Sri Lanka Institute of Information Technology

# BUG BOUNTY

SNP Assignment

IE2012 – Systems and Network Programming.

Submitted by:

**IT22199508 – Athapaththu A.M.M.I.P**

Date of submission

2023.11.05

# Table of Contents

# Acknowledgment

I would like to express my sincere gratitude to Dr. Lakmal Rupasinghe for his relentless effort in guiding us and advising us through difficult and unfamiliar phases of the project and helping us gain practical knowledge and skills in the subject.

It is with heartfelt appreciation that I thank Mr. Tharaniyawarma and Mr.Kohilan for helping me throughout the semester to gain new knowledge and understand concepts of Web security and how to implement them in the practical world.

# Purpose

The purpose of this assignment is the assess vulnerabilities of the web application. So, https://www.hackerone.com/ (Fig.1) platform is used to find the websites and web applications for the Bug Bounty hunting. And there are a lot of Bug Bounty hunting platforms to improve our vulnerability assessing skills. As an example, https://www.bugcrowd.com/ is one of the Bug Bounty hunting platforms. So, the purpose of using this Hackerone platform is because this website legally protects us to do Bug Bounty hunting for real-world web applications.

Using these websites benefits to get powerful knowledge about the penetration testing tool and how to use those tools. And these web audit reports are giving an excellent understanding of how to handle cybersecurity profession skills.

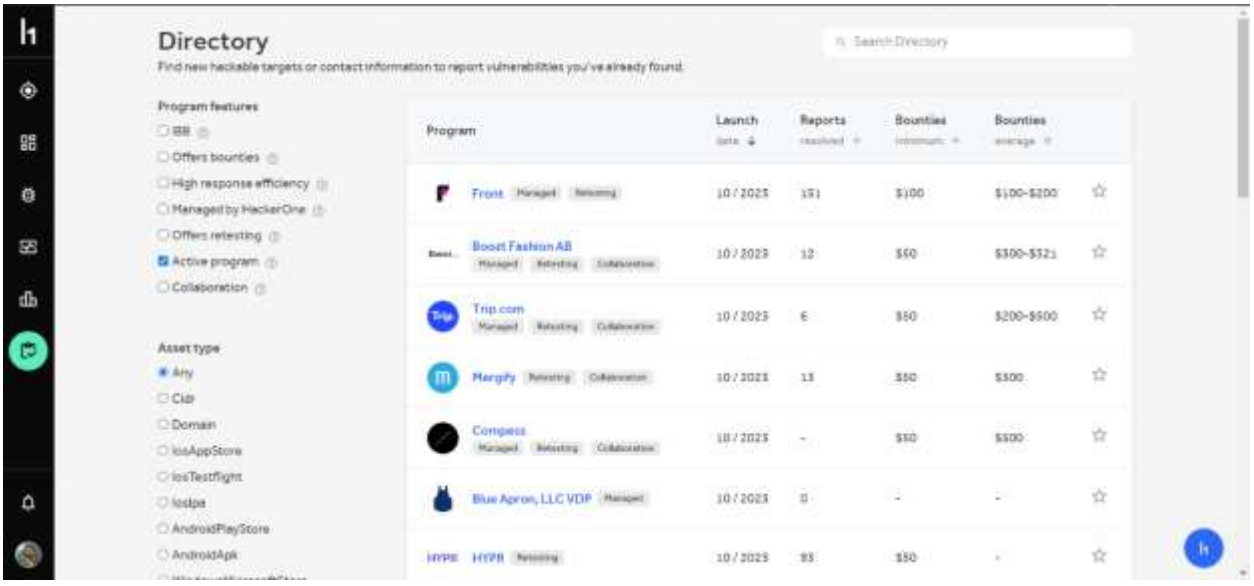



Fig.1. https://hackerone.com/

# Introduction

Web security is critical to web based companies and businesses because cybercrime is increasing day by day. Every moment attackers are finding new paths for exploiting the web applications. And attackers develop their skills not only for fun they focus on money also. That is why ransomware attacks are most popular these days. Because of that protection is a must for web applications to defend against this type of cybercrime.

So, a lot of web based companies and businesses are assigned to Bug Bounty programs to detect the vulnerabilities and fix those vulnerable domains before getting into attack.Hackerone (https://www.hackerone.com/)is one of the platforms that help web-based companies to fix vulnerabilities through Bug Bounty programs. And Hackerone platform and web based companies are paying for penetration testing their web domains. So, I selected a web based company called Trip.com (http://trip.com/) for my Bug Bounty hunting program (Fig. 2). Trip.com platform is used by customers to create their websites (Fig. 3). This includes the ability to add custom JavaScript code to their website. And Trip.com offers a large number of subdomains to this Bug Bounty hunting program and also the little number of reports submitted because they did not pay for those reports and the service.

