certego	Clean

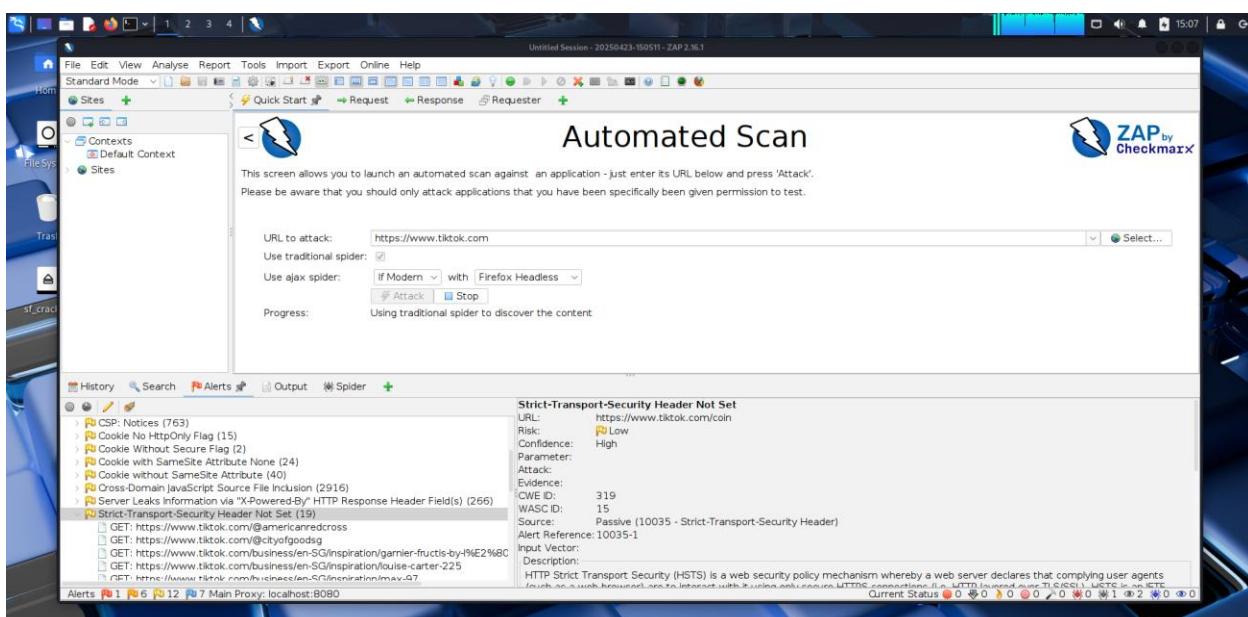
## OWASP ZAP

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](#)]

**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.)

Risk	User Confirmed	Confidence				Total
		High	Medium	Low	Total	
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.

Site	Total	0 (0.0%)	10 (38.5%)	11 (42.3%)	5 (19.2%)	26 (100%)
<a href="https://www.tiktok.com">https://www.tiktok.com</a>						

**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.)

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

ZAP by Checkmarx Scanning + file:///home/vishnu/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 compliant with Spec)	Medium	41 (157.7%)
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

<b>a.Vulnerability Title</b>	<b>Strict-Transport-Security Header Not Set</b>
<b>b.Vulnerability Description</b>	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.
<b>c.Affected Components</b>	Web server configuration, specifically the HTTP response headers.
<b>d.Impact Assessment</b>	Users may unknowingly connect to a website via HTTP, potentially exposing sensitive data to interception.
<b>e.Steps to Reproduce</b>	<ol style="list-style-type: none"><li>1. Try connecting to the target website with http:// rather than https:// by opening a browser.</li><li>2. Note that HTTPS is not immediately updated for the connection.</li><li>3. Verify that the Strict-Transport-Security header is missing by looking at the HTTP response headers.</li></ol>
<b>f.Proof of Concept (if applicable)</b>	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.
<b>g.Proposed Mitigation or Fix</b>	Add the Strict-Transport-Security header to the server to enable the HSTS policy.

## **Report-07**

# Web Audit

# *starbucks.com*

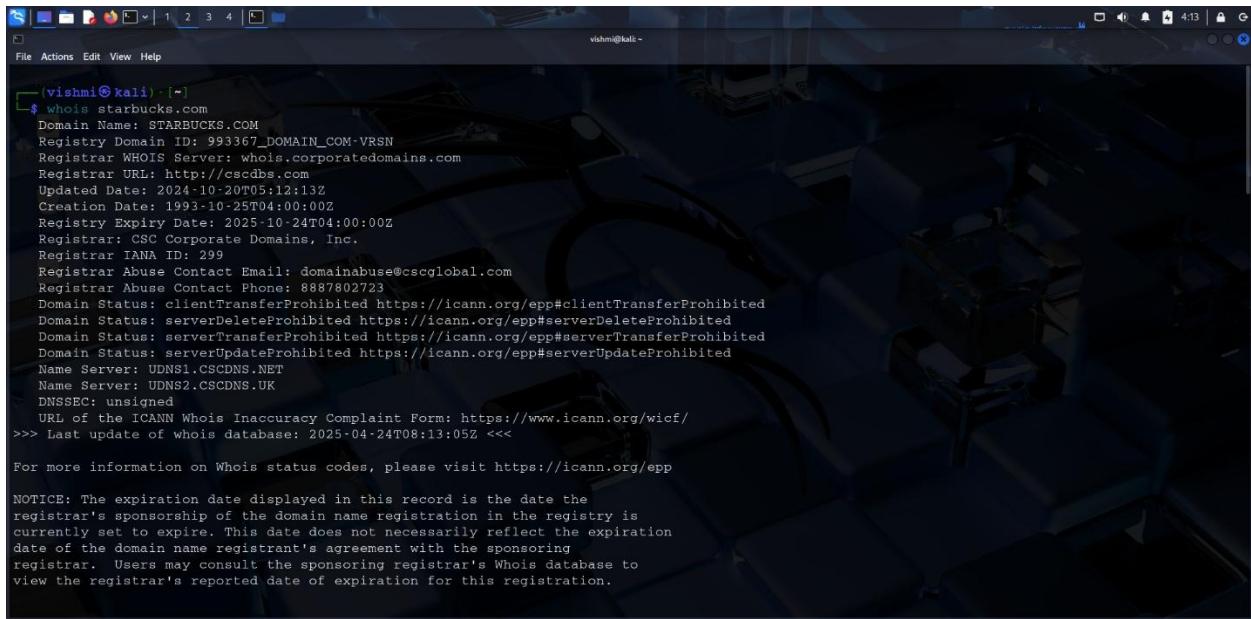
**Domain** = *starbucks.com*

**Sub-domain** = *a.starbucks.com*

**URL** = *https://www.starbucks.com*

# Target Reconnaissance

## Introduction to Starbucks and Audit Scope



```
vishni㉿kali:~$ whois starbucks.com
Domain Name: STARBUCKS.COM
Registry Domain ID: 993367_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2024-10-20T05:12:13Z
Creation Date: 1993-10-25T04:00:00Z
Registry Expiry Date: 2025-10-24T04:00:00Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: UDNS1.CSCDNS.NET
Name Server: UDNS2.CSCDNS.UK
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-24T08:13:05Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

**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

hackerone.com/starbucks/policy\_scopes

Scope

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
secureui.starbucks.com Starbucks Payment Processing <a href="https://secureui.starbucks.com/">https://secureui.starbucks.com/</a>	Domain	In scope	Critical	Eligible	Nov 17, 2022	0 (0%)
com.starbucks.mystarbucks Starbucks US iOS app. <a href="https://itunes.apple.com/us/app/starbucks/id331177714">https://itunes.apple.com/us/app/starbucks/id331177714</a>	iOS: App Store	In scope	Critical	Eligible	Nov 17, 2022	2 (0%)
openapi.starbucks.com Starbucks digital service capabilities to 3rd party business partner(s)/cooperators via standard Open API.	Domain	In scope	Critical	Eligible	Nov 17, 2022	1 (0%)
www.starbucksreserve.com Starbucks Reserve	Domain	In scope	Critical	Eligible	Nov 17, 2022	7 (0%)

1-11 of 11

hackerone.com/starbucks/policy\_scopes

Scope

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
<b>Other assets</b> If you have found a vulnerability in a Starbucks site or app not contained within this list, you can still submit, and Starbucks will triage the report. These types of reports will not result in a monetary reward but valid reports that are resolved can improve your reputation score on the HackerOne platform.	Other	In scope	Critical	Ineligible	Nov 17, 2022	733 (37%)
<b>New</b> <a href="#">apply.starbucks.com</a> This site is powered by Eightfold. Any vulnerabilities identified involving this asset should be submitted to Eightfold's Bug Bounty Program. <a href="https://hackerone.com/eightfold?type=team">https://hackerone.com/eightfold?type=team</a>	Domain	Out of scope	None	Ineligible	Apr 18, 2025	0 (0%)

1-11 of 11

## **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

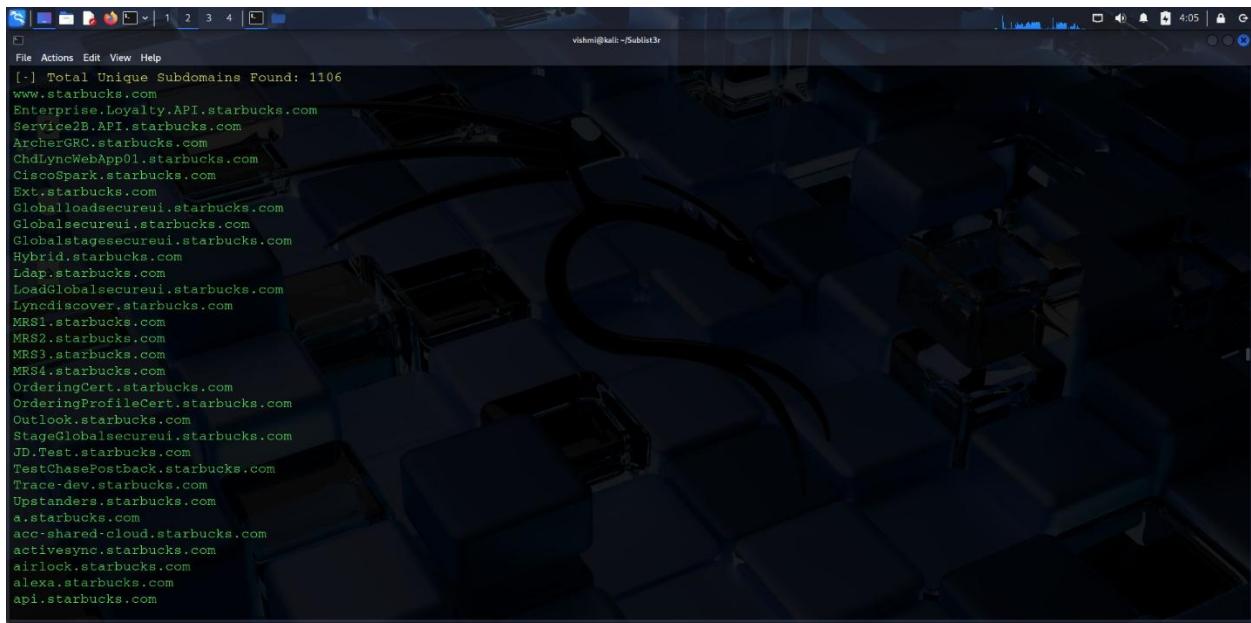
## Sublist3r

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.



```
vishnu@kali:~/Sublist3r
File Actions Edit View Help
[+] Total Unique Subdomains Found: 1106
www.starbucks.com
Enterprise.Loyalty.API.starbucks.com
Service2B.API.starbucks.com
ArcherGRC.starbucks.com
ChdLyncWebApp01.starbucks.com
CiscoSpark.starbucks.com
Ext.starbucks.com
Globalloadsecureui.starbucks.com
Globalsecureui.starbucks.com
Globalstagesecureui.starbucks.com
Hybrid.starbucks.com
Ldap.starbucks.com
Loadglobalsecureui.starbucks.com
Lyncdiscover.starbucks.com
MRS1.starbucks.com
MRS2.starbucks.com
MRS3.starbucks.com
MRS4.starbucks.com
OrderingCert.starbucks.com
OrderingProfileCert.starbucks.com
Outlook.starbucks.com
StageGlobalsecureui.starbucks.com
JD.Test.starbucks.com
TestChasePostBack.starbucks.com
Trace-dev.starbucks.com
Upstanders.starbucks.com
&.starbucks.com
acc-shared-cloud.starbucks.com
activesync.starbucks.com
airlock.starbucks.com
alexa.starbucks.com
api.starbucks.com
```

## HTTPProbe

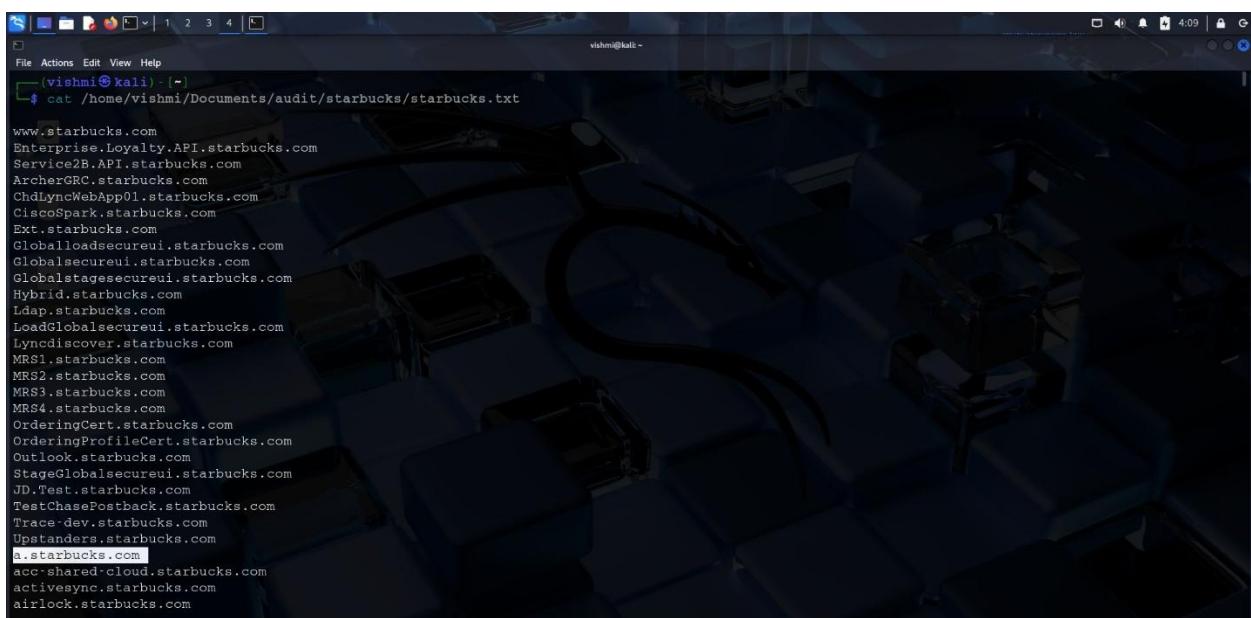
HTTPProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing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



```
vishmi@kali:~$ httpprobe </home/vishmi/Documents/audit/starbucks/starbucks.txt > /home/vishmi/Documents/audit/starbucks/active_sd.txt
```

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

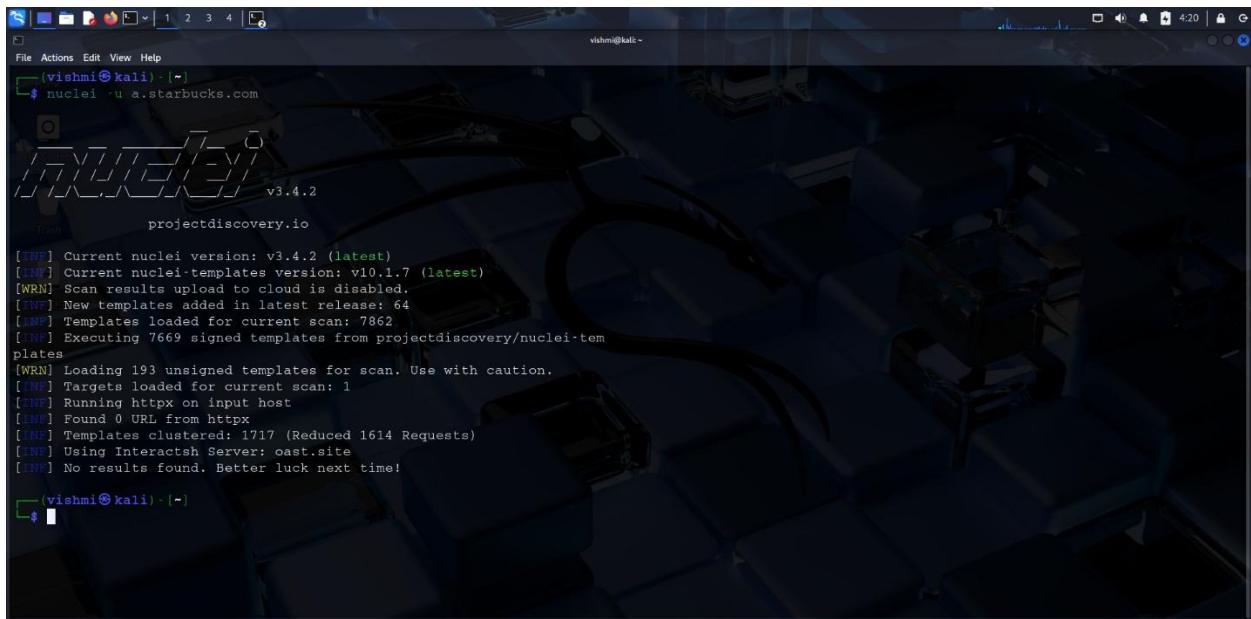


```
vishmi@kali:~$ cat /home/vishmi/Documents/audit/starbucks/starbucks.txt
www.starbucks.com
Enterprise.Loyalty.API.starbucks.com
Service2B.API.starbucks.com
ArcherGRC.starbucks.com
ChdiSyncWebApp01.starbucks.com
CiscoSpark.starbucks.com
Ext.starbucks.com
Globalloadsecureui.starbucks.com
Globalsecureui.starbucks.com
Globalstagesecureui.starbucks.com
Hybrid.starbucks.com
Ldap.starbucks.com
LoadGlobalsecureui.starbucks.com
Lyncdiscover.starbucks.com
MRS1.starbucks.com
MRS2.starbucks.com
MRS3.starbucks.com
MRS4.starbucks.com
OrderingCert.starbucks.com
OrderingProfileCert.starbucks.com
Outlook.starbucks.com
StageGlobalsecureui.starbucks.com
JD.Test.starbucks.com
TestChasePostback.starbucks.com
Trace-dev.starbucks.com
Upstanders.starbucks.com
a.starbucks.com
acc-shared-cloud.starbucks.com
activesync.starbucks.com
airlock.starbucks.com
```

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).



```
vishni㉿kali: ~]$ nuclei -u a.starbucks.com
v3.4.2
projectdiscovery.io

[INFO] Current nuclei version: v3.4.2 (latest)
[INFO] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 64
[INFO] Templates loaded for current scan: 7862
[INFO] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[INFO] Targets loaded for current scan: 1
[INFO] Running httpx on input host
[INFO] Found 0 URL from httpx
[INFO] Templates clustered: 1717 (Reduced 1614 Requests)
[INFO] Using Interactsh Server: east.site
[INFO] No results found. Better luck next time!
[vishni㉿kali: ~]$
```

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.

The screenshot shows two terminal windows side-by-side. Both windows have a dark blue background with a geometric pattern and are running on a Kali Linux system, as indicated by the terminal prompt 'vishni@kali: ~'.

**Top Terminal Window:**

```
vishni@kali: ~
$ sqlmap -h
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 04:21:16 /2025-04-24/
[04:21:16] [INFO] testing connection to the target URL
[04:22:16] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[04:22:16] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--proxy', '--proxy-file...')
[04:25:16] [CRITICAL] connection timed out to the target URL
[*] ending @ 04:25:16 /2025-04-24/

```

**Bottom Terminal Window:**

```
vishni@kali: ~
$ sqlmap -u a.starbucks.com --level 5 --risk 3 --batch
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 04:21:16 /2025-04-24/
[04:21:16] [INFO] testing connection to the target URL
[04:22:16] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[04:22:16] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--proxy', '--proxy-file...')
[04:25:16] [CRITICAL] connection timed out to the target URL
[*] ending @ 04:25:16 /2025-04-24/

```

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

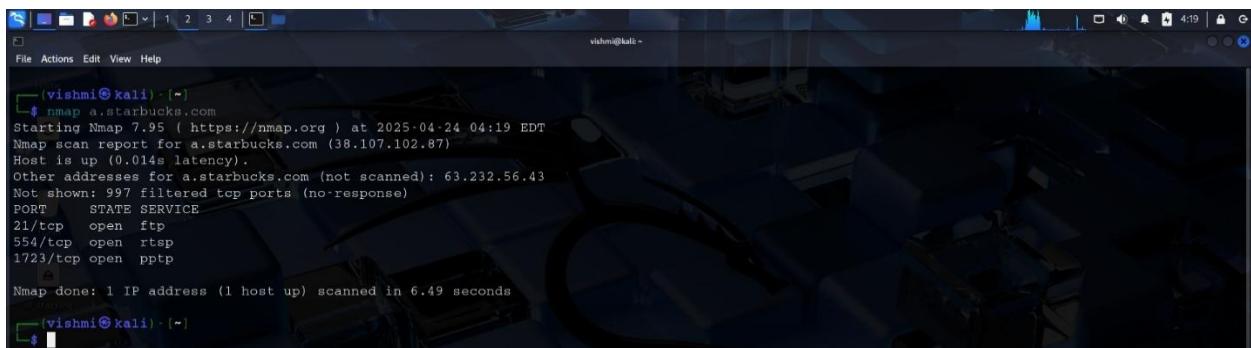
### **Detected Information**

\* **[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.



The screenshot shows a terminal window on a Kali Linux desktop environment. The user has run the command `nmap a.starbucks.com`. The output indicates that the host is up with 0.014s latency. It shows three open TCP ports: 21/tcp (ftp), 554/tcp (rtsp), and 1723/tcp (pptp). The scan took 6.49 seconds.

```
vishmi㉿kali: ~
$ nmap a.starbucks.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 04:19 EDT
Nmap scan report for a.starbucks.com (38.107.102.87)
Host is up (0.014s latency).
Other addresses for a.starbucks.com (not scanned): 63.232.56.43
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
554/tcp   open  rtsp
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 6.49 seconds
vishmi㉿kali: ~
```

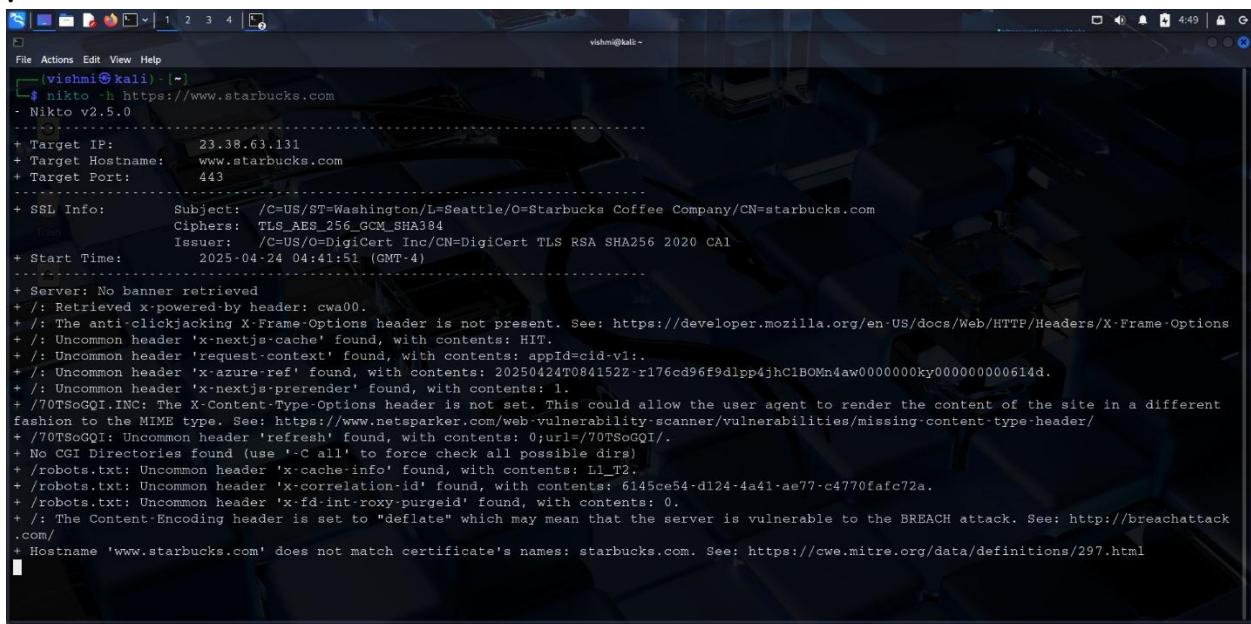
I discovered these details by using Nmap to search *a.starbucks.com*.

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



```
vishni@kali:~$ nikto -h https://www.starbucks.com
- Nikto v2.5.0

+ Target IP:      23.38.63.131
+ Target Hostname: www.starbucks.com
+ Target Port:    443

+ SSL Info:       Subject: /C=US/ST=Washington/L=Seattle/O=Starbucks Coffee Company/CN=starbucks.com
                  Ciphers: TLS_AES_256_GCM_SHA384
                  Issuer: /C=US/O=DigiCert Inc/CN=DigiCert TLS RSA SHA256 2020 CA1
+ Start Time:    2025-04-24 04:41:51 (GMT+4)

+ Server: No banner retrieved
+ /: Retrieved x-powered-by header: cwa00.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-nextjs-cache' found, with contents: HIT.
+ /: Uncommon header 'request-context' found, with contents: appId=cid-v1..
+ /: Uncommon header 'x-azure-ref' found, with contents: 20250424T084152Z-r176cd96f9dlpp4jhC1BOMn4aw0000000ky000000000614d.
+ /: Uncommon header 'x-nextjs-prerender' found, with contents: 1.
+ /70TSqGQI:INC: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different
fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /70TSqGQI: Uncommon header 'refresh' found, with contents: 0;url=/70TSqGQI/.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Uncommon header 'x-cache-info' found, with contents: Li_T2.
+ /robots.txt: Uncommon header 'x-correlation-id' found, with contents: 6145ce54-d124-4a41-ae77-c4770fafc72a.
+ /robots.txt: Uncommon header 'x-fd-int-roxy-purgeid' found, with contents: 0.
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack
.com/
+ Hostname 'www.starbucks.com' does not match certificate's names: starbucks.com. See: https://cwe.mitre.org/data/definitions/297.html
```

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 .

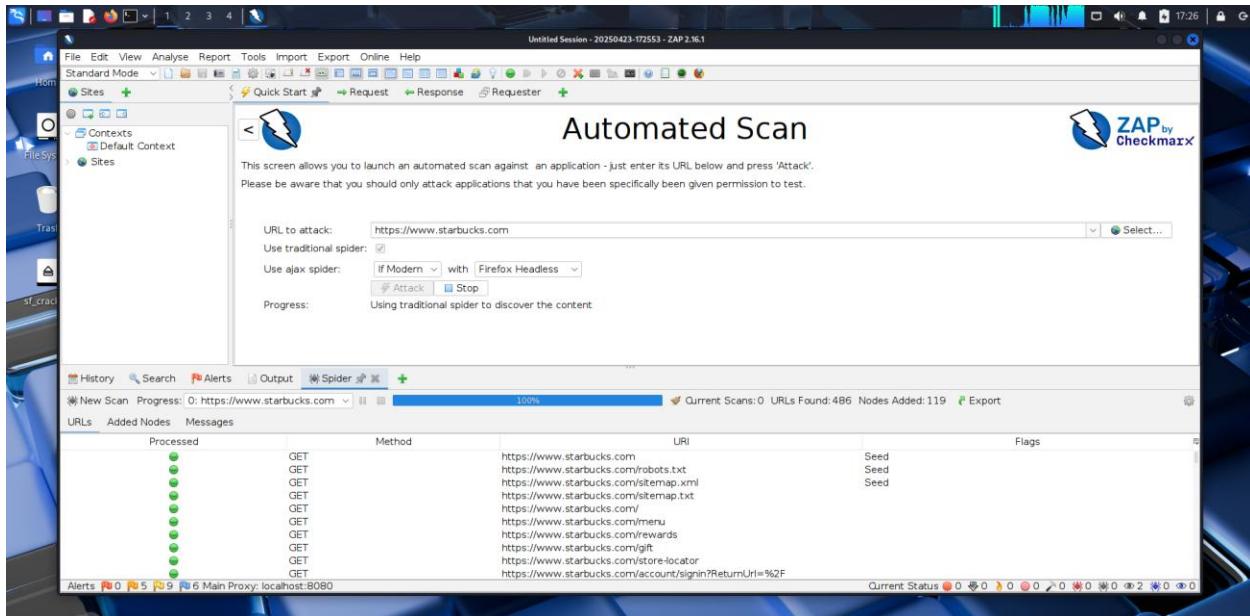
The screenshot shows two stacked browser windows for VirusTotal. The top window displays the homepage with a search bar containing 'https://www.starbucks.com'. The bottom window shows the detailed analysis results for the same URL. The results indicate that 0 security vendors flagged the URL as malicious. The analysis table lists several engines, all showing 'Clean' status. A green banner at the bottom encourages joining the community. The URL in the address bar of the bottom window is: <https://www.starbucks.com/>.

Security vendor	Result
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Artists Against 419	Clean
BitDefender	Clean
Acronis	Clean
AI Labs (MONITORAPP)	Clean
Anti-AVL	Clean
benkow.cc	Clean
BlockList	Clean

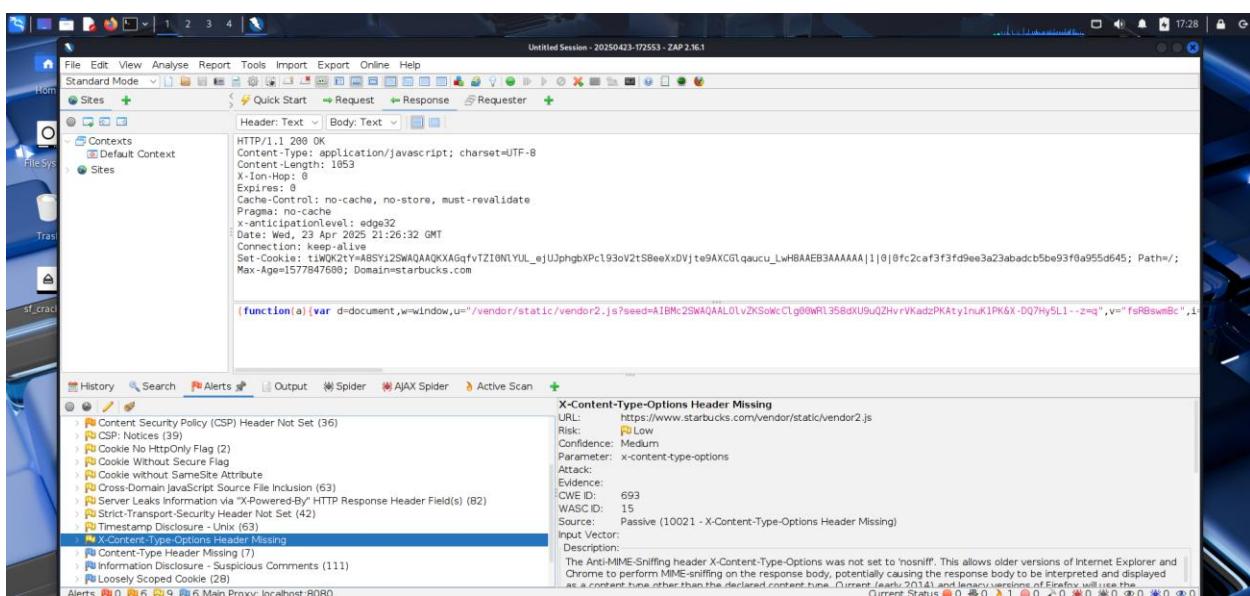
## OWASP ZAP

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](#) ]

The screenshot shows a web browser window with a dark blue theme. The address bar displays the URL: file:///home/vishmi/2025-04-23-ZAP-Report-.html. The title bar says "ZAP by Checkmarx Scanning X". The main content area has a white background with blue header sections.

**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.)

Risk	User Confirmed	Confidence				Total
		High	Medium	Low	Total	
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.)

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

ZAP by Checkmark Scanning + file:///home/vishnu/2025-04-23-ZAP-Report-.html

Kali Linux Kali Tools Kali Docs Kali Forums 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
<a href="#">CSP: Failure to Define Directive with No Fallback</a>	Medium	61 (290.5%)
<a href="#">CSP: Wildcard Directive</a>	Medium	39 (185.7%)
<a href="#">CSP: script-src unsafe-eval</a>	Medium	61 (290.5%)
<a href="#">CSP: script-src unsafe-inline</a>	Medium	61 (290.5%)
<a href="#">CSP: style-src unsafe-inline</a>	Medium	61 (290.5%)
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	36 (171.4%)
<a href="#">CSP: Notices</a>	Low	39 (185.7%)
<a href="#">Cookie No HttpOnly Flag</a>	Low	2 (1.0%)
<a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a>	Low	82 (390.5%)
<a href="#">Strict-Transport-Security Header Not Set</a>	Low	42 (200.0%)
<a href="#">Timestamp Disclosure - Unix</a>	Low	63 (300.0%)
<a href="#">X-Content-Type-Options Header Missing</a>	Low	1 (4.8%)
<a href="#">Content-Type Header Missing</a>	Informational	7 (33.3%)
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	111 (528.6%)
<a href="#">Loosely Scoped Cookie</a>	Informational	28 (133.3%)
<a href="#">Modern Web Application</a>	Informational	61 (290.5%)
<a href="#">Re-examine Cache-control Directives</a>	Informational	65 (309.5%)
<a href="#">Session Management Response Identified</a>	Informational	2 (9.5%)
Total		21

## Vulnerabilities

<b>a.Vulnerability Title</b>	<b>X-Content-Type Header Missing</b>
<b>b.Vulnerability Description</b>	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.
<b>c.Affected Components</b>	HTTP response headers, Web server configuration
<b>d.Impact Assessment</b>	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.
<b>e.Steps to Reproduce</b>	<ol style="list-style-type: none"><li>Send an HTTP request to the web server.</li><li>Use tools such as network scanners or browser developer tools to examine the HTTP response headers.</li><li>Make sure the response does not contain the X-Content-Type header.</li></ol>
<b>f.Proof of Concept (if applicable)</b>	The vulnerability is not directly exploitable, but a simple examination reveals the absence of the header in HTTP responses, verifying the vulnerability.
<b>g.Proposed Mitigation or Fix</b>	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***

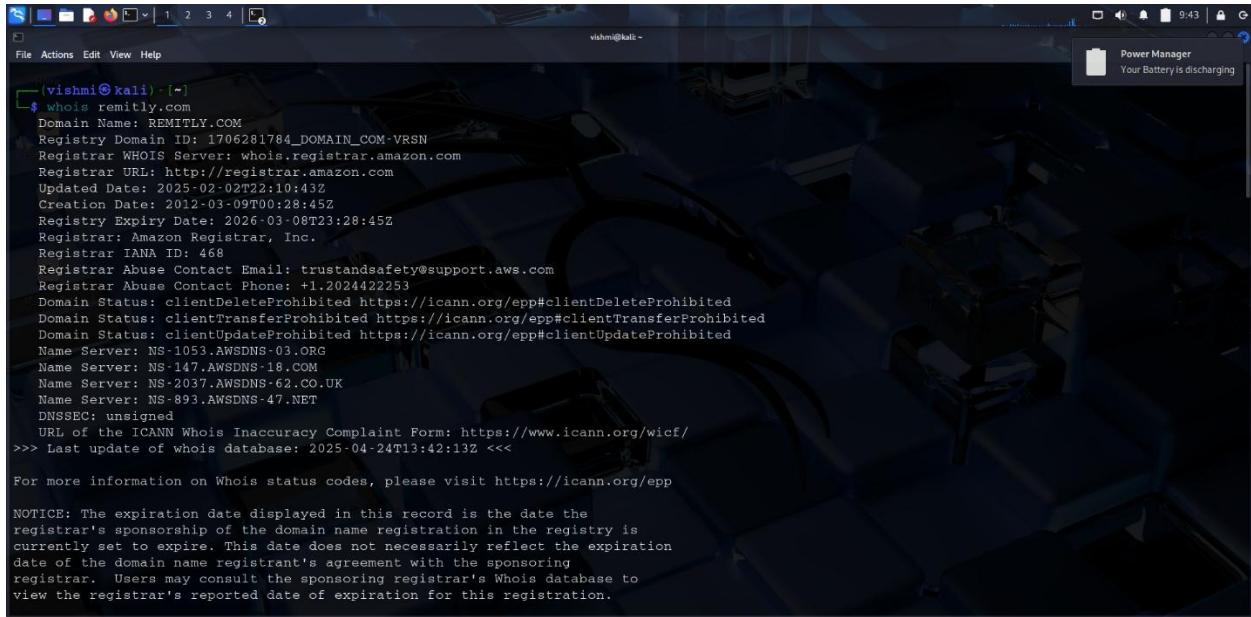
**Domain** = *remitly.com*

**Sub-domain** = *www.remitly.com*

**URL** = *https://www.remitly.com*

# Target Reconnaissance

Introduction to Remitly and Audit Scope.