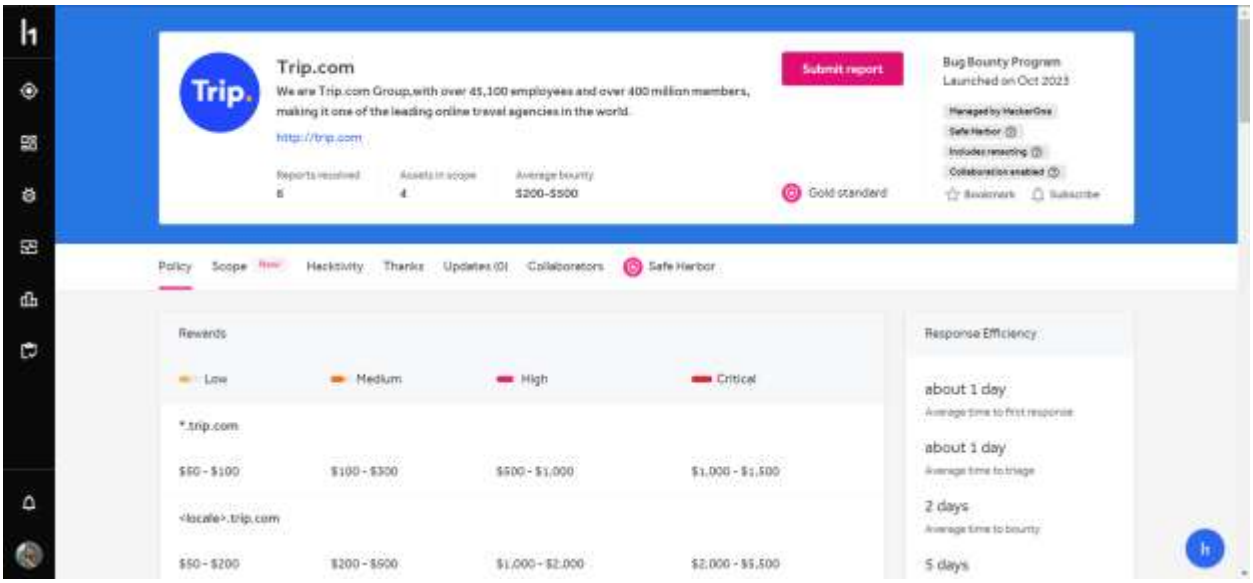



Fig.2. Trip.com ’s Hackerone page


Fig.3. http://trip.com/

This Bug Bounty Assignment is used to be done according to the following web application security testing methodology (Fig. 4).


Fig.4. web application security testing methodology

Before moving into the information gathering stage, we need to consider the top 10 web application's Security Risks and vulnerabilities in 2023. Because we can get an excellent idea for success in our information gathering stage. According to the Sucuri Guides, The Open Web Application Security Project (OWASP) is an online community that creates web application security papers, techniques, documentation, tools, and technologies. The OWASP Top 10 is a list of the top ten most frequent application Security Risks and vulnerabilities [1]

- Injection
- Broken authentication
- Sensitive data exposure
- XML external entities (XXE)
- Broken access control
- Security misconfigurations
- Cross-site scripting (XSS)
- Insecure deserialization
- Using components with known vulnerabilities
- Insufficient logging and monitoring

So, these are the top 10 vulnerabilities found by the OWASP in 2023. We need to focus on these types of vulnerabilities according to the scope and rules provided by Jimdo web-based company and the Hackerone platform.

# Information Gathering

Information gathering is the first step to building a strong foundation for this Bug Bounty hunting program. Because this step is about collecting the critical details of the targeted web application. If this step is not done well entire project can be a useless effort. So, more information means that we can capture more vulnerabilities from targeted domains. As an example, we have to find the targeted domain's IP addresses, details about open ports in the targeted domain, and what type of protection they use to protect their web application. According to the All About Testing (AAT), “The more useful information you have about a target, the more you can find vulnerabilities in the target and find more serious problems in the target by exploiting them.” [2]. So, perfect information gathering is key to unlocking vulnerabilities from the target and it will help improve our vulnerability scanning process.

Information Gathering can be divided into two parts. They are,

1. Passive information gathering
    - Passive information gathering is collecting information from the targeted domain without invoking any kind of communication with the target systems.

2. Active information gathering
    - Active information gathering is collecting information from the targeted domain involves monitoring the target systems by building communication with the target. This method is detectable to the targeted system.

Considering the Passive and Active information gathering, there are many tools to gather information from the target domain using both methods. They are,

1) Passive information gathering tools
    - sublist3r
    - nslookup
    - whois
    - whatweb
    - dig
    - Netcraft (https://sitereport.netcraft.com/)
    - Whois Lookup (https://whois.domaintools.com/)

2) Active information gathering tools
    - Nmap
    - Dmitry

These are the information-gathering tools used to analyze the targeted web domain. And I give priority to Passive information gathering tools. Because Active information gathering is very noisy. But we need active information gathering to analyze information about what is open ports are in our targeted system.

# 1.Passive information gathering tools

- ## Sublist3r

Sublist3r is a subdomain enumeration tool. That means this is a tool to identify the unique subdomains associated with the target domain. Because of this tool, we can gather more information about subdomains. This tool is not built-in and comes with Kali Linux operating system and first, we need to install this tool in the Kali Linux operating system.

- Download the Sublist3r [3].

```
┌──(malith㉿kali)-[~/Documents/Tools]
└─$ 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
Receiving objects: 100% (383/383), 1.12 MiB | 1.34 MiB/s, done.
Resolving deltas: 100% (213/213), done.
```

Fig. 5. Download the Sublist3r using github link

- Check the downloaded location and go into the Sublist3r directory.

```
┌──(malith㉿kali)-[~/Documents/Tools]
└─$ ls
Sublist3r

┌──(malith㉿kali)-[~/Documents/Tools]
└─$ cd Sublist3r

┌──(malith㉿kali)-[~/Documents/Tools/Sublist3r]
└─$ ls
LICENSE  MANIFEST.in  README.md  requirements.txt  setup.py  subbrute  sublist3r.py
```

Fig. 6. Go into Sublist3r directory

- Install Python3-pip in Kali Linux.

```
┌──(malith㉿kali)-[~/Documents/Tools/Sublist3r]
└─$ sudo apt install python3-pip
[sudo] password for malith:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pip-whl
The following packages will be upgraded:
  python3-pip python3-pip-whl
2 upgraded, 0 newly installed, 0 to remove and 1045 not upgraded.
Need to get 3118 kB of archives.
After this operation, 61.4 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 python3-pip all 23.3+dfsg-1 [1346 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 python3-pip-whl all 23.3+dfsg-1 [1772 kB]
Fetched 3118 kB in 8s (394 kB/s)
(Reading database ... 395558 files and directories currently installed.)
Preparing to unpack .../python3-pip_23.3+dfsg-1_all.deb ...
Unpacking python3-pip (23.3+dfsg-1) over (23.2+dfsg-1) ...
Preparing to unpack .../python3-pip-whl_23.3+dfsg-1_all.deb ...
Unpacking python3-pip-whl (23.3+dfsg-1) over (23.2+dfsg-1) ...
Setting up python3-pip-whl (23.3+dfsg-1) ...
Setting up python3-pip (23.3+dfsg-1) ...
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...
```