```
vishni@kali:~$ whois remitly.com
Domain Name: REMITLY.COM
Registry Domain ID: 1706281784_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon.com
Registrar URL: http://registrar.amazon.com
Updated Date: 2025-02-02T22:10:43Z
Creation Date: 2012-03-09T00:28:45Z
Registry Expiry Date: 2026-03-08T23:28:45Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: trustandsafety@support.aws.com
Registrar Abuse Contact Phone: +1.2024422253
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS-1053.AWSDNS-03.ORG
Name Server: NS-147.AWSDNS-18.COM
Name Server: NS-2037.AWSDNS-62.CO.UK
Name Server: NS-893.AWSDNS-47.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-24T13:42:13Z <<
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

**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.

This screenshot shows the 'Scope' section of the HackerOne platform. The left sidebar includes links for Security page, Program guidelines, Scope (which is selected), Hacktivity, Thanks, Updates, Collaborators, and Safe harbor. The main content area displays a table of assets. The columns are: Asset name, Type, Coverage, Max. severity, Bounty, Last update, and Resolved Reports. The table lists several domains, all marked as 'In scope' with a maximum severity of 'Critical' and marked as 'Eligible'. The last row shows 'rewire.com' as a Domain with 'In scope' status, 'Critical' severity, and 'Eligible' status.

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
cardpayments.remitly.io	Domain	In scope	Critical	Eligible	May 24, 2024	0 (0%)
com.remitly.androidapp	Android: Play Store	In scope	Critical	Eligible	Oct 3, 2018	5 (4%)
cards.remitly.io	Domain	In scope	Critical	Eligible	Oct 19, 2018	0 (0%)
api.remitly.io	Domain	In scope	Critical	Eligible	Oct 19, 2018	10 (7%)
access.remitly.com	Domain	In scope	Critical	Eligible	Sep 5, 2024	0 (0%)
rewire.com	Domain	In scope	Critical	Eligible	Aug 28, 2023	12 (9%)

This screenshot shows the 'Scope' section of the HackerOne platform. The left sidebar includes links for Security page, Program guidelines, Scope (selected), Hacktivity, Thanks, Updates, Collaborators, and Safe harbor. The main content area displays a table of assets. The columns are: Asset name, Type, Coverage, Max. severity, Bounty, Last update, and Resolved Reports. The table lists several domains, all marked as 'In scope' with a maximum severity of 'Medium' and marked as 'Eligible'. The last row shows 'https://www.remitly.com/blog' as an 'Other' asset with 'Out of scope' status, 'None' severity, and 'Ineligible' status.

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
app3.rewire.to	Domain	In scope	Medium	Eligible	Mar 18, 2024	1 (1%)
rates.rewire.com	Domain	In scope	Medium	Eligible	Mar 15, 2024	3 (2%)
metrics.int.remitly.com	Domain	In scope	Medium	Eligible	Jul 16, 2024	0 (0%)
site.rewire.com	Domain	In scope	Medium	Eligible	Oct 21, 2024	1 (1%)
careers.remitly.com	Domain	In scope	Medium	Eligible	Mar 20, 2025	1 (1%)
https://www.remitly.com/blog	Other	Out of scope	None	Ineligible	Aug 1, 2019	0 (0%)

## **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

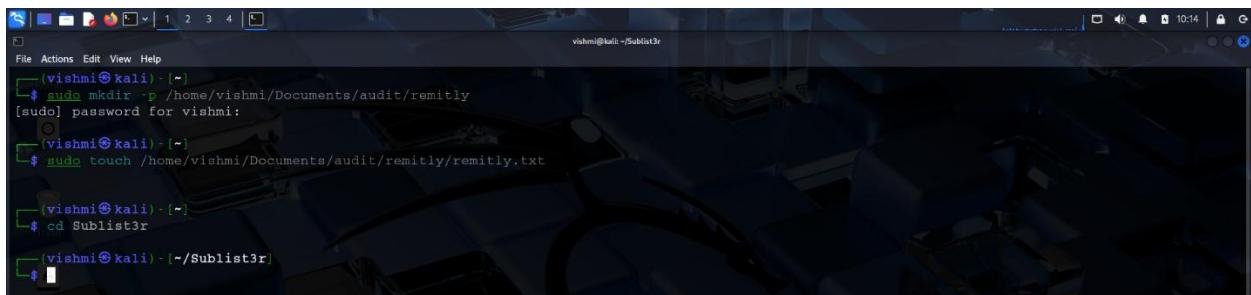
# Finding active subdomains and their states

## Sublist3r

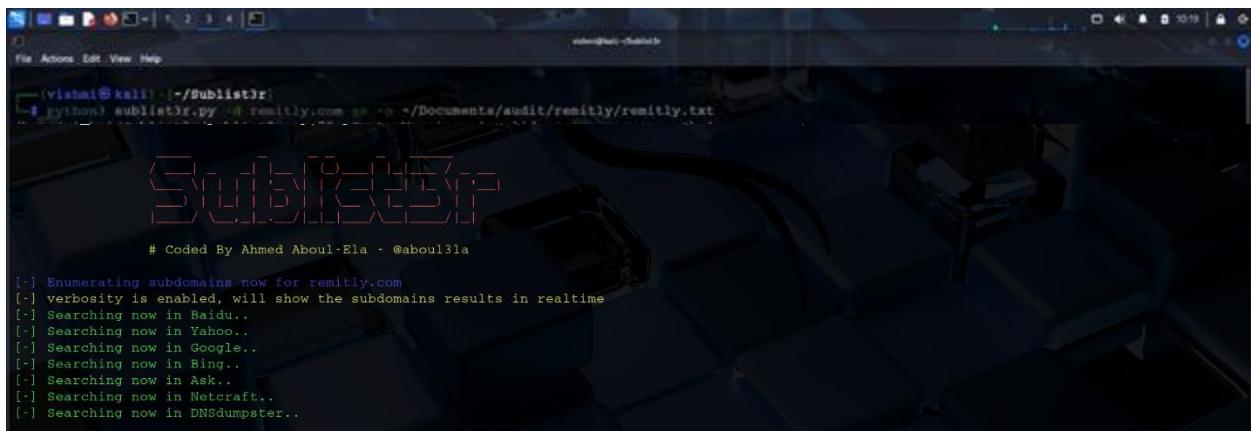
Sublist3r is an open-source Python application that uses OSINT (Open Source Intelligence) techniques to quickly and effectively scan subdomains. Subdomains linked to a target domain can be found by penetration testers, security researchers, and bug bounty hunters using a variety of search engine queries (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***



```
vishmi@kali: ~$ sudo mkdir -p /home/vishmi/Documents/audit/remitly  
[sudo] password for vishmi:  
vishmi@kali: ~$ sudo touch /home/vishmi/Documents/audit/remitly/remitly.txt  
vishmi@kali: ~$ cd Sublist3r  
vishmi@kali: ~/Sublist3r$
```



```
vishmi@kali: ~/Sublist3r$ python sublist3r.py -t remitly.com > ~/Documents/audit/remitly/remitly.txt  
# Coded By Ahmed Aboul-Ela - @aboul3la  
[+] Enumerating subdomains now for remitly.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..
```

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



```
vishnu@kali: ~
```

```
[+] Saving results to file: /home/vishnu/Documents/audit/remitly/remitly.txt
[-] Total Unique Subdomains Found: 76
www.remitly.com
access.remitly.com
api.access.remitly.com
access.sandbox.remitly.com
api.access.sandbox.remitly.com
ablink.accounts.remitly.com
barclays.remitly.com
blog.remitly.com
branch.remitly.com
brand.remitly.com
careers.remitly.com
cdn.remitly.com
webflow.circle.remitly.com
client.tls.remitly.com
autoTIX.clienttls.remitly.com
singpass.clienttls.remitly.com
www.singpass.clienttls.remitly.com
singpass.preprod.clienttls.remitly.com
www.singpass.preprod.clienttls.remitly.com
cn.survey.remitly.com
email.comms.remitly.com
credit.remitly.com
client.tls.dev.remitly.com
docs.dev.remitly.com
guidebook.dev.remitly.com
help-preprod.dev.remitly.com
icici-sign.dev.remitly.com
jpm.dev.remitly.com
www.jpm.dev.remitly.com
jpm-signing.dev.remitly.com
login.dev.remitly.com
```

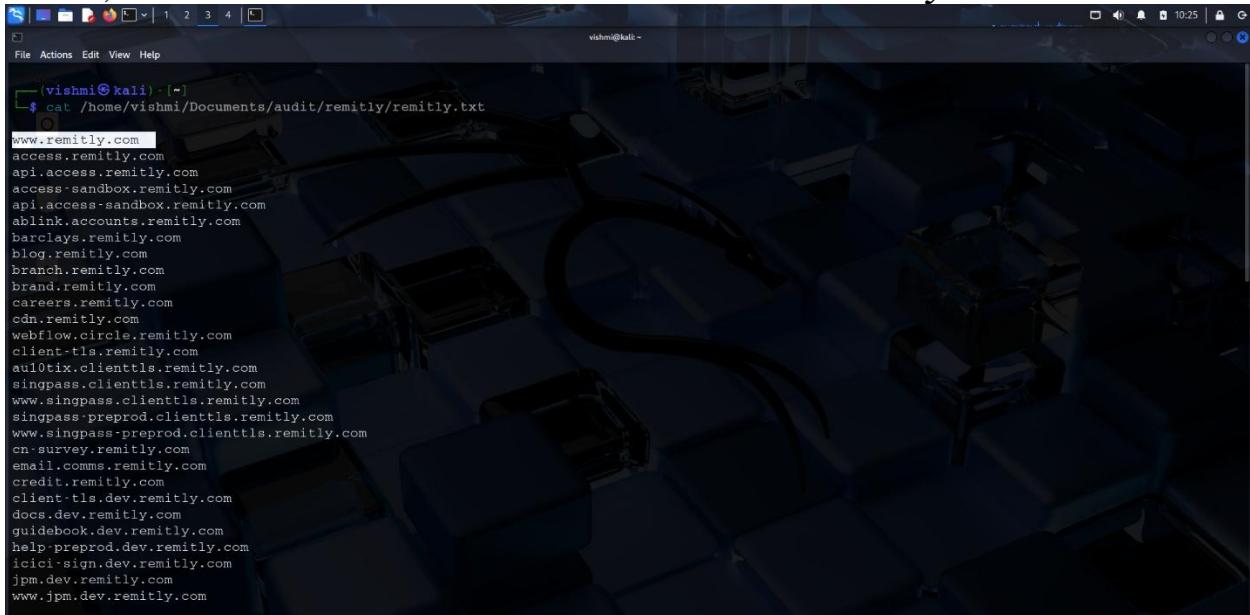
## HTTPProbe

HTTPProbe 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.



```
vishmi@kali:~$ httpprobe < /home/vishmi/Documents/audit/remitly/remitly.txt > /home/vishmi/Documents/audit/remitly/active_sd.txt
```

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



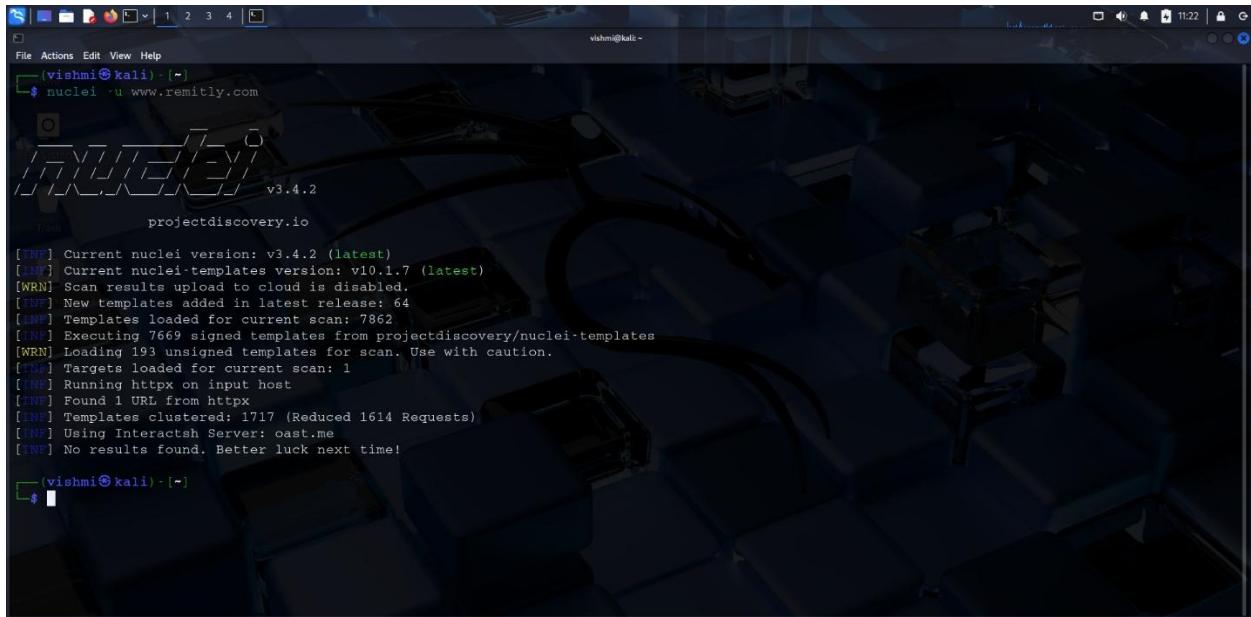
```
vishmi@kali:~$ cat /home/vishmi/Documents/audit/remitly/remitly.txt
```

```
www.remitly.com
access.remitly.com
api.access.remitly.com
access.sandbox.remitly.com
api.access.sandbox.remitly.com
ablink.accounts.remitly.com
barclays.remitly.com
blog.remitly.com
branch.remitly.com
brand.remitly.com
careers.remitly.com
cdn.remitly.com
webflow.circle.remitly.com
client-tls.remitly.com
autoTlxit.clienttls.remitly.com
singpass.clienttls.remitly.com
www.singpass.clienttls.remitly.com
singpass_preprod.clienttls.remitly.com
www.singpass_preprod.clienttls.remitly.com
cn-survey.remitly.com
email.comms.remitly.com
credit.remitly.com
client-tls.dev.remitly.com
docs.dev.remitly.com
guidebook.dev.remitly.com
help-preprod.dev.remitly.com
icici-sign.dev.remitly.com
jpm.dev.remitly.com
www.jpm.dev.remitly.com
```

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).



```
vishmi㉿kali: [~]
$ nuclei -u www.remitly.com
v3.4.2
projectdiscovery.io

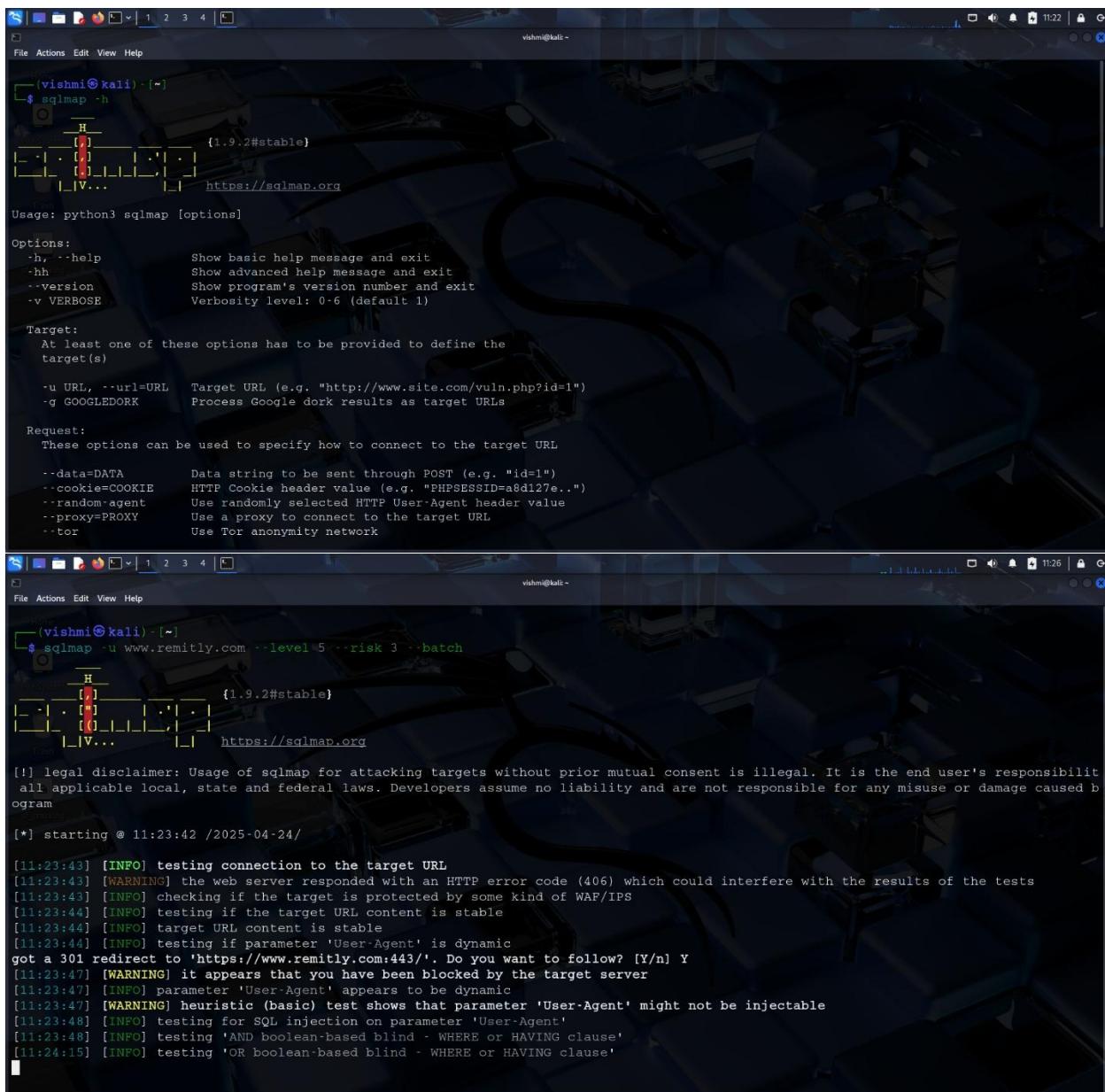
[INFO] Current nuclei version: v3.4.2 (latest)
[INFO] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 64
[INFO] Templates loaded for current scan: 7862
[INFO] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[INFO] Targets loaded for current scan: 1
[INFO] Running httpx on input host
[INFO] Found 1 URL from httpx
[INFO] Templates clustered: 1717 (Reduced 1614 Requests)
[INFO] Using Interactsh Server: oast.me
[INFO] No results found. Better luck next time!

[vishmi㉿kali: [~]]
```

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.



The screenshot shows two terminal windows side-by-side, both running on a Kali Linux desktop environment. The top window displays the SQLmap help screen, providing usage instructions and a detailed list of command-line options. The bottom window shows the execution of a SQLmap command against the URL `www.remitly.com`, specifying a risk level of 5 and a batch mode. The output includes a legal disclaimer, connection testing logs, and various informational and warning messages related to the target's behavior and potential injectability.

```
vishmi㉿kali:~$ sqlmap -h
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to respect all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:23:42 /2025-04-24/
[11:23:43] [INFO] testing connection to the target URL
[11:23:43] [WARNING] the web server responded with an HTTP error code (406) which could interfere with the results of the tests
[11:23:43] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:23:44] [INFO] testing if the target URL content is stable
[11:23:44] [INFO] target URL content is stable
[11:23:44] [INFO] testing if parameter 'User-Agent' is dynamic
got a 301 redirect to 'https://www.remitly.com:443/'. Do you want to follow? [Y/n] Y
[11:23:47] [WARNING] it appears that you have been blocked by the target server
[11:23:47] [INFO] parameter 'User-Agent' appears to be dynamic
[11:23:47] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[11:23:48] [INFO] testing for SQL injection on parameter 'User-Agent'
[11:23:48] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:24:15] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
```

<b>Option</b>	<b>Meaning</b>
<b>-u</b>	For basic testing, the target URL is required.
<b>--level5</b>	Increases the number of payloads and tests that are done (maximum is 5).
<b>--risk3</b>	Increase the danger level of the payloads used (maximum is 3)
<b>--batch</b>	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.]

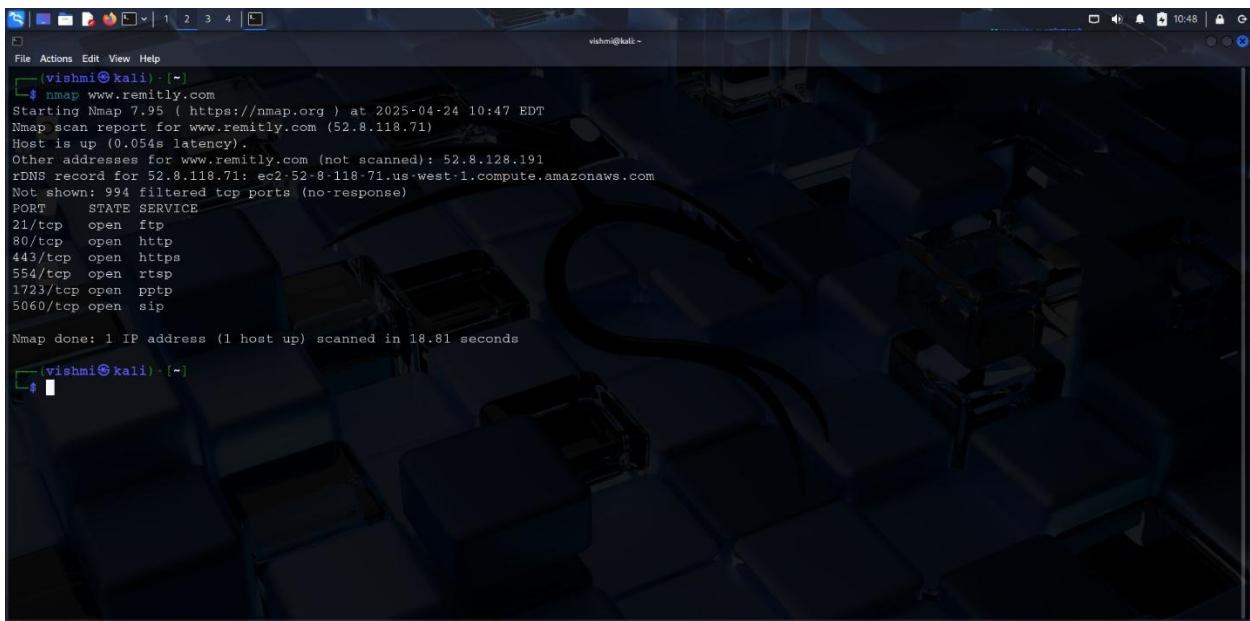
\* *[INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'*

[ 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.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running the command `nmap www.remitly.com`. The output of the scan is displayed, showing the host is up with 0.05ms latency. It lists various open ports and their corresponding services:

```
vishmi㉿kali: ~]$ nmap www.remitly.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 10:47 EDT
Nmap scan report for www.remitly.com (52.8.118.71)
Host is up (0.05ms latency).
Other addresses for www.remitly.com (not scanned): 52.8.128.191
rDNS record for 52.8.118.71: ec2-52-8-118-71.us-west-1.compute.amazonaws.com
Not shown: 994 filtered tcp ports (no-response)
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

Nmap done: 1 IP address (1 host up) scanned in 18.81 seconds
vishmi㉿kali: ~]$
```

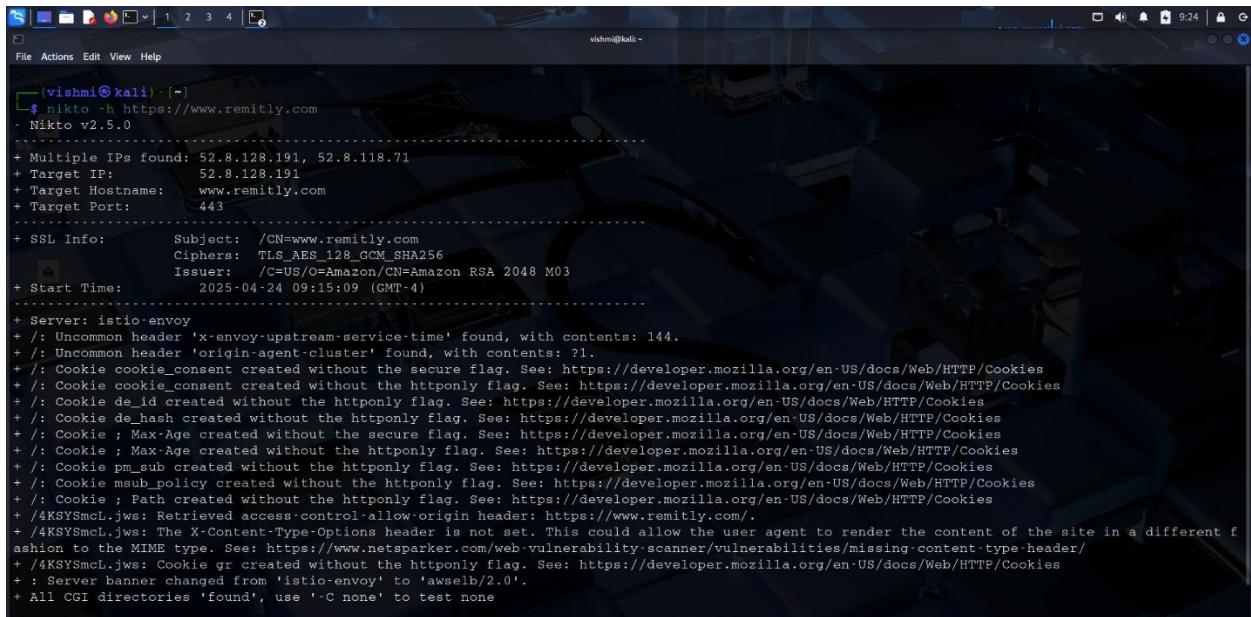
I discovered these details by using Nmap to search [www.remitly.com](http://www.remitly.com).

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

PORT	SERVICE	Vulnerabilities
<b>21/tcp</b>	ftp	Unencrypted credentials are accepted.
<b>80/tcp</b>	http	Transmits plain text data.
<b>443/tcp</b>	https	Deprecated TLS versions are supported.
<b>554/tcp</b>	Rtsp	Usually doesn't have authenticity.
<b>1723/tcp</b>	pptp	Makes use of a weak encryption
<b>5060/tcp</b>	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.



```
vishni@kali:~$ nikto -h https://www.remitly.com
Nikto v2.5.0

+ Multiple IPs found: 52.8.128.191, 52.8.118.71
+ Target IP: 52.8.128.191
+ Target Hostname: www.remitly.com
+ Target Port: 443

+ SSL Info: Subject: /CN=www.remitly.com
Ciphers: TLS_AES_128_GCM_SHA256
Issuer: /C=US/O=Amazon/CN=Amazon RSA 2048 M03
+ Start Time: 2025-04-24 09:15:09 (GMT-4)

+ Server: istio-envoy
+ /: Uncommon header 'x-envoy-upstream-service-time' found, with contents: 144.
+ /: Uncommon header 'origin-agent-cluster' found, with contents: ?1.
+ /: Cookie cookie_consent created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie cookie_consent created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie de_id created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie de_hash created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ; Max-Age created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ; Max-Age created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie pm_sub created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie msrb_policy created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ; Path created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /4KSYSmcL.jws: Retrieved access-control-allow-origin header: https://www.remitly.com/.
+ /4KSYSmcL.jws: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /4KSYSmcL.jws: Cookie gr created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+: Server banner changed from 'istio-envoy' to 'awselb/2.0'.
+ All CGI directories 'found', use '-C none' to test none
```

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 .

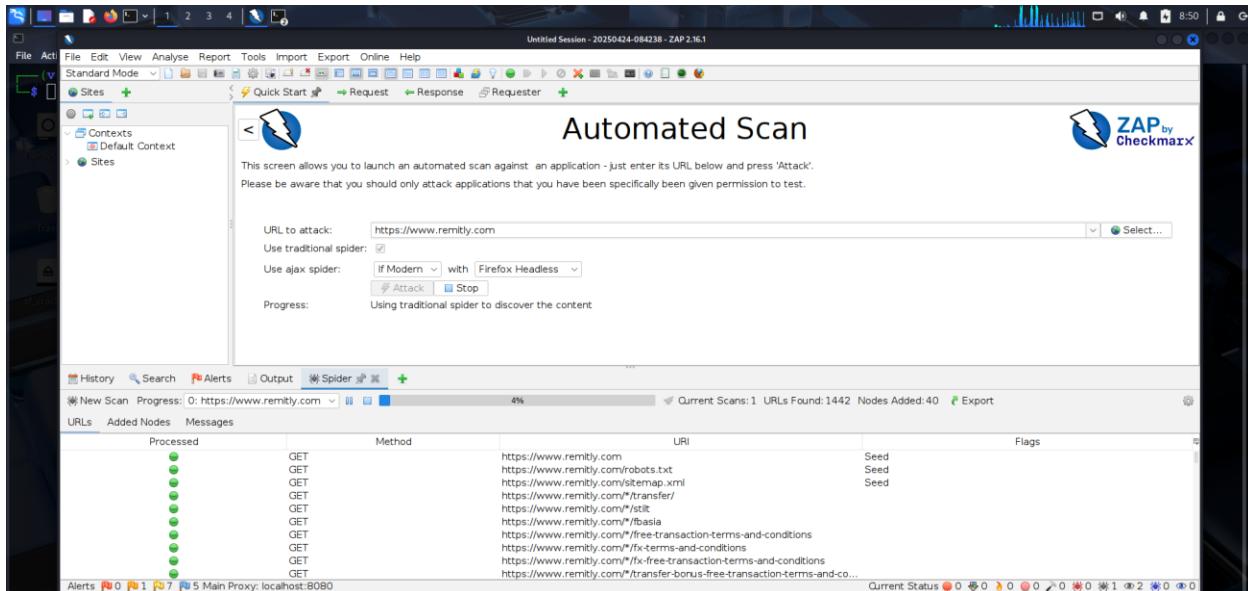
The screenshot shows two instances of the Virustotal interface. The top instance is the main landing page with a search bar and a large 'VIRUSTOTAL' logo. The bottom instance is the detailed analysis page for the URL <https://www.remitly.com>. On this page, it states 'No security vendors flagged this URL as malicious'. The analysis table shows results from various engines:

Security vendor	Result
Abusix	Clean
ADMINUSlabs	Clean
AlienVault	Clean
Artists Against 419	Clean
BitDefender	Clean
Blueliv	Clean
Acronis	Clean
Allabs (MONITORAPP)	Clean
Antiy-AVL	Clean
benkow.cc	Clean
BlockList	Clean
Certego	Clean

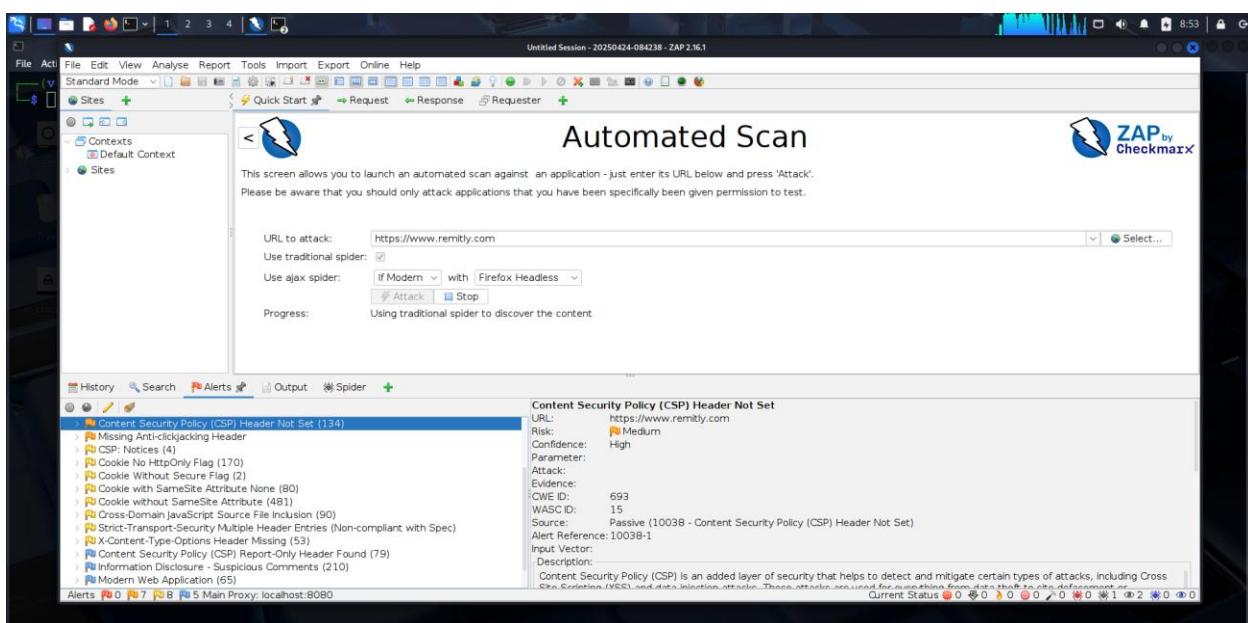
## OWASP ZAP

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](#) ]

The screenshot shows a web browser window with the title "ZAP by Checkmarx Scanner" and the URL "file:///home/vishmi/2025-04-24-ZAP-Report-.html". The page content is as follows:

## 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.)

Risk	User Confirmed	Confidence				Total
		High	Medium	Low		
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.)

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

ZAP by Checkmarx Scanning +

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

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

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

## Vulnerabilities

<b>a.Vulnerability Title</b>	<b>Content-Security-Policy(CSP) Header Not Set</b>
<b>b.Vulnerability Description</b>	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.
<b>c.Affected Components</b>	Web server configuration, HTTP response headers of the web application.
<b>d.Impact Assessment</b>	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.
<b>e.Steps to Reproduce</b>	<ol style="list-style-type: none"><li>1.Open a browser and navigate to the impacted website.</li><li>2.Use the browser developer tools (F12 → Network → Headers tab) to examine the HTTP response headers.</li><li>3.Verify that the answer does not contain the Content-Security-Policy header.</li></ol>
<b>f.Proof of Concept (if applicable)</b>	<ol style="list-style-type: none"><li>1. Open the website (e.g., youtube.google.com) in a web browser.</li><li>2.Use browser Developer Tools (F12), navigate to the "Network" tab, and inspect the HTTP response headers.</li><li>3.Verify that there is no <i>Content-Security-Policy</i> header listed among the response headers.</li></ol>
<b>g.Proposed Mitigation or Fix</b>	Implement a strict Content-Security-Policy (CSP) in the server configuration.