Fig. 7. Install Python3-pip

- Install Dependencies in the Sublist3r directory.

```
┌──(malith㉿kali)-[~/Documents/Tools/Sublist3r]
└─$ sudo pip install -r requirements.txt
Collecting argparse (from -r requirements.txt (line 1))
  Downloading argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (2.4.1)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (2.31.0)
Installing collected packages: argparse
Successfully installed argparse-1.4.0
```

Fig. 8. Install Dependencies

- Install argparse module in the Sublist3r directory.

```
┌──(malith㉿kali)-[~/Documents/Tools/Sublist3r]
└─$ sudo apt-get install python-argparse
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'libpython2.7-stdlib' instead of 'python-argparse'
libpython2.7-stdlib is already the newest version (2.7.18-13.2).
libpython2.7-stdlib set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1045 not upgraded.
```

Fig. 9.

Install argparse module

- Check Sublist3r is ready to use and test the tool.

```
┌──(malith㉿kali)-[~/Documents/Tools/Sublist3r]
└─$ ls
LICENSE      README.md         setup.py  sublist3r.py
MANIFEST.in  requirements.txt  subbrute

┌──(malith㉿kali)-[~/Documents/Tools/Sublist3r]
└─$ python3 sublist3r.py -d trip.com
```

Fig. 10. Checking the tool

After installing Sublist3r next step is to do scan the main domain to capture subdomains in the targeted system (trip.com).

```
┌──(malith㉿kali)-[~/Documents/Tools/Sublist3r]
└─$ python3 sublist3r.py -d trip.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for trip.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..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 173
awesome--trip.com
www.awesome--trip.com
c-ctrip.com
dimg01.c-ctrip.com
dimg02.c-ctrip.com
dimg03.c-ctrip.com
dimg04.c-ctrip.com
dimg05.c-ctrip.com
dimg06.c-ctrip.com
dimg07.c-ctrip.com
dimg08.c-ctrip.com
dimg09.c-ctrip.com
dimg10.c-ctrip.com
dimg11.c-ctrip.com
dimg12.c-ctrip.com
dimg13.c-ctrip.com
dimg14.c-ctrip.com
dimg15.c-ctrip.com
dimg16.c-ctrip.com
```

Fig. 11. Sublist3r scan result

After the scan, the Sublist3r tool found 173 unique subdomains related to the main domain (trip.com).

## Nslookup

Nslookup is perfect DNS enumeration. That means this is a tool for gathering information about the Domain Name System (DNS) of the targeted system. Nslookup tool help to find out the information related to DNS record names, IP addresses of a target, DNS domain names, and the MX records for the domain or the NS servers of the domain. This tool is already built in the Kali Linux environment. So, I gather the information that all selected domains to get a better understanding of DNS information related to the web application (trip.com).

- Gather information about the IP address of the hostname.

```
┌──(malith㉿kali)-[~/Documents/WSTools]
└─$ sudo su
┌──(root㉿kali)-[/home/malith/Documents/WSTools]
└─# nslookup trip.com
Server:         172.20.10.1
Address:        172.20.10.1#53

Non-authoritative answer:
Name:   trip.com
Address: 103.143.160.200
Name:   trip.com
Address: 103.158.15.28
```

Fig. 12. IP address of the hostname (trip.com)

- Gather information about the mail exchange (MX) records.

```
┌──(root㉿kali)-[/home/malith/Documents/WSTools]
└─# nslookup -query=mx trip.com
Server:         172.20.10.1
Address:        172.20.10.1#53

Non-authoritative answer:
trip.com        mail exchanger = 10 mx2.trip.com.ctripgslb.com.
trip.com        mail exchanger = 50 mx3.trip.com.ctripgslb.com.
trip.com        mail exchanger = 10 mx1.trip.com.ctripgslb.com.

Authoritative answers can be found from:
```

Fig. 13. MX records (-query=mx) of the trip.com

- Gather information about the nameserver (NS) records.

```
┌──(root㉿kali)-[/home/malith/Documents/WSTools]
└─# nslookup -query=ns trip.com
Server:         172.20.10.1
Address:        172.20.10.1#53

Non-authoritative answer:
trip.com        nameserver = a16-67.akam.net.
trip.com        nameserver = a11-65.akam.net.
trip.com        nameserver = a1-244.akam.net.
trip.com        nameserver = a26-64.akam.net.
trip.com        nameserver = a14-66.akam.net.
trip.com        nameserver = a9-65.akam.net.

Authoritative answers can be found from:
```

Fig. 14. NS records (-query=ns) of the trip.com

- Gather information about the “start of authority” (SOA) records. That means we can get details about the domain or region, like the administrator's email address, how long the server should wait between refreshes, and the very last time the domain was modified.

```
┌──(root㉿kali)-[/home/malith/Documents/WSTools]
└─# nslookup -query=soa trip.com
Server:         172.20.10.1
Address:        172.20.10.1#53

Non-authoritative answer:
trip.com
        origin = a9-65.akam.net
        mail addr = hostmaster.trip.com
        serial = 2019126712
        refresh = 60
        retry = 300
        expire = 604800
        minimum = 900

Authoritative answers can be found from:
```

Fig. 15. OSA records (-query=OSA) of the trip.com

- “Any” keyword can use gather all the above information using only one command. So, I use that command to gather information on the in-scope domains.

```
┌──(root㉿kali)-[/home/malith/Documents/WSTools]
└─# nslookup -query=any trip.com
Server:         172.20.10.1
Address:        172.20.10.1#53

Non-authoritative answer:
Name:   trip.com
Address: 103.143.160.200
Name:   trip.com
Address: 103.158.15.28
trip.com        mail exchanger = 10 mx2.trip.com.ctripgslb.com.
trip.com        mail exchanger = 50 mx3.trip.com.ctripgslb.com.
trip.com        mail exchanger = 10 mx1.trip.com.ctripgslb.com.
trip.com        nameserver = a16-67.akam.net.
trip.com        nameserver = a11-65.akam.net.
trip.com        nameserver = a1-244.akam.net.
trip.com        nameserver = a26-64.akam.net.
trip.com        nameserver = a14-66.akam.net.
trip.com        nameserver = a9-65.akam.net.
trip.com
        origin = a9-65.akam.net
        mail addr = hostmaster.trip.com
        serial = 2019126712
        refresh = 60
        retry = 300
        expire = 604800
        minimum = 900
trip.com
        origin = a9-65.akam.net
        mail addr = hostmaster.trip.com
        serial = 2019126712
        refresh = 60
        retry = 300
        expire = 604800
        minimum = 900
Name:   trip.com
Address: 103.143.160.200
Name:   trip.com
Address: 103.158.15.28
```

```
trip.com        mail exchanger = 10 mx2.trip.com.ctripgslb.com.
trip.com        mail exchanger = 50 mx3.trip.com.ctripgslb.com.
trip.com        mail exchanger = 10 mx1.trip.com.ctripgslb.com.
trip.com        nameserver = a16-67.akam.net.
trip.com        nameserver = a11-65.akam.net.
trip.com        nameserver = a1-244.akam.net.
trip.com        nameserver = a26-64.akam.net.
trip.com        nameserver = a14-66.akam.net.
trip.com        nameserver = a9-65.akam.net.
trip.com
        origin = a9-65.akam.net
        mail addr = hostmaster.trip.com
        serial = 2019126712
        refresh = 60
        retry = 300
        expire = 604800
        minimum = 900
trip.com
        origin = a9-65.akam.net
        mail addr = hostmaster.trip.com
        serial = 2019126712
        refresh = 60
        retry = 300
        expire = 604800
        minimum = 900
Name:   trip.com
Address: 103.143.160.200
Name:   trip.com
Address: 103.158.15.28
trip.com        mail exchanger = 10 mx2.trip.com.ctripgslb.com.
trip.com        mail exchanger = 50 mx3.trip.com.ctripgslb.com.
trip.com        mail exchanger = 10 mx1.trip.com.ctripgslb.com.
trip.com        nameserver = a16-67.akam.net.
trip.com        nameserver = a11-65.akam.net.
trip.com        nameserver = a1-244.akam.net.
trip.com        nameserver = a26-64.akam.net.

Authoritative answers can be found from:
trip.com        nameserver = a9-65.akam.net.
trip.com
        origin = a9-65.akam.net
        mail addr = hostmaster.trip.com
        serial = 2019126712
        refresh = 60
        retry = 300
        expire = 604800
        minimum = 900
trip.com
        origin = a9-65.akam.net
        mail addr = hostmaster.trip.com
        serial = 2019126712
        refresh = 60
        retry = 300
        expire = 604800
        minimum = 900
```

Fig. 16. Gather all information using “-query=any” examples

- ## Whois

Whois command gathers information related to targeted domain unknown and distant hosts, server information, network details, and many more details. This command also has a lot of filtering options and uses that “whois --help” command to grant filtering techniques (Fig. 17.).

```
┌──(malith㉿kali)-[~]
└─$ sudo su
[sudo] password for malith:
┌──(root㉿kali)-[/home/malith]
└─# whois --help
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST   connect to server HOST
-p PORT, --port PORT   connect to PORT
-I                     query whois.iana.org and follow its referral
-H                     hide legal disclaimers
      --verbose        explain what is being done
      --no-recursion   disable recursion from registry to registrar servers
      --help           display this help and exit
      --version        output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                     find the one level less specific match
-L                     find all levels less specific matches
-m                     find all one level more specific matches
-M                     find all levels of more specific matches
-c                     find the smallest match containing a mnt-irt attribute
-x                     exact match
-b                     return brief IP address ranges with abuse contact
-B                     turn off object filtering (show email addresses)
-G                     turn off grouping of associated objects
-d                     return DNS reverse delegation objects too
-i ATTR[,ATTR]...      do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...      only look for objects of TYPE
-K                     only primary keys are returned
-r                     turn off recursive look-ups for contact information
-R                     force to show local copy of the domain object even
                       if it contains referral
-a                     also search all the mirrored databases
-s SOURCE[,SOURCE]...  search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST   find updates from SOURCE from serial FIRST to LAST
-t TYPE                request template for object of TYPE
-v TYPE                request verbose template for object of TYPE
-q [version|sources|types]  query specified server info
```

Fig. 17. Whois --help

I did not want to filter the output because I need a full detailed report for my information gathering process. So, these are the sample output of this command (Fig. 18.).