## Report-09

# Web Audit playtika.com

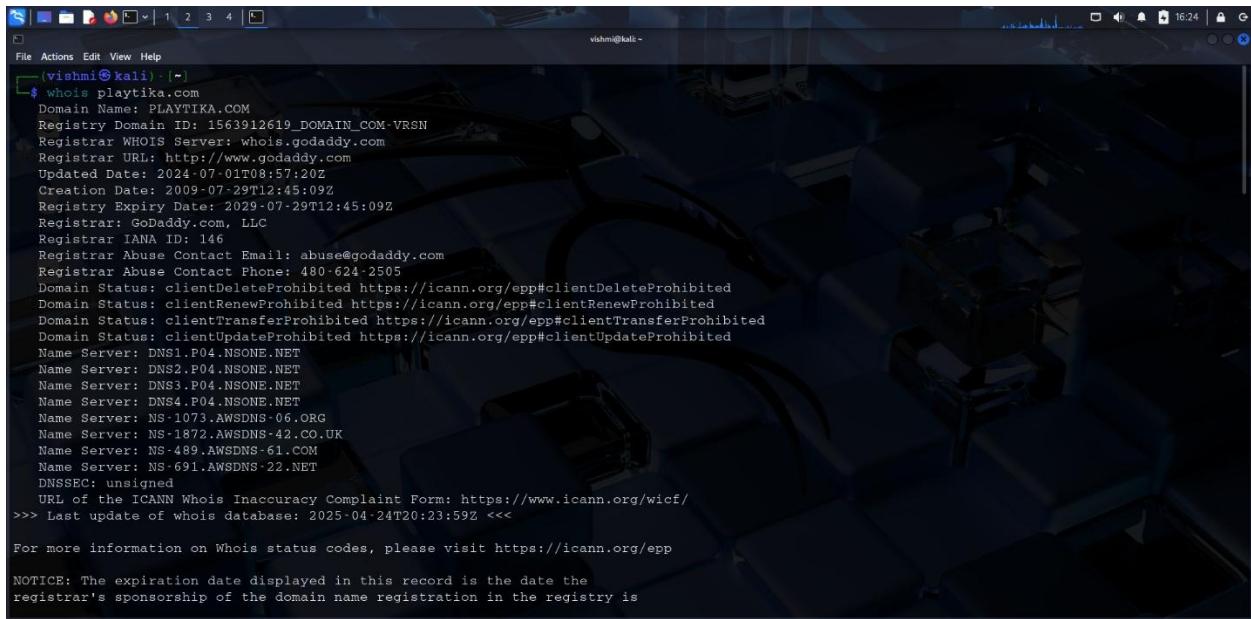
**Domain** = *playtika.com*

**Sub-domain** = *www.playtika.com*

**URL** = *https://www.playtika.com*

# Target Reconnaissance

## Introduction to Playtika and Audit Scope



```
vishni@kali:~$ whois playtika.com
Domain Name: PLAYTIKA.COM
Registry Domain ID: 1563912619_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2024-07-01T08:57:20Z
Creation Date: 2009-07-29T12:45:09Z
Registry Expiry Date: 2029-07-29T12:45:09Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: DNS1.P04.NSONE.NET
Name Server: DNS2.P04.NSONE.NET
Name Server: DNS3.P04.NSONE.NET
Name Server: DNS4.P04.NSONE.NET
Name Server: NS-1073.AWSDNS-06.ORG
Name Server: NS-1872.AWSDNS-42.CO.UK
Name Server: NS-489.AWSDNS-61.COM
Name Server: NS-691.AWSDNS-22.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-24T20:23:59Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
```

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.

The screenshot shows a list of assets within a scope. The columns include Asset name, Type, Coverage, Max. severity, Bounty, Last update, and Resolved Reports. All assets listed are marked as 'In scope' and 'Critical' with an 'Eligible' bounty status. The last update for most assets is from January 2023, while one is from June 2022.

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
586634331	iOS: App Store	In scope	Critical	Eligible	Jun 26, 2022	0 (0%)
1510325826	iOS: App Store	In scope	Critical	Eligible	Jan 18, 2023	0 (0%)
net.wooga.switchcraft.googleplay	Android: Play Store	In scope	Critical	Eligible	Jan 18, 2023	0 (0%)
594802437	iOS: App Store	In scope	Critical	Eligible	Jan 18, 2023	0 (0%)

The screenshot shows a list of assets within a scope. The columns include Asset name, Type, Coverage, Max. severity, Bounty, Last update, and Resolved Reports. Most assets are marked as 'In scope' and 'Critical' with an 'Eligible' bounty status. One asset, com.playtika.caesarscasino, has a different type and severity. The last update for most assets is from October 2021, while others are from May 2023.

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
caesarsgames.com	Wildcard	In scope	Critical	Eligible	2023	0 (0%)
com.playtika.caesarscasino	Android: Play Store	In scope	Critical	Eligible	Oct 27, 2021	0 (0%)
*.wooga.com	Wildcard	In scope	Critical	Eligible	May 15, 2023	12 (5%)
*.playtika.com	Wildcard	In scope	Critical	Eligible	May 15, 2023	75 (34%)
com.jellybtn.cashkingmobile	Android: Play Store	In scope	Critical	Eligible	Aug 24, 2022	0 (0%)

## **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.

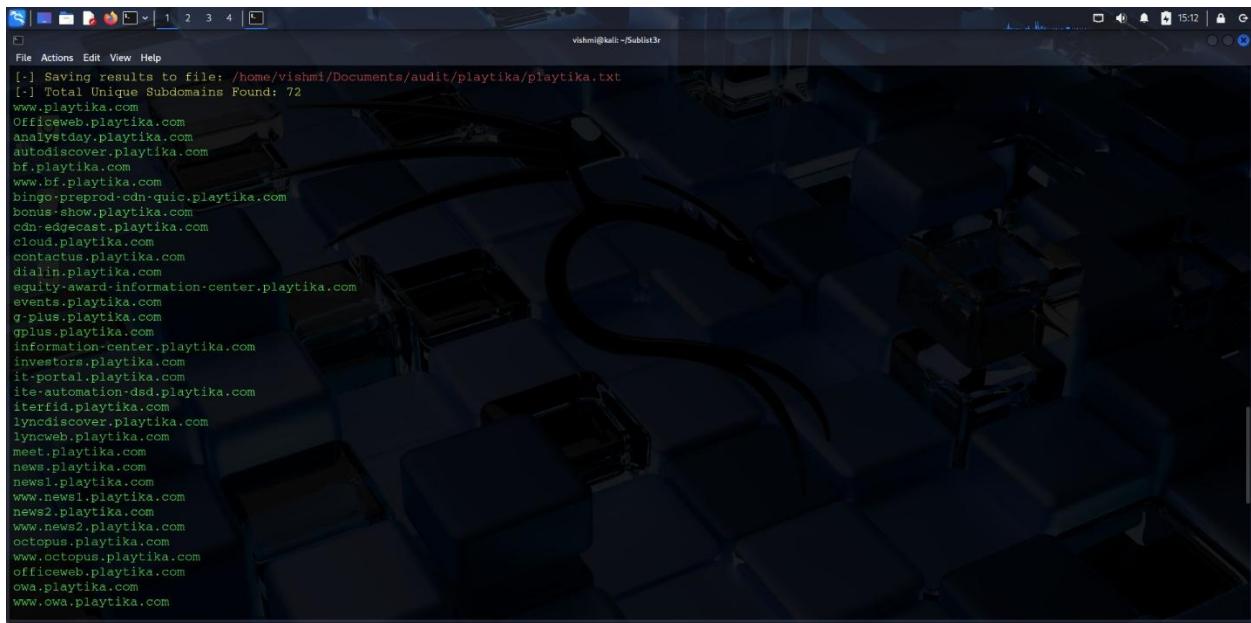
Path to .txt file = *home/vishmi/Documents/audit/ playtika / playtika.txt*

```
vishmi@kali: ~$ sudo mkdir -p /home/vishmi/Documents/audit/playtika
vishmi@kali: ~$ sudo touch /home/vishmi/Documents/audit/playtika/playtika.txt
vishmi@kali: ~$ cd Sublist3r
vishmi@kali: ~/Sublist3r$
```

```
vishmi@kali: ~$ sudo python3 /home/vishmi/Sublist3r/sublist3r.py -d playtika.com -v -o /home/vishmi/Documents/audit/playtika/playtika.txt
```

```
# Coded By Ahmed Aboul-Ela - @aboul3la
[+] Enumerating subdomains now for playtika.com
[+] Verbosity now, 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 SST Certificates..
[+] Searching now in PassiveDNS.
Process GoogleEnum-4:
Traceback (most recent call last):
HTTPConnectionPool(host='dnsdumpster.com', port=443): Max retries exceeded with url: / (Caused by NameResolutionError('<urllib3.connection.HTTPSConnection object at 0x7fad150be900>: Failed to resolve \'dnsdumpster.com\' ([Errno -3] Temporary failure in name resolution)'))
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 240, in enumerate
    if not self.check_response_errors(resp):
  File "/home/vishmi/Sublist3r/sublist3r.py", line 303, in check_response_errors
```

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

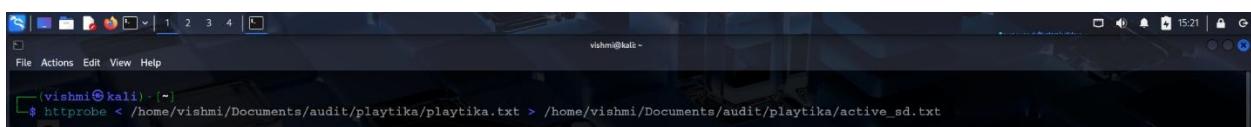


```
vishni@kaiz:/Sublist3r
File Actions Edit View Help
[-] Saving results to file: /home/vishni/Documents/audit/playtika/playtika.txt
[-] Total Unique Subdomains Found: 72
www.playtika.com
Officeweb.playtika.com
analystday.playtika.com
autodiscover.playtika.com
bf.playtika.com
www.bf.playtika.com
bingo-prod-cdn-quic.playtika.com
bonus-show.playtika.com
cdn-edgecast.playtika.com
cloud.playtika.com
contactus.playtika.com
dialin.playtika.com
equity-award-information-center.playtika.com
events.playtika.com
g-plus.playtika.com
oplus.playtika.com
information-center.playtika.com
investors.playtika.com
it-portal.playtika.com
ite-automation-dds.playtika.com
tierid.playtika.com
lyncdiscover.playtika.com
lynctweb.playtika.com
meet.playtika.com
news.playtika.com
news1.playtika.com
www.news1.playtika.com
news2.playtika.com
www.news2.playtika.com
octopus.playtika.com
www.octopus.playtika.com
owa.playtika.com
www.owa.playtika.com
```

## HTTPProbe

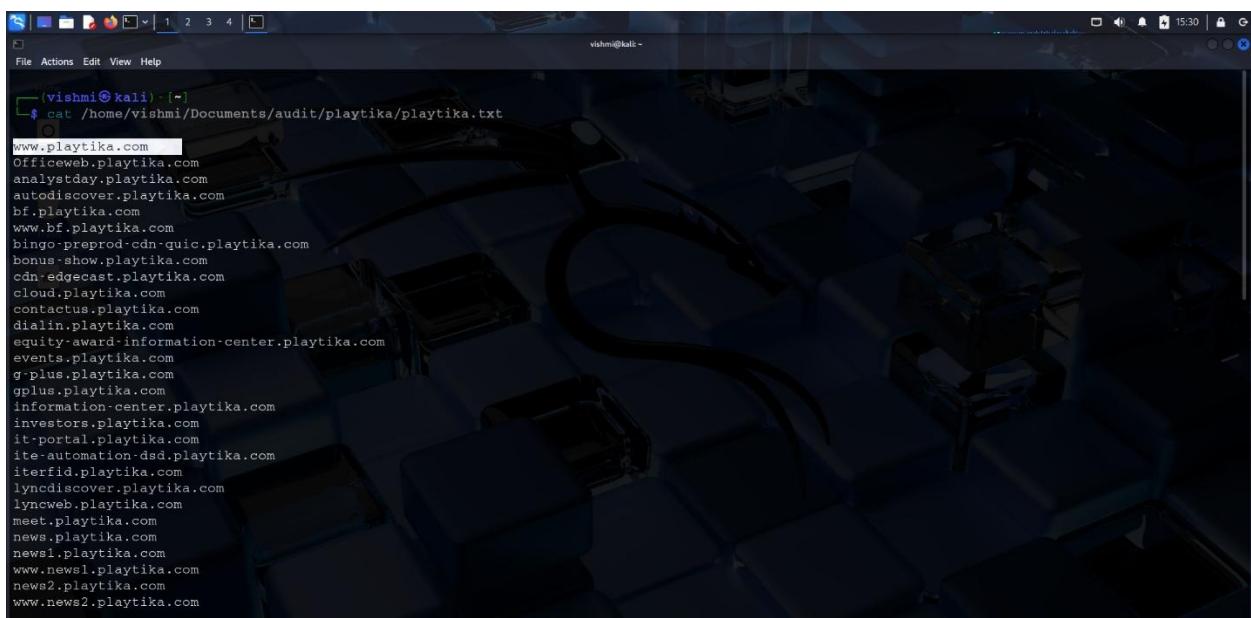
HTTPProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing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



```
vishmi@kali:~$ httpprobe </home/vishmi/Documents/audit/playtika/playtika.txt >/home/vishmi/Documents/audit/playtika/active_sd.txt
```

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

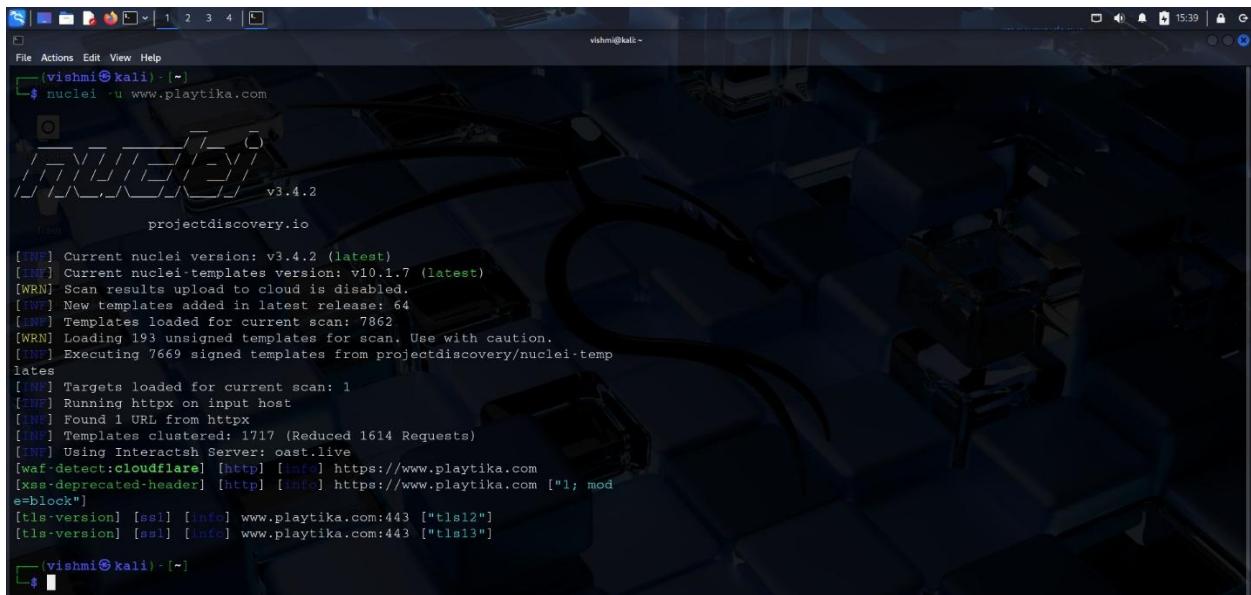


```
vishmi@kali:~$ cat /home/vishmi/Documents/audit/playtika/playtika.txt
www.playtika.com
Officeweb.playtika.com
analystday.playtika.com
autodiscover.playtika.com
bf.playtika.com
www.bf.playtika.com
bingo-preprod-cdn-quic.playtika.com
bonus-show.playtika.com
cdn-edgecast.playtika.com
cloud.playtika.com
contactus.playtika.com
dialin.playtika.com
equity-award-information-center.playtika.com
events.playtika.com
g-plus.playtika.com
gplus.playtika.com
information-center.playtika.com
investors.playtika.com
it-portal.playtika.com
ite-automation-dsd.playtika.com
iterfid.playtika.com
lyncdiscover.playtika.com
lyncweb.playtika.com
meet.playtika.com
news.playtika.com
news1.playtika.com
www.news1.playtika.com
news2.playtika.com
www.news2.playtika.com
```

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).



```
vishmi㉿kali: ~]$ nuclei -u www.playtika.com
v3.4.2
projectdiscovery.io

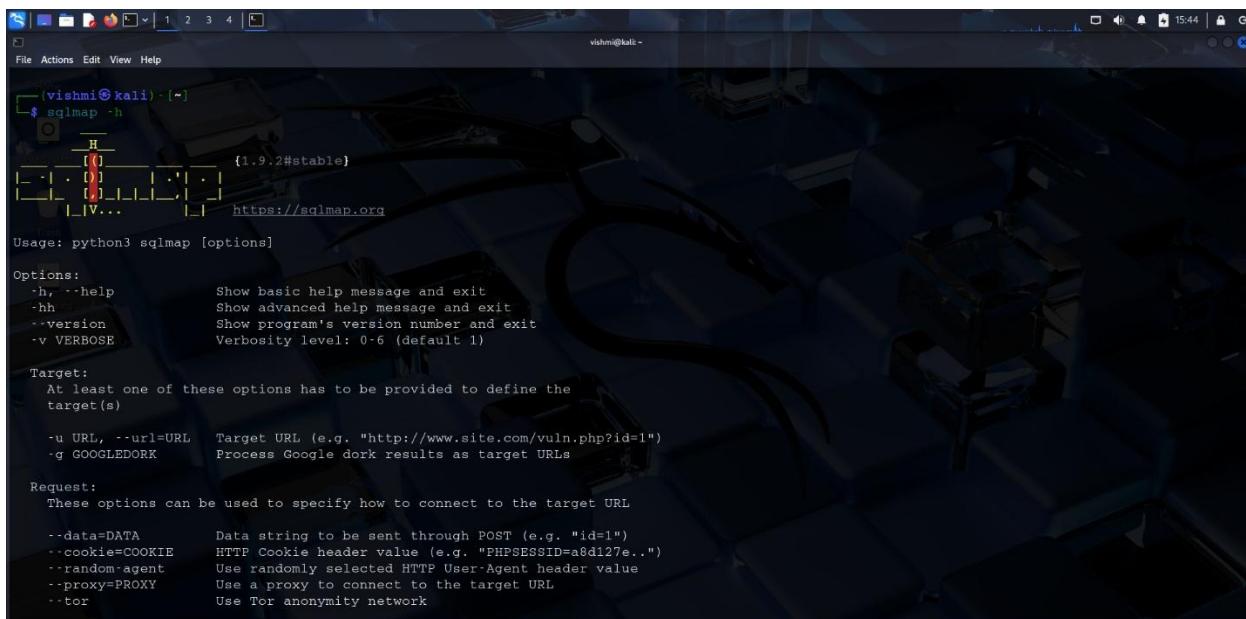
[INFO] Current nuclei version: v3.4.2 (latest)
[INFO] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 64
[INFO] Templates loaded for current scan: 7862
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[INFO] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[INFO] Targets loaded for current scan: 1
[INFO] Running httpx on input host
[INFO] Found 1 URL from httpx
[INFO] Templates clustered: 1717 (Reduced 1614 Requests)
[INFO] Using Interactsh Server: cast.live
[waf-detect:cloudflare] [http] [info] https://www.playtika.com
[xss-deprecated-header] [http] [info] https://www.playtika.com ["1; mod_ebblock"]
[tls-version] [ssl] [info] www.playtika.com:443 ["tls12"]
[tls-version] [ssl] [info] www.playtika.com:443 ["tls13"]

[vishmi㉿kali: ~]$
```