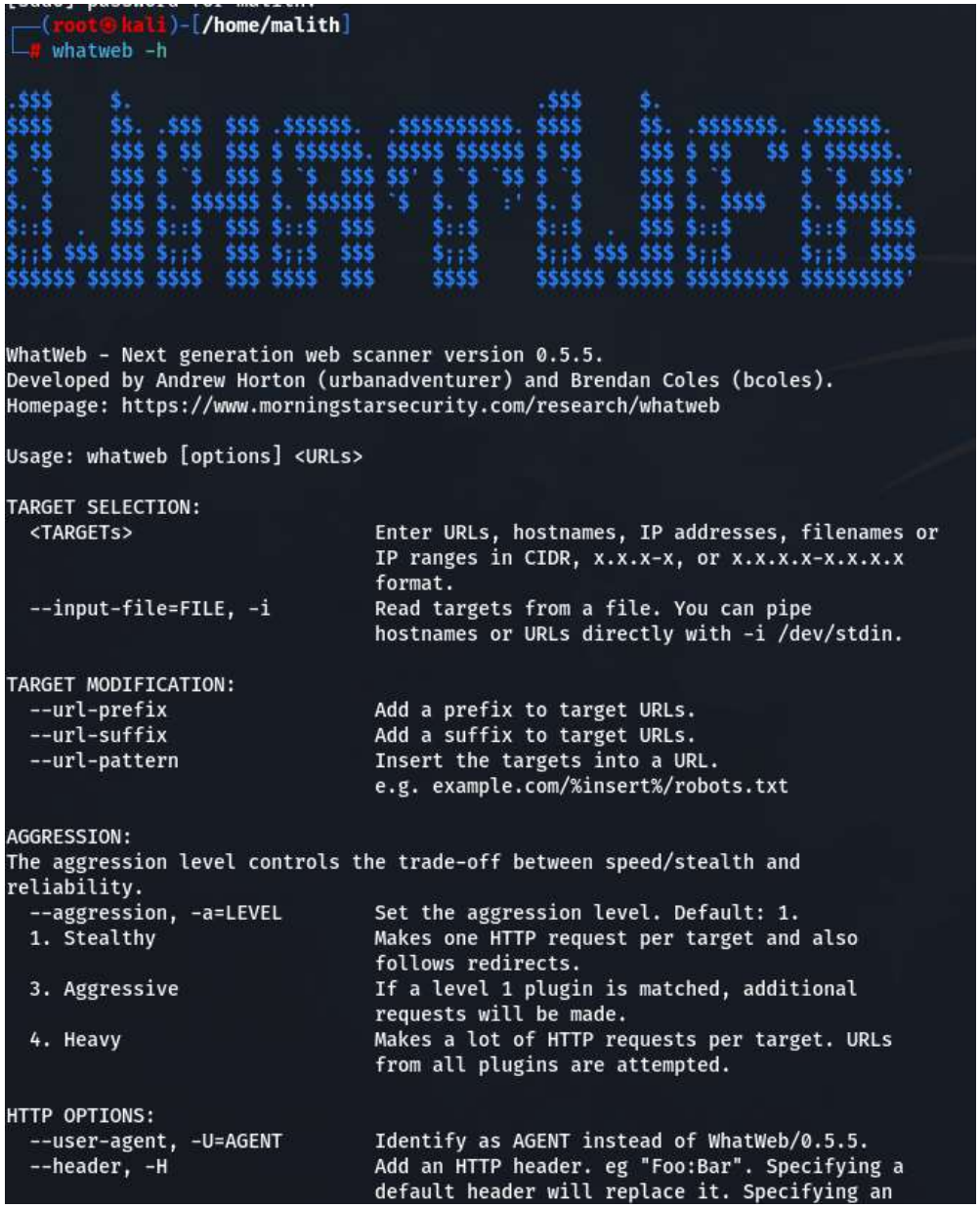
```
┌──(malith㉿kali)-[~]
└─$ whois trip.com
   Domain Name: TRIP.COM
   Registry Domain ID: 3445521_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-06-13T03:46:10Z
   Creation Date: 1998-02-09T05:00:00Z
   Registry Expiry Date: 2027-12-19T05:18:17Z
   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
   Name Server: A1-244.AKAM.NET
   Name Server: A11-65.AKAM.NET
   Name Server: A14-66.AKAM.NET
   Name Server: A16-67.AKAM.NET
   Name Server: A26-64.AKAM.NET
   Name Server: A9-65.AKAM.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: trip.com
Registry Domain ID: 3445521_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2020-02-26T07:29:42+0000
Creation Date: 1998-02-09T05:00:00+0000
Registrar Registration Expiration Date: 2027-12-19T05:18:17+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Registrant Organization: Trip.com Travel Singapore Pte. Ltd.
Registrant State/Province: Singapore
Registrant Country: SG
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/trip.com
Admin Organization: Trip.com Travel Singapore Pte. Ltd.
Admin State/Province: Singapore
Admin Country: SG
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/trip.com
Tech Organization: Trip.com Travel Singapore Pte. Ltd.
Tech State/Province: Singapore
Tech Country: SG
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/trip.com
Name Server: a26-64.akam.net
Name Server: a9-65.akam.net
Name Server: a14-66.akam.net
Name Server: a11-65.akam.net
Name Server: a1-244.akam.net
Name Server: a16-67.akam.net
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-10-31T10:23:50+0000 <<<
```

Fig. 18.

Whois Jimdo.com

- ## Whatweb

According to Kali Linux, “WhatWeb identifies websites. It recognizes web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices.” [4]. This tool is very powerful because we can capture a lot of details using this Whatweb tool. Specially, we can gather information about what type of protection mechanism is used that the targeted domain to protect their web application. But the output information is not sorted well. So, we can use filtering options to gather information in a sorted way.



```
┌──(root㉿kali)-[/home/malith]
└─# whatweb -h

WhatWeb - Next generation web scanner version 0.5.5.
Developed by Andrew Horton (urbanadventurer) and Brendan Coles (bcoles).
Homepage: https://www.morningstarsecurity.com/research/whatweb

Usage: whatweb [options] <URLs>

TARGET SELECTION:
  <TARGETs>                    Enter URLs, hostnames, IP addresses, filenames or
                               IP ranges in CIDR, x.x.x-x, or x.x.x.x-x.x.x.x
                               format.
  --input-file=FILE, -i        Read targets from a file. You can pipe
                               hostnames or URLs directly with -i /dev/stdin.

TARGET MODIFICATION:
  --url-prefix                 Add a prefix to target URLs.
  --url-suffix                 Add a suffix to target URLs.
  --url-pattern                Insert the targets into a URL.
                               e.g. example.com/%insert%/robots.txt

AGGRESSION:
The aggression level controls the trade-off between speed/stealth and
reliability.
  --aggression, -a=LEVEL       Set the aggression level. Default: 1.
  1. Stealthy                  Makes one HTTP request per target and also
                               follows redirects.
  3. Aggressive                If a level 1 plugin is matched, additional
                               requests will be made.
  4. Heavy                     Makes a lot of HTTP requests per target. URLs
                               from all plugins are attempted.

HTTP OPTIONS:
  --user-agent, -U=AGENT       Identify as AGENT instead of WhatWeb/0.5.5.
  --header, -H                 Add an HTTP header. eg "Foo:Bar". Specifying a
                               default header will replace it. Specifying an
```

Fig. 19. whatweb -h

But I did not filter the output because I need informative result about what kind of protection method that the targeted domain use to protect their web application and the filtering is a time-consuming process.

- Gather information related to www.trip.com

```
┌──(root㉿kali)-[/home/malith]
└─# whatweb www.trip.com
http://www.trip.com [301 Moved Permanently] Akamai-Global-Host, Country[UNITED STATES][US], HTTPServer[AkamaiGHost], IP[23.209.46.142], RedirectLocation[https://www.trip.com/]
https://www.trip.com/ [200 OK] Cookies[UBT_VID,_abtest_userid,cookiePricesDisplayed,ibu_online_home_language_match,ibulanguage,ibulocale,kafka_result], Country[UNITED STATES][US], Email[
], IP[23.209.46.142], Open-Graph-Protocol[website], Script[application/ld+json], Title[Trip.com Official Site | Travel Deals and Promotions], UncommonHeaders[x-content-type-opti
trip-app-version,x-trip-app-idc,x-trip-region,content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=edge], X-XSS-Protection[1; mode=block], nginx[1.20.1]
```

Fig. 20. whatweb www.trip.com

- Gather information related to vcc.trip.com

```
┌──(root㉿kali)-[/home/malith]
└─# whatweb vcc.trip.com

http://vcc.trip.com [404 Not Found] Country[UNITED STATES][US], HTML5, HTTPServer[nginx/1.20.1], IP[23.209.46.138], Script[text/javascript>!function(n,r,a,e,t){function], Tit
```

Fig. 21. whatweb vcc.trip.com

- Gather information related to vn.trip.com

```
┌──(root㉿kali)-[/home/malith]
└─# whatweb vn.trip.com
http://vn.trip.com [301 Moved Permanently] Akamai-Global-Host, Country[UNITED STATES][US], HTTPServer[AkamaiGHost], IP[23.209.46.160], RedirectLocation[https://vn.trip.com/]
https://vn.trip.com/ [200 OK] Cookies[UBT_VID,_abtest_userid,cookiePricesDisplayed,ibu_online_home_language_match,ibulanguage,ibulocale,kafka_result], Country[UNITED STATES][US],
], IP[23.209.46.160], Open-Graph-Protocol[website], Script[application/ld+json], Title[Trip.com | Đặt Vé Máy Bay Giá Rẻ, Khách Sạn Và Vé Tàu], UncommonHeaders[x-content-ty
trip-app-version,x-trip-app-idc,x-trip-region,content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=edge], X-XSS-Protection[1; mode=block], nginx[1
```

Fig. 22. whatweb vn.trip.com

- Gather information related to tc.trip.com

```
┌──(root㉿kali)-[/home/malith]
└─# whatweb tc.trip.com
http://tc.trip.com [301 Moved Permanently] IP[103.158.15.28], RedirectLocation[https://tw.trip.com/], Title[301 Moved Permanently]
https://tw.trip.com/ [200 OK] Cookies[UBT_VID,_abtest_userid,cookiePricesDisplayed,ibu_online_home_language_match,ibulanguage,ibulocale,kafka_result], Country[UNITED STATES][US], Emai
], IP[23.52.40.121], Open-Graph-Protocol[website], Script[application/ld+json], Title[Trip.com | 往來動店預訂，機票優惠，旅遊資訊], UncommonHeaders[x-content-type-options,x-dow
sion,x-trip-app-idc,x-trip-region,content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=edge], X-XSS-Protection[1; mode=block], nginx[1.20.1]
```

Fig. 23. whatweb tc.trip.com

- Gather information related to sin-im3.trip.com

```
┌──(root㉿kali)-[/home/malith]
└─# whatweb sin-im3.trip.com
http://sin-im3.trip.com/ [200 OK] Country[UNITED STATES][US], IP[54.179.124.5]
```

Fig. 24. whatweb sin-im3.trip.com

- Gather information related to investors.trip.com

```
┌──(root㉿kali)-[/home/malith]
└─# whatweb investors.trip.com

http://investors.trip.com [403 Forbidden] Country[UNITED STATES][US], IP[23.209.46.142], Title[Access Denied], UncommonHeaders[x-reference-error]
```