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

## SQLmap

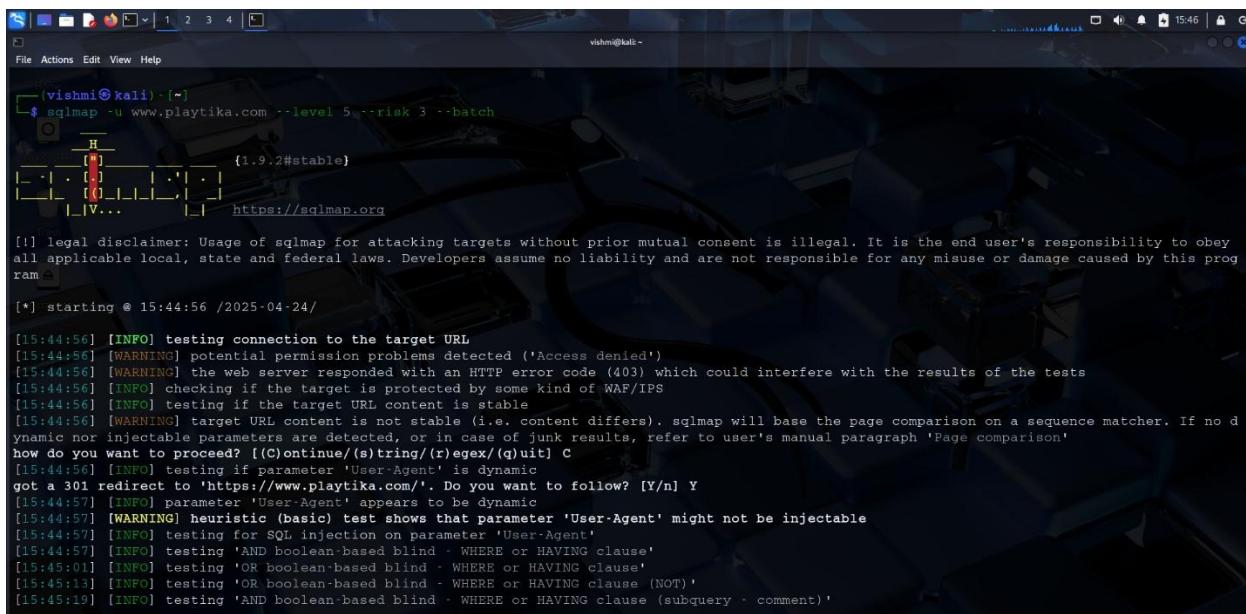
An open-source penetration testing tool called SQLmap makes it easier to find and take advantage of SQL injection flaws in web apps. If the database permits, it can even access the underlying file system or run commands on the server in addition to identifying the type of database and extracting data.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



```
vishmi㉿kali: ~]$ sqlmap -h
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[!] starting @ 15:44:56 /2025-04-24

[15:44:56] [INFO] testing connection to the target URL
[15:44:56] [WARNING] potential permission problems detected ('Access denied')
[15:44:56] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
[15:44:56] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:44:56] [INFO] testing if the target URL content is stable
[15:44:56] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(S)tring/(R)egeX/(Q)uit] C
[15:44:56] [INFO] testing if parameter 'User-Agent' is dynamic
got a 301 redirect to 'https://www.playtika.com/'. Do you want to follow? [Y/n] Y
[15:44:57] [INFO] parameter 'User-Agent' appears to be dynamic
[15:44:57] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[15:44:57] [INFO] testing for SQL injection on parameter 'User-Agent'
[15:44:57] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:45:01] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[15:45:13] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[15:45:19] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
```



```
vishmi㉿kali: ~]$ sqlmap -u www.playtika.com --level 5 --risk 3 --batch
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[!] starting @ 15:44:56 /2025-04-24

[15:44:56] [INFO] testing connection to the target URL
[15:44:56] [WARNING] potential permission problems detected ('Access denied')
[15:44:56] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
[15:44:56] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:44:56] [INFO] testing if the target URL content is stable
[15:44:56] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(S)tring/(R)egeX/(Q)uit] C
[15:44:56] [INFO] testing if parameter 'User-Agent' is dynamic
got a 301 redirect to 'https://www.playtika.com/'. Do you want to follow? [Y/n] Y
[15:44:57] [INFO] parameter 'User-Agent' appears to be dynamic
[15:44:57] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[15:44:57] [INFO] testing for SQL injection on parameter 'User-Agent'
[15:44:57] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:45:01] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[15:45:13] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[15:45:19] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
```

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

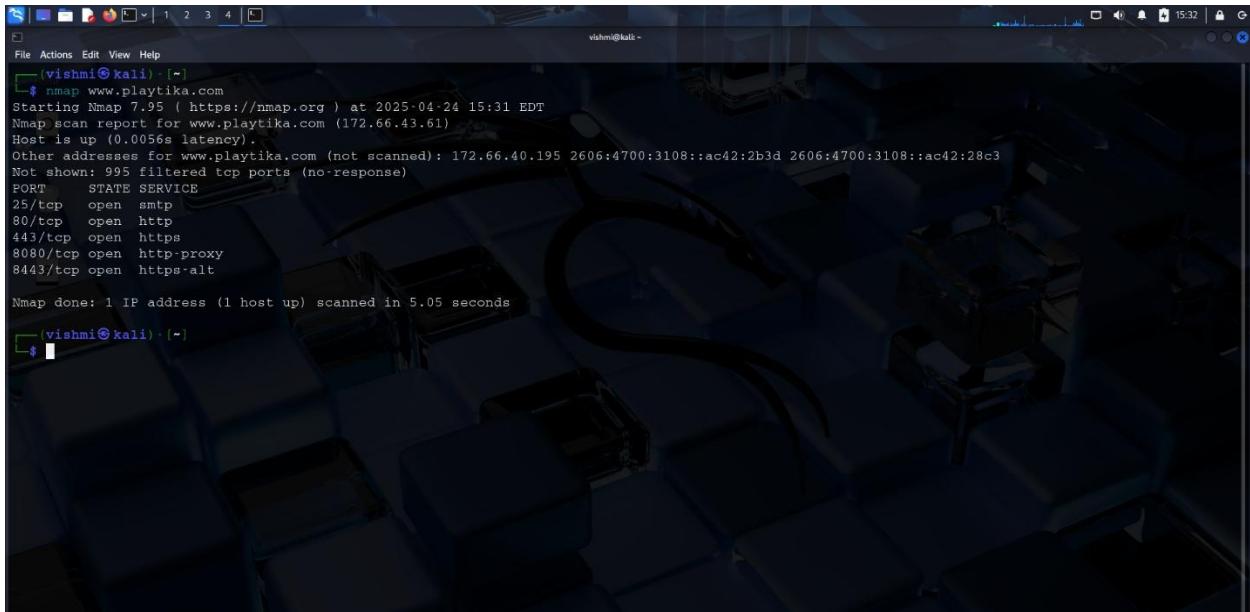
## Detected Information

- \* **[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.



```
vishni㉿kali: ~
$ nmap www.playtika.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 15:31 EDT
Nmap scan report for www.playtika.com (172.66.43.61)
Host is up (0.0056s latency).
Other addresses for www.playtika.com (not scanned): 172.66.40.195 2606:4700:3108::ac42:2b3d 2606:4700:3108::ac42:28c3
Not shown: 995 filtered tcp ports (no-response)
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

Nmap done: 1 IP address (1 host up) scanned in 5.05 seconds

```

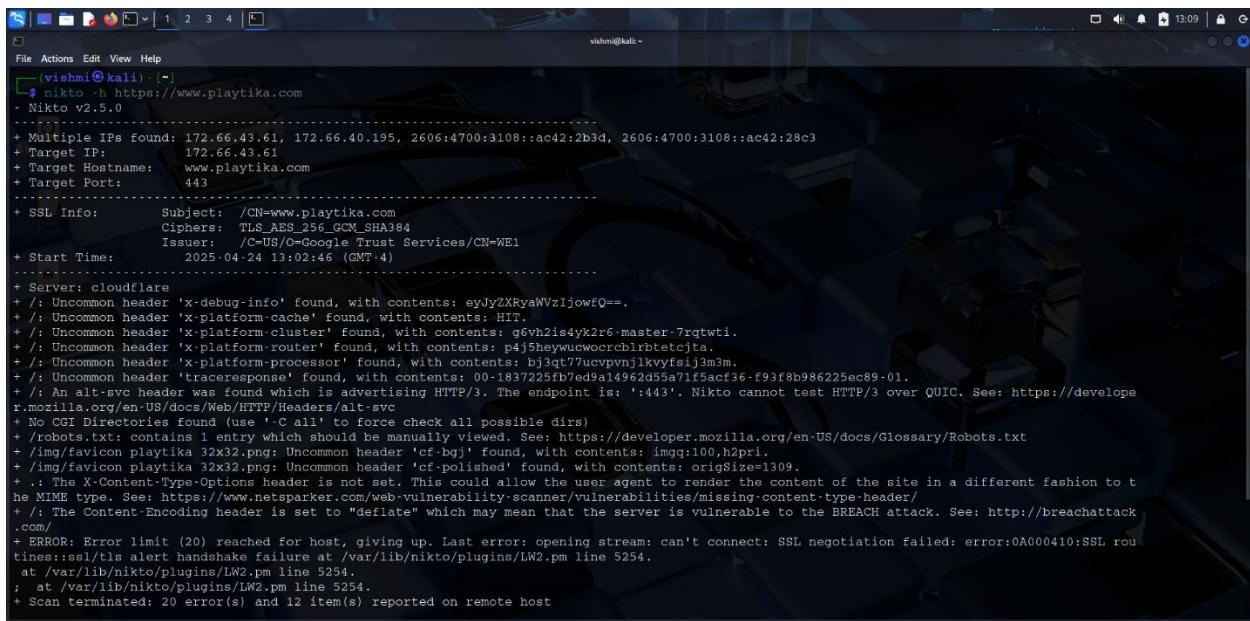
I discovered these details by using Nmap to search [www.playtika.com](http://www.playtika.com).

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

PORT	SERVICE	Vulnerabilities
<b>25/tcp</b>	smtp	Allows open relay if misconfigured; transmits credentials in plaintext.
<b>80/tcp</b>	http	Transmits plain text data.
<b>443/tcp</b>	https	Deprecated TLS versions are supported.
<b>8080/tcp</b>	http-proxy	May expose internal services; often lacks proper authentication.
<b>8443/tcp</b>	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.

A screenshot of a terminal window titled "vishni@kali ~". The command "nikto -h https://www.playtika.com" is run. The output shows Nikto version 2.5.0 scanning multiple IPs (172.66.43.61, 172.66.40.195, 2606:4700:3108::ac42:2b3d, 2606:4700:3108::ac42:28c3) and Target Port 443. It details SSL info, including Subject, Ciphers (TLS\_AES\_256\_GCM\_SHA384), and Issuer (C=US/O=Google Trust Services/CN=WEI). The Start Time was 2025-04-24 13:02:46 (GMT+4). The server is identified as cloudflare. The scan finds various headers like x-debug-info, x-platform-cache, x-platform-cluster, x-platform-router, x-platform-processor, traceresponse, alt-svc, and Content-Encoding. It also finds robots.txt, favicons, and missing Content-Type headers. An error message about SSL negotiation failing is shown. The scan ends with 20 errors and 12 items reported.

```
vishni@kali ~
$ nikto -h https://www.playtika.com
[+] Nikto v2.5.0
[+] Multiple IPs found: 172.66.43.61, 172.66.40.195, 2606:4700:3108::ac42:2b3d, 2606:4700:3108::ac42:28c3
[+] Target IP: 172.66.43.61
[+] Target Hostname: www.playtika.com
[+] Target Port: 443
[+] SSL Info: Subject: /CN=www.playtika.com
[+] Ciphers: TLS_AES_256_GCM_SHA384
[+] Issuer: /C=US/O=Google Trust Services/CN=WEI
[+] Start Time: 2025-04-24 13:02:46 (GMT+4)
[+] Server: cloudflare
[+] /: Uncommon header 'x-debug-info' found, with contents: eyJyZXByaWVzIjowfQ==.
[+] /: Uncommon header 'x-platform-cache' found, with contents: HIT.
[+] /: Uncommon header 'x-platform-cluster' found, with contents: 7rgtwi.
[+] /: Uncommon header 'x-platform-router' found, with contents: p4j5heywucworcb1rbtetcjtia.
[+] /: Uncommon header 'x-platform-processor' found, with contents: bj3qt77ucvpvnjlkvysfisij3m3m.
[+] /: Uncommon header 'traceresponse' found, with contents: 00-1837225fb7ed9a14962d55a71f5acf36-f93f8b986225ec89-01.
[+] /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
[+] No CGI Directories Found (use '-C all' to force check all possible dirs)
[+] /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
[+] /img/favicon playtika 32x32.png: Uncommon header 'cf-bgi' found, with contents: imqg100,h2pri.
[+] /img/favicon playtika 32x32.png: Uncommon header 'cf-polished' found, with contents: origSize=1309.
[+] .: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
[+] .: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
[+] ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::ssl/tls alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
; at /var/lib/nikto/plugins/LW2.pm line 5254.
[+] Scan Terminated: 20 error(s) and 12 item(s) reported on remote host
```

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 .

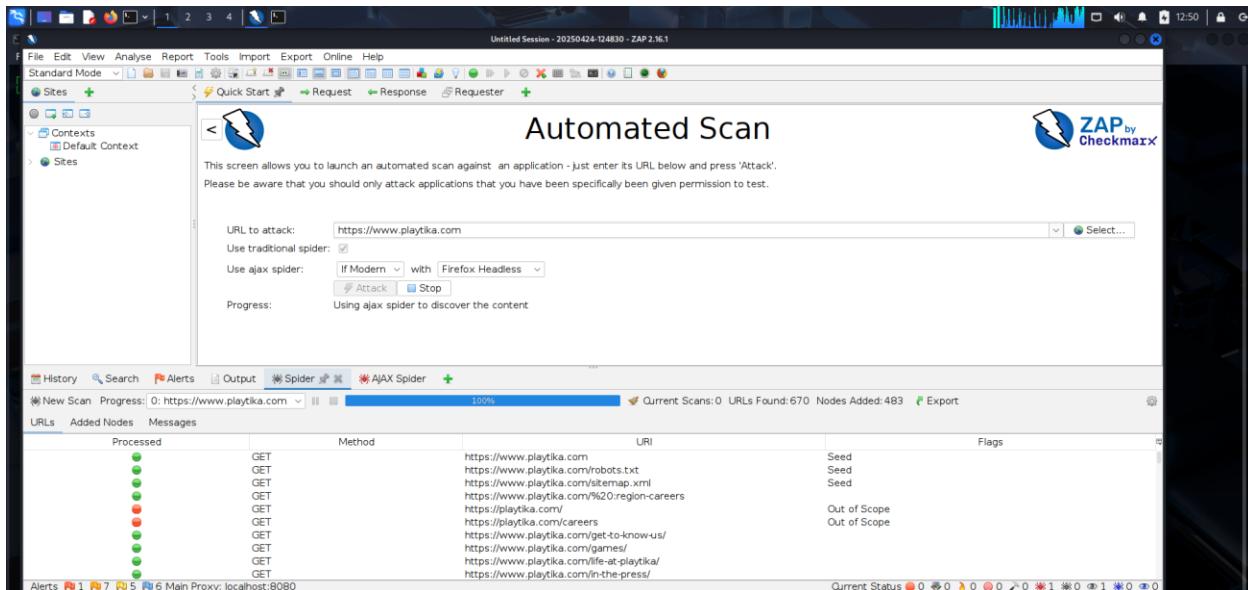
The screenshot shows the Virustotal interface. At the top, there's a search bar with the URL <https://www.playtika.com>. Below the search bar, the main heading is "VIRUSTOTAL". A sub-instruction reads: "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community." There are three tabs: FILE, URL (which is selected), and SEARCH. A "Reanalyze" button is also present. The analysis results for the URL are displayed below. The "Community Score" is shown as 0 / 97, with a note that "No security vendors flagged this URL as malicious". The URL itself is listed as <https://www.playtika.com/>, with the domain [www.playtika.com](http://www.playtika.com). The status is 200, the content type is text/html, and the last analysis date was 19 days ago. Below this, there are tabs for DETECTION, DETAILS, and COMMUNITY. The DETECTION tab is active, showing a table of security vendor analysis results. The table has two columns: "Security vendors' analysis" and "Do you want to automate checks?". The vendors and their findings are:

Security vendors' analysis	Do you want to automate checks?
Abusix Clean	Clean
ADMINUSLabs Clean	Clean
AlienVault Clean	Clean
Antly-AVL Clean	Clean
benkow.cc Clean	Clean
BlockList Clean	Clean
Acronis Clean	Clean
AI Labs (MONITORAPP) Clean	Clean
alphaMountain.ai Clean	Clean
Artists Against 419 Clean	Clean
BitDefender Clean	Clean
Blueliv Clean	Clean

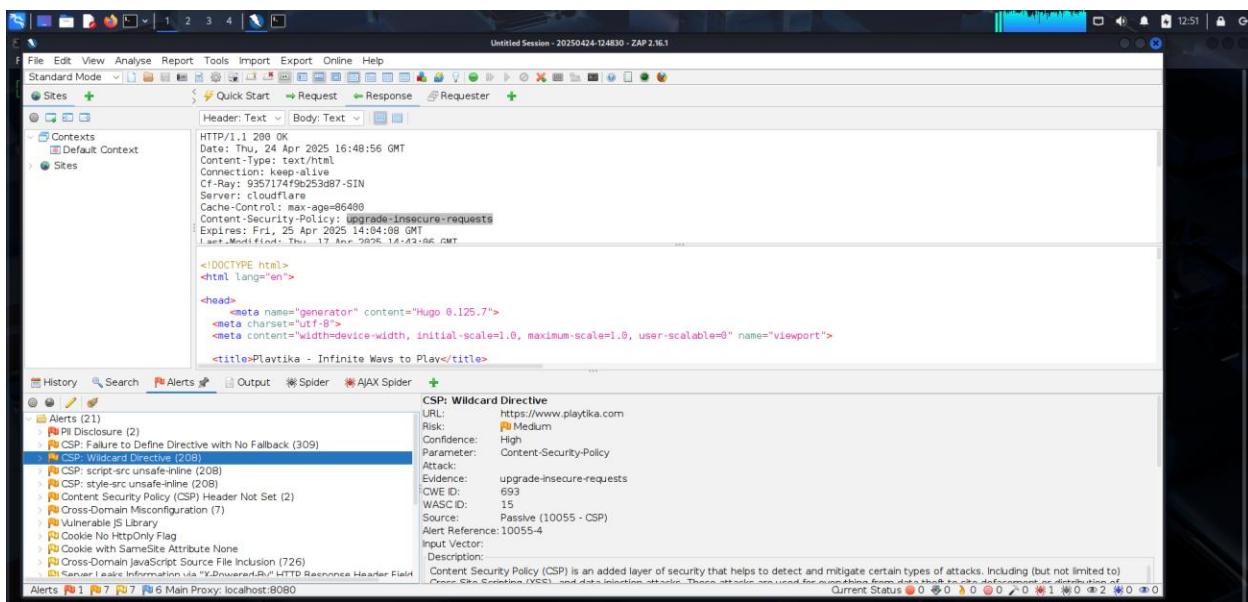
# OWASP ZAP

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](#) ]

The screenshot shows a Firefox browser window with the title "ZAP by Checkmark Scanning" and the URL "file:///home/vishmi/2025-04-24-ZAP-Report-.html". The page content is as follows:

## 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.)

Risk	User Confirmed	Confidence				Total
		High	Medium	Low		
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.)