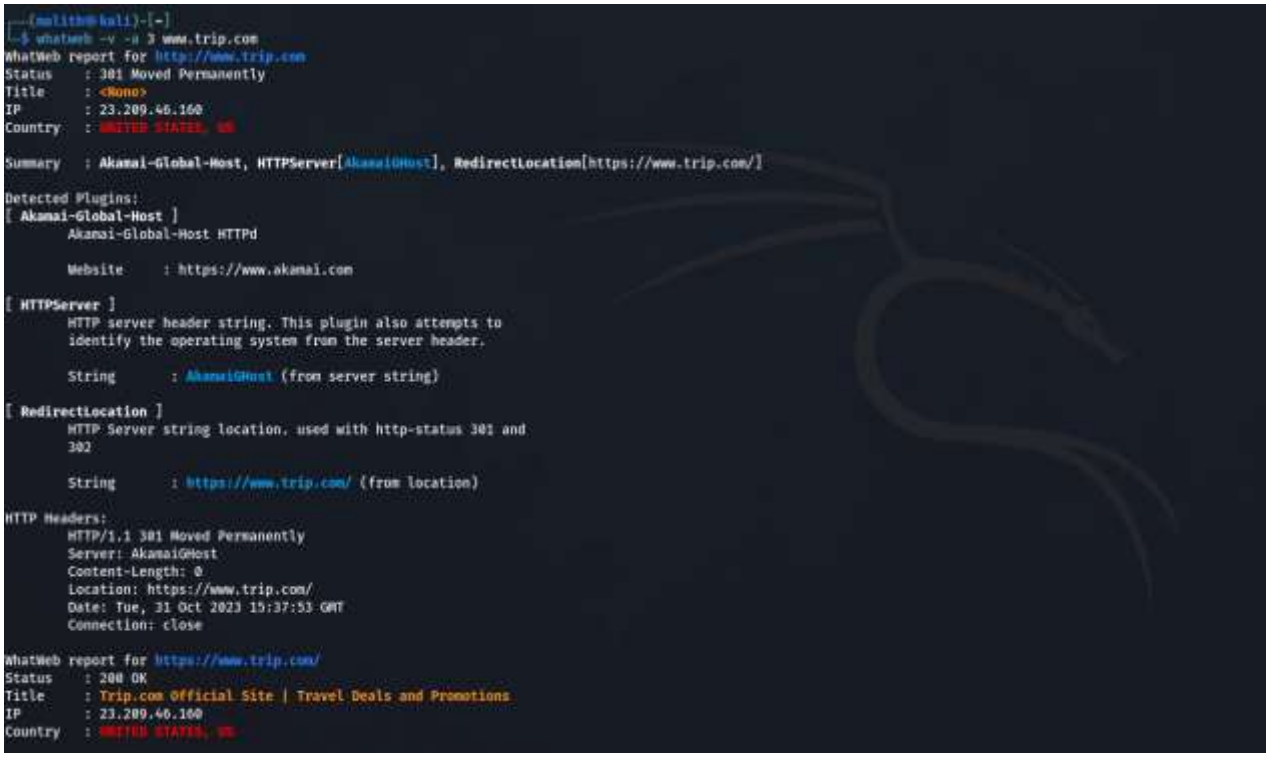
Fig. 25. Whatweb investors.trip.com

- Other gathered targeted subdomains.


Fig. 26. Other targeted domains

- Gather information about www.trip.com in a sorted way with filtering methods.

  - ✓ Scan www.trip.com with verbose plugin descriptions (./whatweb -v www.trip.com) [4].
  - ✓ An aggressive scan of www.trip.com detects the exact version of WordPress (./whatweb -a 3 www.trip.com) [4].



```
Summary   : Cookies[UBT_VID,_abtest_userid,cookiePricesDisplayed,ibu_online_home_language_match,ibulanguage,ibulocale,kafka_result], Email[googledesign@2x.jpeg]
[495475], Script[application/ld+json], UncommonHeaders[x-content-type-options,x-download-options,x-readtime,x-trip-app-name,x-trip-app-version,x-trip-app-idc,x-
 X-UA-Compatible[IE=edge], X-XSS-Protection[1; mode=block]

Detected Plugins:
[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : UBT_VID
        String       : kafka_result
        String       : ibu_online_home_language_match
        String       : ibulanguage
        String       : ibulanguage
        String       : ibulocale
        String       : ibulocale
        String       : cookiePricesDisplayed
        String       : cookiePricesDisplayed
        String       : _abtest_userid

[ Email ]
        Extract email addresses. Find valid email address and
        syntactically invalid email addresses from mailto: link
        tags. We match syntactically invalid links containing
        mailto: to catch anti-spam email addresses, eg. bob at
        gmail.com. This uses the simplified email regular
        expression from
        http://www.regular-expressions.info/email.html for valid
        email address matching.

        String       : googledesign@2x.jpeg

[ HTML5 ]
        HTML version 5, detected by the doctype declaration


[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : nginx/1.20.1 (from server string)

[ Open-Graph-Protocol ]
        The Open Graph protocol enables you to integrate your Web
        pages into the social graph. It is currently designed for
        Web pages representing profiles of real-world things .
        things like movies, sports teams, celebrities, and
        restaurants. Including Open Graph tags on your Web page,
        makes your page equivalent to a Facebook Page.

        Module       : [illegible]

[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.

        String       : application/ld+json

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : x-content-type-options,x-download-options,x-readtime,x-trip-app-name,x-trip-app-version,x-trip-app-idc,x-trip-region,content-security-policy

[ X-Frame-Options ]
        This plugin retrieves the X-Frame-Options value from the
        HTTP header. - More Info:
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx

        String       : SAMEORIGIN

[ X-UA-Compatible ]
        This plugin retrieves the X-UA-Compatible value from the
        HTTP header and meta http-equiv tag. - More Info:
        http://msdn.microsoft.com/en-us/library/cc817574.aspx

        String       : IE=edge
```

```
[ X-XSS-Protection ]
        This plugin retrieves the X-XSS-Protection value from the
        HTTP header. - More Info:
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx

        String       : 1; mode=block

[ nginx ]
        Nginx (Engine-X) is a free, open-source, high-performance
        HTTP server and reverse proxy, as well as an IMAP/POP3
        proxy server.

        Version      : 1.20.1
        Website      : http://nginx.net/

HTTP Headers:
        HTTP/1.1 200 OK
        Server: nginx/1.20.1
        Content-Type: text/html; charset=utf-8
        Cache-Control: no-cache, no-store, must-revalidate
        Pragma: no-cache
        Expires: 0
        ETag: W/"10130-zdwz6FakIi7sl0w9aFgfN33/2IQ"
        x-frame-options: SAMEORIGIN
        x-xss-protection: 1; mode=block
        x-content-type-options: nosniff
        x-download-options: noopen
        x-readtime: 136
        x-trip-app-name: online-home
        x-trip-app-version: 2.29.0
        x-trip-app-idc: SIN-AWS
        x-trip-region: sg
        Content-Security-Policy-Report-Only: default-src * data: blob:; connect-src  https://*.tripcdn.com *.c-ctrip.com https://*.trip.com   https://*.ctrip.com https
*.bing.com https://*.mapbox.com https://*.skyscanner.net https://*.tripcdn.cn https://*.google-analytics.com https://*.braze.com https://*.yandex.ru https://*.googleap
gstatic.com https://wcs.naver.com https://wcs.naver.net https://connect.facebook.net https://cdn.2trk.info https://b98.yahoo.co.jp https://widget.trustpilot.com https:
l' 'unsafe-inline' https://*.naver.net https://*.trip.com https://*.tripcdn.com https://*.tripcdn.cn https://*.c-ctrip.com https://*.google.com https://*.doubleclick.n
//unpkg.com https://altopd.com https://*.tiktok.com https://*.facebook.net https://*.bing.com https://*.googleapis.com https://*.yahoo.co.jp https://*.2trk.info https:
er.net https://*.alipayobjects.com https://*.rakuten.com https://*.qunarzz.com https://*.googleadservices.com https://*.yandex.ru https://*.qq.com https://*.ctrip.com
googlesyndication.com https://*.jsdelivr.net https://*.tripcdn.com https://hubloak.com https://*.ying.com https://boxclone.com https://*.hotjar.com https://*.google.ae
t https://*.innity.com https://appx https://*.criteo.com https://*.apaylater.com https://*.maynhtml.com https://*.google.com.my https://*.google.com.hk https://*.mapbo
trip.com https://*.tripcdn.cn https://*.google.com https://*.googleapis.com https://*.fontawesome.com https://*.honey.io https://*.gstatic.com https://*.c-ctrip.com ht
 https://*.invol.co https://*.googlesyndication.com https://*.google.com https://*.trustpilot.com https://*.facebook.com https://*.lcmark.net https://*.ubpixel.com htt
trck.pro https://*.doubleclick.net https://*.kakao.com https://*.dotomi.com https://*.tkqlhce.com https://*.criteo.com https://*.infobip.com https://*.ucweb.com https:
*.trip.com https://altopd.com https://invol.co https://stvkr.com https://redirtrack.tech https://noop.style https://*.admitad.com https://*.kittyswell.one https://*.ke
        Vary: user-agent
        Vary: Accept-Encoding
        Date: Tue, 31 Oct 2023 15:37:55 GMT
        Transfer-Encoding:  chunked
        Connection: close
        Connection: Transfer-Encoding
        Set-Cookie: UBT_VID=1698766675519.12022lxC5uik;domain=.trip.com;path=/;expires=Wed, 04 Dec 2024 15:37:55 GMT
        Set-Cookie: kafka_result={"isDirectVisit":"1","hasUrlLocale":"0","hasCookieLocale":"0","isUrlCookieSame":"0","isJump":"0","jumpType":"targetLocale","platform":"
        Set-Cookie: ibu_online_home_language_match={"isRedirect":false,"isShowSuggestion":false,"lastVisited":true,"region":"lk","redirectSymbol":false,"site_url":[]};
        Set-Cookie: ibulanguage=; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT
        Set-Cookie: ibulanguage=EN; Max-Age=2592000; Domain=trip.com; Path=/
        Set-Cookie: ibulocale=; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT
        Set-Cookie: ibulocale=en_xx; Max-Age=2592000; Domain=trip.com; Path=/
        Set-Cookie: cookiePricesDisplayed=; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT
        Set-Cookie: cookiePricesDisplayed=USD; Max-Age=2592000; Domain=trip.com; Path=/
        Set-Cookie: _abtest_userid=ad80e153-5100-4b6c-93d6-a2fcfa2a0f70; domain=.trip.com; max-age=86400000; path=/; SameSite=None; Secure
```