Site	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informati onal)
<a href="https://www.playtika.com">https://www.playtika.com</a>	1 (1)	6 (7)	5 (12)	5 (17)

ZAP by Checkmark Scanning + file:///home/vishnu/2025-04-24-ZAP-Report-.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

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

# Vulnerabilities

<b>a.Vulnerability Title</b>	<b>CSP:Wildcard directive</b>
<b>b.Vulnerability Description</b>	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.
<b>c.Affected Components</b>	HTTP response headers defining the Content Security Policy. Directives like script-src, style-src, img-src, and others using the wildcard (*).
<b>d.Impact Assessment</b>	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.
<b>e.Steps to Reproduce</b>	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:  <code>&lt;script&gt;alert('Vulnerability Confirmed');&lt;/script&gt;</code>
<b>f.Proof of Concept (if applicable)</b>	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.
<b>g.Proposed Mitigation or Fix</b>	Replace wildcard (*) directives with specific, trusted sources. Avoid using <i>unsafe-inline</i> or <i>unsafe-eval</i> in CSP directives.

## **Report-10**

# **Web Audit**

## ***front.com***

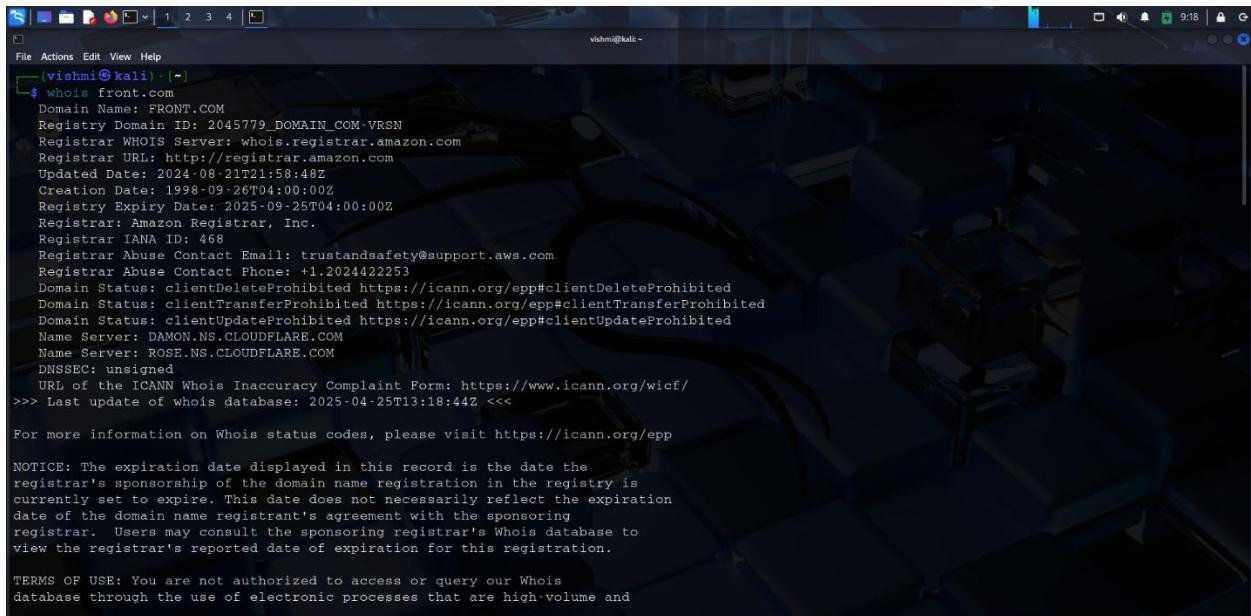
**Domain** = *front.com*

**Sub-domain** = *help.front.com*

**URL** = *https://front.com*

# Target Reconnaissance

Introduction to Front and Audit Scope.



```
vishni@kali: ~
$ whois front.com
Domain Name: FRONT.COM
Registry Domain ID: 2045779_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon.com
Registrar URL: http://registrar.amazon.com
Updated Date: 2024-08-21T21:58:48Z
Creation Date: 1998-09-26T04:00:00Z
Registry Expiry Date: 2025-09-25T04:00:00Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: trustandsafety@support.aws.com
Registrar Abuse Contact Phone: +1.2024422253
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: DAMON.NS.CLOUDFLARE.COM
Name Server: ROSE.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-25T13:18:44Z <<
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
```

**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.

This screenshot shows the 'Scope' section of the hackerone.com frontapp policy\_scopes page. The page displays a table of assets with the following columns: Asset name, Type, Coverage, Max. severity, Bounty, Last update, and Resolved Reports. The table lists the following assets:

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
api2.frontapp.com This scope is our public API documented at <a href="https://dev.frontapp.com/">https://dev.frontapp.com/</a>	Domain	In scope	Critical	Eligible	May 14, 2019	1 (0%)
app.frontapp.com	Domain	In scope	Critical	Eligible	Nov 23, 2018	172 (83%)
Front for Mac Download here: <a href="https://front.com/download">https://front.com/download</a>	Executable	In scope	High	Eligible	Oct 14, 2021	1 (0%)
com.frontapp.mobile <a href="https://play.google.com/store/apps/details?id=com.frontapp.mobile">https://play.google.com/store/apps/details?id=com.frontapp.mobile</a>	Android: Play Store	In scope	High	Eligible	Oct 14, 2021	3 (1%)
						1-6 of 6

This screenshot shows the 'Scope' section of the hackerone.com frontapp policy\_scopes page. The page displays a table of assets with the following columns: Asset name, Type, Coverage, Max. severity, Bounty, Last update, and Resolved Reports. The table lists the following assets:

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
Front for Mac Download here: <a href="https://front.com/download">https://front.com/download</a>	Executable	In scope	High	Eligible	Oct 14, 2021	1 (0%)
com.frontapp.mobile <a href="https://play.google.com/store/apps/details?id=com.frontapp.mobile">https://play.google.com/store/apps/details?id=com.frontapp.mobile</a>	Android: Play Store	In scope	High	Eligible	Oct 14, 2021	3 (1%)
com.frontapp.mobile <a href="https://apps.apple.com/us/app/frontapp/id983808769">https://apps.apple.com/us/app/frontapp/id983808769</a>	iOS: App Store	In scope	High	Eligible	Oct 14, 2021	1 (0%)
Front for Windows Download here: <a href="https://front.com/download">https://front.com/download</a>	Executable	In scope	High	Eligible	Oct 14, 2021	3 (1%)
						1-6 of 6

## **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

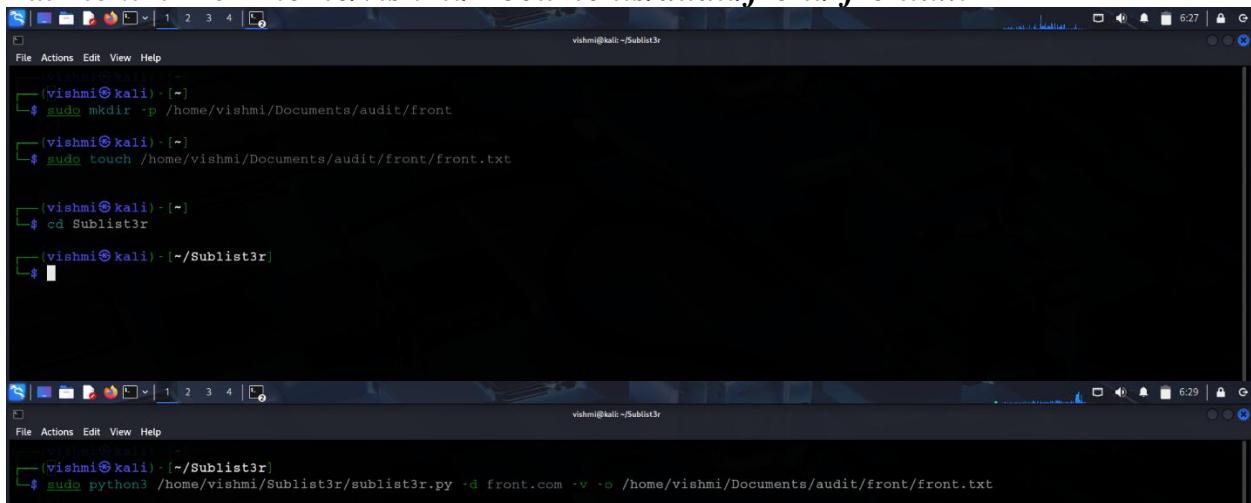
# Finding active subdomains and their states

## 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*



```
vishmi@kali: ~$ sudo mkdir -p /home/vishmi/Documents/audit/front
vishmi@kali: ~$ sudo touch /home/vishmi/Documents/audit/front/front.txt
vishmi@kali: ~$ cd Sublist3r
vishmi@kali: ~/Sublist3r$ 

vishmi@kali: ~$ sudo python3 /home/vishmi/Sublist3r/sublist3r.py -d front.com -v -o /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()
    ~~~~~~^A
  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]
    ~~~~~~^A
```

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

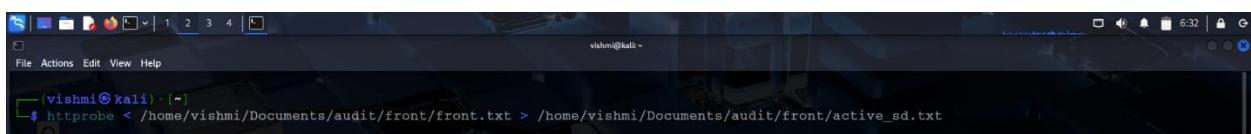
```
[+] Saving results to file: /home/vishmi/Documents/audit/front/front.txt
[+] Total Unique Subdomains Found: 16
www.front.com
academy.front.com
onboarding.api.front.com
beta.front.com
upflow-email.billing.front.com
chat.front.com
community.front.com
help.front.com
it-support.front.com
onboarding.front.com
trust.front.com
vercel-beta.front.com
out--front.com
www.out--front.com
wave--front.com
www.wave--front.com

(vishmi㉿kali) - ~/Sublist3r
└─$ └─
```

## HTTPProbe

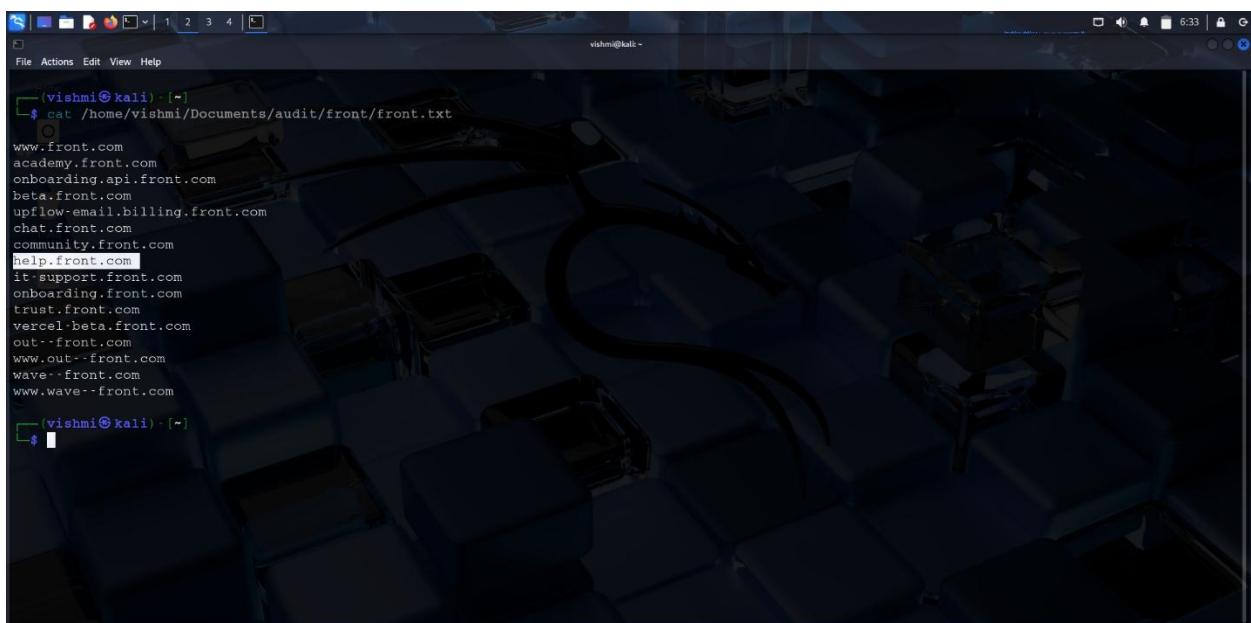
HTTPProbe is a command-line tool designed to quickly check which domains or subdomains from a list are serving content over HTTP or HTTPS. For effectively identifying active web servers during detection, it is especially common among hackers and bug bounty hunters. The tool helps you target your testing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



```
vishmi@kali:~$ httpprobe </home/vishmi/Documents/audit/front/front.txt > /home/vishmi/Documents/audit/front/active_sd.txt
```

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

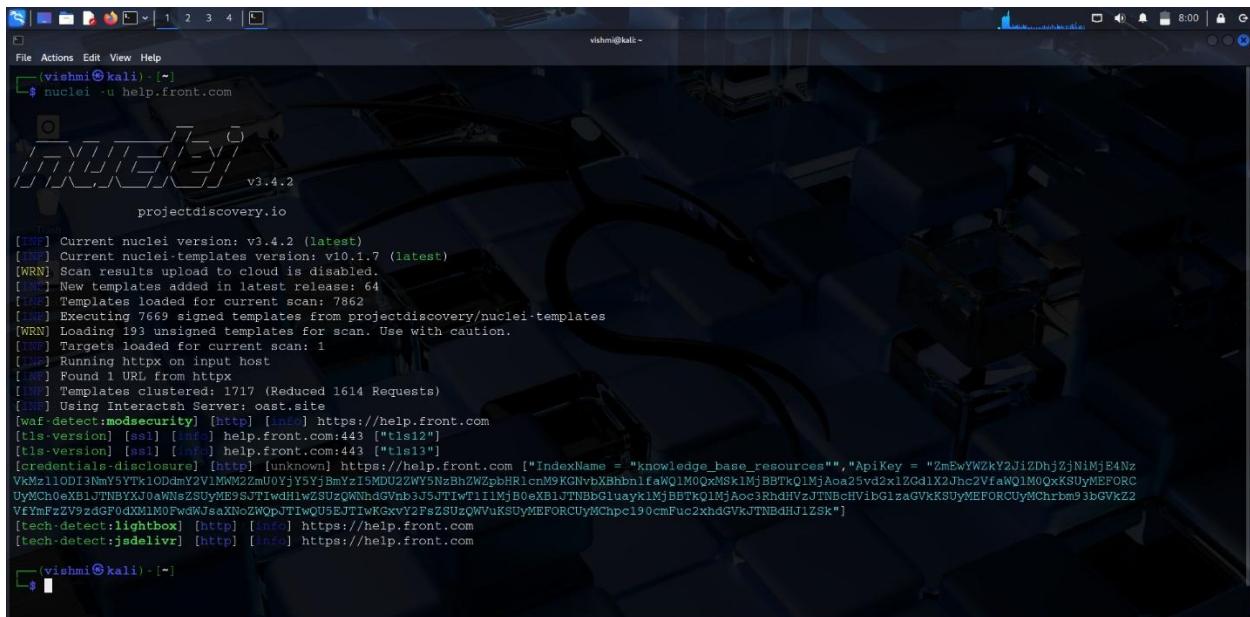


```
vishmi@kali:~$ cat /home/vishmi/Documents/audit/front/front.txt
www.front.com
academy.front.com
onboarding.api.front.com
beta.front.com
upflow-email.billing.front.com
chat.front.com
community.front.com
help.front.com
it-support.front.com
onboarding.front.com
trust.front.com
vercel-beta.front.com
out-front.com
www.out-front.com
wave-front.com
www.wave-front.com
```

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).



```
vishni@kali: ~$ nuclei -u help.front.com
[INFO] Current nuclei version: v3.4.2 (latest)
[INFO] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 64
[INFO] Templates loaded for current scan: 7862
[INFO] Executing 7669 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[INFO] Targets loaded for current scan: 1
[INFO] Running httpx on input host
[INFO] Found 1 URL from httpx
[INFO] Templates clustered: 1717 (Reduced 1614 Requests)
[INFO] Using interactx Server: east.site
[waf-detect:modsecurity] [http] [http] https://help.front.com
[tls-version] [ssl] [http] help.front.com:443 ["tls12"]
[tls-version] [ssl] [http] help.front.com:443 ["tls13"]
[credentials-disclosure] [http] [unknown] https://help.front.com ["IndexName = "knowledge_base_resources","ApiKey = "ZmEwYWZkY2JiZDhjZjNiMjE4NzVkJ1ODI3NmYTTk1ODmY2V1MW22m0UyJY5YjBmYz15MDU22WY5NzBhZWZpbHRlcnM9KGNvbXBhbnifaWQ1M0QxMSk1MjBBTkQ1MjAoa25vd2x1ZGd1X2Jhc2VfaWQ1M0QxKSUyMEFORCuyMChrbm93bGVkZ2UyMCh0eXB1jTNByJ0aNzSUyME5SJTIdh1wZSUQzWNhGvNj5JTi1wT1i1MjB0eXB1jTNBbGluayk1MjBBTkQ1MjAoc3RhdHVzJTNBcHViZlaGVKKSUyMEFORCuyMChpc190cmFuc2xhdGVkjTNBdHj1ZSk"]
[tech-detect:lightbox] [http] [http] https://help.front.com
[tech-detect:jsdelivr] [http] [http] https://help.front.com
[vishni@kali: ~]$
```

Vulnerability Type	Description	Risk
<b>Modsecurity</b> <b>WAF (Web Application Firewall)</b>	Web firewall detected	Low/ Informational
<b>Tech-detect:lightbox</b>	Possibly allowing illegal access to data or information by implementing weak protections.	Medium
<b>SSL/TLS Certificate Expiry</b>	SSL/TLS certificate expired for go.figma.com:443.	High
<b>Tech-detect:jsdelivr</b>	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.

```
vishni㉿kali: ~]$ sqlmap -h
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 07:47:30 / 2025-04-25

[07:47:31] [INFO] testing connection to the target URL
[07:47:34] [INFO] checking if the target is protected by some kind of WAF/IPS
[07:47:35] [INFO] testing if the target URL content is stable
[07:47:36] [INFO] target URL content is stable
[07:47:36] [INFO] testing if parameter 'User-Agent' is dynamic
[07:47:37] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[07:47:38] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[07:47:39] [INFO] testing for SQL injection on parameter 'User-Agent'
[07:47:39] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:49:01] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[07:50:02] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[07:50:40] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[07:51:12] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[07:51:48] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[07:51:56] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[07:52:09] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[07:52:16] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)',
```

Option	Meaning
<b>-u</b>	For basic testing, the target URL is required.
<b>--level5</b>	Increases the number of payloads and tests that are done (maximum is 5).
<b>--risk3</b>	Increase the danger level of the payloads used (maximum is 3)
<b>--batch</b>	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.]

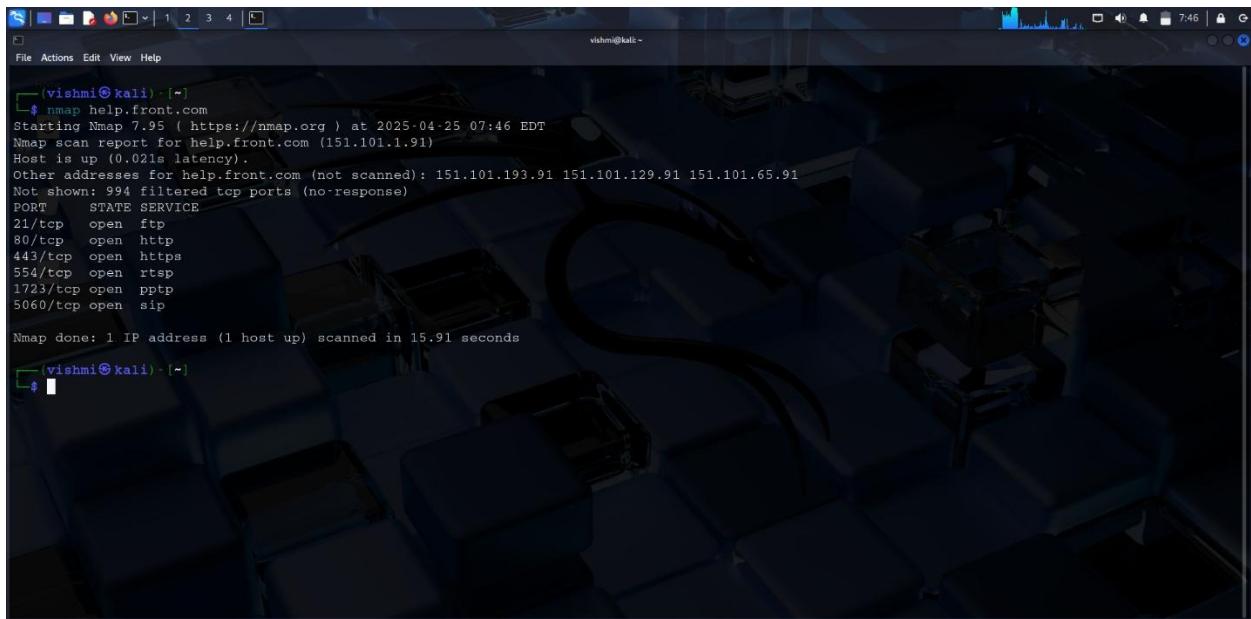
\* **[INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'**

[ 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.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal output displays the results of an Nmap scan against the host help.front.com. The scan report includes information about the host being up with 0.02ms latency, other addresses on the network, and a table of open ports with their corresponding states and services. The scan completed in 15.91 seconds.

```
vishmi㉿kali:~$ nmap help.front.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 07:46 EDT
Nmap scan report for help.front.com (151.101.1.91)
Host is up (0.02ms latency).
Other addresses for help.front.com (not scanned): 151.101.193.91 151.101.129.91 151.101.65.91
Not shown: 994 filtered tcp ports (no-response)
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

Nmap done: 1 IP address (1 host up) scanned in 15.91 seconds
vishmi㉿kali:~$
```

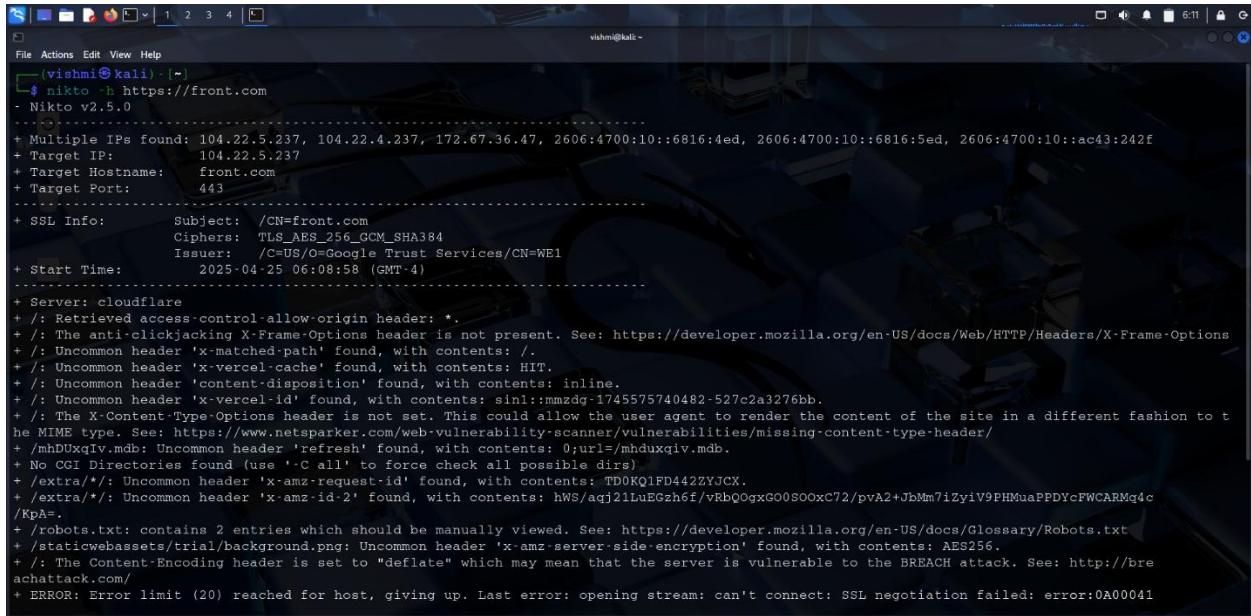
I discovered these details by using Nmap to search *help.front.com*.

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

PORT	SERVICE	Vulnerabilities
<b>21/tcp</b>	ftp	Unencrypted credentials are accepted.
<b>80/tcp</b>	http	Transmits plain text data.
<b>443/tcp</b>	https	Deprecated TLS versions are supported.
<b>554/tcp</b>	Rtsp	Usually doesn't have authenticity.
<b>1723/tcp</b>	pptp	Makes use of a weak encryption
<b>5060/tcp</b>	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.



```
vishni@kali:~$ nikto -h https://front.com
[+] Nikto v2.5.0
[+] Multiple IPs found: 104.22.5.237, 104.22.4.237, 172.67.36.47, 2606:4700:10::6816:4ed, 2606:4700:10::6816:5ed, 2606:4700:10::ac43:242f
[+] Target IP: 104.22.5.237
[+] Target Hostname: front.com
[+] Target Port: 443
[+] SSL Info: Subject: /CN=front.com
[+] Ciphers: TLS_AES_256_GCM_SHA384
[+] Issuer: /C=US/O=Google Trust Services/CN=WE1
[+] Start Time: 2025-04-25 06:08:58 (GMT -4)
[+] Server: cloudflare
[+] Retrieved access-control-allow-origin header: *.
[+] The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
[+] Uncommon header 'x-matched-path' found, with contents: /.
[+] Uncommon header 'x-vercel-cache' found, with contents: HIT.
[+] Uncommon header 'content-disposition' found, with contents: inline.
[+] Uncommon header 'x-vercel-id' found, with contents: sin1:mmzdg-1745575740482-527c2a3276bb.
[+] The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
[+] /mhDUXqIV.mdb: Uncommon header 'refresh' found, with contents: 0;url=/mhduxqiv.mdb.
[+] No CGI Directories found (use '-C all' to force check all possible dirs)
[+] /extra//: Uncommon header 'x-amz-request-id' found, with contents: TD0KQ1FD442ZYJCX.
[+] /extra//: Uncommon header 'x-amz-id-2' found, with contents: hWS/aqj21LuEGzh6f/vRbQ0gxG00SO0xC72/pvA2+JbMm7iZyiV9PHMuapPPDYcFWCARm4c/KpA=.
[+] /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
[+] /staticwebassets/trial/background.png: Uncommon header 'x-amz-server-side-encryption' found, with contents: AES256.
[+] The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
[+] ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A00041
```

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 .

The screenshot shows two browser windows for the Virustotal URL analysis service.

**Top Window:** The main landing page for VirusTotal. It features a large blue 'Σ' logo and the word 'VIRUSTOTAL'. Below the logo is a subtitle: "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community." There are tabs for FILE, URL (which is selected), and SEARCH. A search bar contains the URL <https://front.com>. A "Search" button is below the bar. A note at the bottom states: "By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Notice](#), and to the **sharing of your URL submission with the security community**. Please do not submit any personal information; we are not responsible for the contents of your submission. [Learn more](#)".

**Bottom Window:** The detailed analysis report for the submitted URL. The URL is listed as <https://front.com/>. The report indicates "0 / 97" for the Community Score. The status is 200, Content type is text/html; charset=utf-8, and Last Analysis Date is 17 hours ago. Below this, there are tabs for DETECTION, DETAILS, and COMMUNITY. The DETECTION tab is active, showing a table of security vendor analysis results:

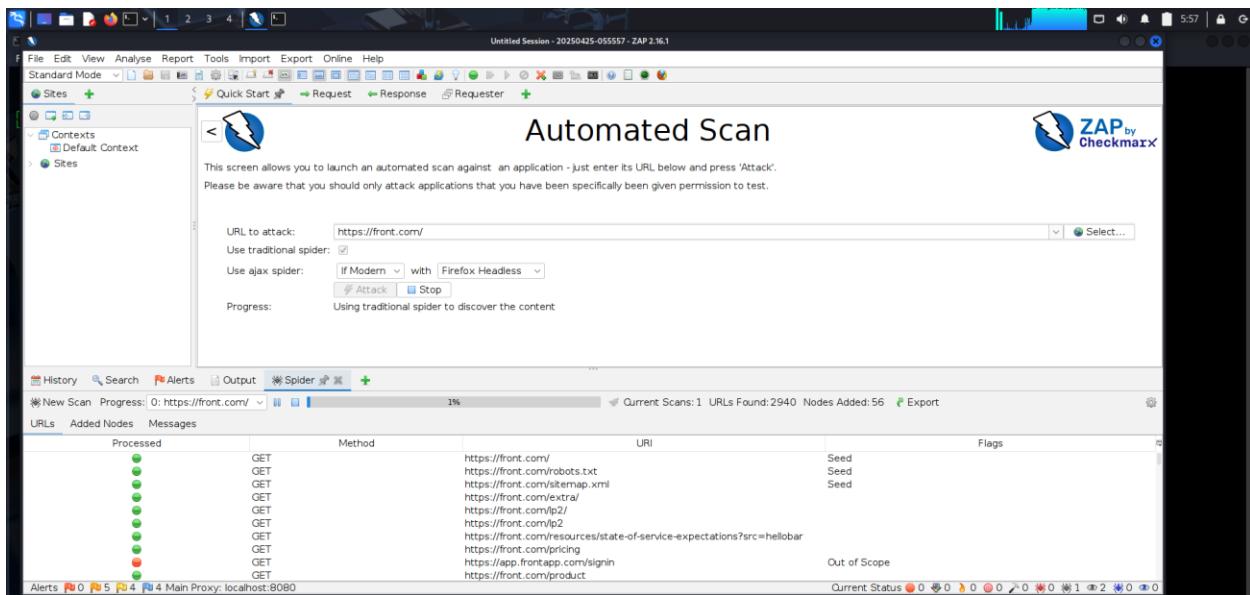
Security vendor	Result	Details	
URLQuery	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AllLabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Anti-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean
BitDefender	Clean	BlockList	Clean

A "Join our Community" button is visible above the detection table. To the right of the table, there is a "Do you want to automate checks?" link and a blue circular icon with a white question mark.

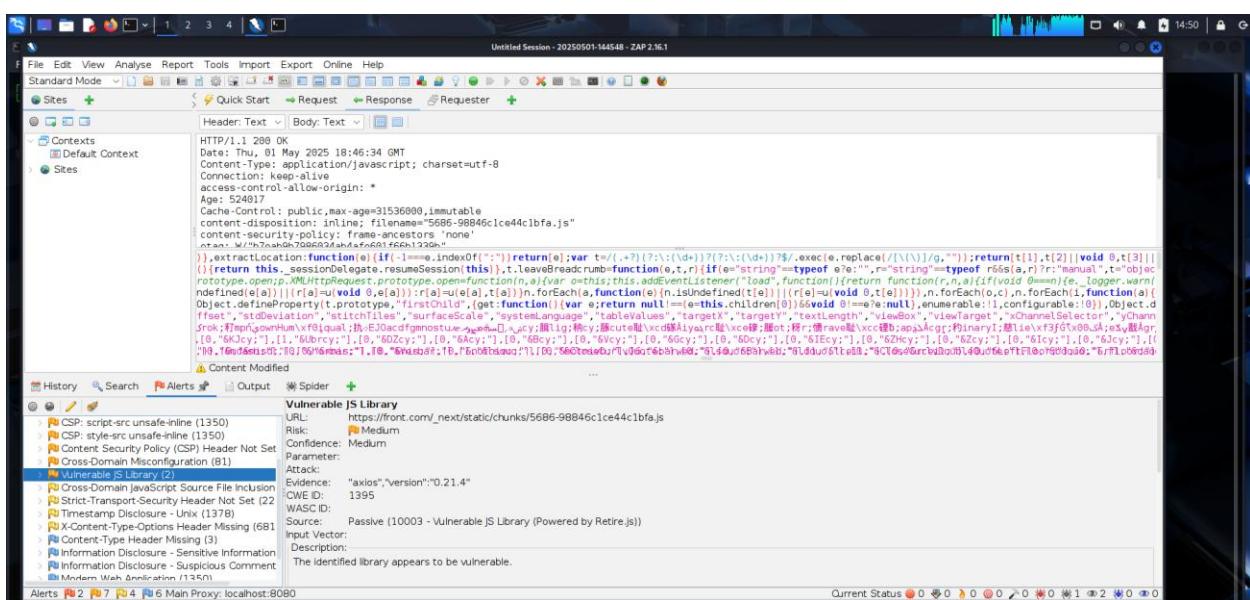
## OWASP ZAP

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](#)]

The screenshot shows a web browser window with a dark theme. The address bar indicates the page is 'file:///home/vishmi/2025-04-25-ZAP-Report-.html'. The main content area is titled '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.)

Risk	User Confirmed	Confidence				Total
		High	Medium	Low	Total	
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**

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.)

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

## Vulnerabilities

<b>a.Vulnerability Title</b>	<b>Vulnerable JavaScript Library(Axios v0.21.4)</b>
<b>b.Vulnerability Description</b>	The application's Axios JavaScript library version (v0.21.4) is vulnerable to security flaws, increasing the attack surface and potentially affecting data integrity.
<b>c.Affected Components</b>	<a href="https://front.com/_next/static/chunks/5686-98846c1ce44c1bfa.js">https://front.com/_next/static/chunks/5686-98846c1ce44c1bfa.js</a>
<b>d.Impact Assessment</b>	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.
<b>e.Steps to Reproduce</b>	<ol style="list-style-type: none"><li>1. Start OWASP ZAP, then crawl the application (in this case, <a href="https://front.com">https://front.com</a>).</li><li>2. Find the "Vulnerable JS Library" notice under the "Alerts" tab.</li><li>3. Examine the information indicating that Axios version="0.21.4" is marked as problematic.</li><li>4. Use <i>Retire.js</i> to compare this version to known vulnerabilities.</li></ol>
<b>f.Proof of Concept (if applicable)</b>	Select the alert associated with the JS chunk <i>5686-98846c1ce44c1bfa.js</i> after opening ZAP.  Verify the Axios version that is vulnerable in the metadata that <i>Retire.js</i> provides.  Open the JS file or look for version metadata in the headers to manually check the library version.
<b>g.Proposed Mitigation or Fix</b>	Regularly update the Axios library, audit third-party libraries, and incorporate dependency checking tools like <i>Retire.js</i> , <i>Snyk</i> , or <i>npm audit</i> 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=bf2Yuqga\\_eWo&list=PLH8n\\_ayg-60J9i3nsLybper-DR3zJw6Z5](https://www.youtube.com/watch?v=bf2Yuqga_eWo&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>