Fig. 27. whatweb -v -a 3 www.trip.com

Consider the information I gathered, these are my ideas related to targeted domains.

- ✓ X-Frame-Options HTTP Header is in the DENY use only two domains. And those are the login pages of this web application. DENY is about the page must not be embedded into another page within an iframe [5]. So, using a frame to hijack the usernames and passwords using clickjacking attacks is protected.
- ✓ X-Frame-Options HTTP Header is in the SAMEORIGIN used by other web domains including the main domain. SAMEORIGIN is about the website can only be embedded in a site that's paired in terms of scheme, hostname, and port [5].
- ✓ X-XSS-Protection HTTP Header is in the 1; mode=block use by all domains. Using X-Frame-Options HTTP Header to detect the cross-site scripting attack. And using 1; mode=block to enable the filter and completely blocks the page [6].
- ✓ According to fig. 27, this domain uses Nginx to version 1.20.1 as the HTTP server software. This version is older, and it might be vulnerable to exploiting the target domain

So, the Whatweb tool give me a perfect understanding of targeted domains and the above details are the resent why I am mostly focused on this tool.

- ## Dig

Domain Information Groper (dig) is used for gathering information relevant to Domain Name System (DNS). This command is also the same as the nslookup command. But dig command present the information sorted way than the nslookup command.

```
┌──(malith㉿kali)-[~]
└─$ dig www.trip.com

; <<>> DiG 9.18.16-1-Debian <<>> www.trip.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28860
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.trip.com.                  IN      A

;; ANSWER SECTION:
www.trip.com.           868     IN      CNAME   slb-trip-aws.ctripgslb.com.
slb-trip-aws.ctripgslb.com. 205 IN      CNAME   c229846.edgekey.net.
c229846.edgekey.net.    118     IN      CNAME   agoda-dscx.tripgslb.akadns.net.
agoda-dscx.tripgslb.akadns.net. 55 IN   CNAME   e229846.dscx.akamaiedge.net.
e229846.dscx.akamaiedge.net. 15 IN      A       23.209.46.138
e229846.dscx.akamaiedge.net. 15 IN      A       23.209.46.141

;; Query time: 76 msec
;; SERVER: 172.20.10.1#53(172.20.10.1) (UDP)
;; WHEN: Wed Nov 01 10:39:39 +0530 2023
;; MSG SIZE  rcvd: 222
```

Fig. 28. www.trip.com

```
┌──(malith㉿kali)-[~]
└─$ dig vcc.trip.com

; <<>> DiG 9.18.16-1-Debian <<>> vcc.trip.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14456
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;vcc.trip.com.                  IN      A

;; ANSWER SECTION:
vcc.trip.com.           1127    IN      CNAME   slb-trip-aws.ctripgslb.com.
slb-trip-aws.ctripgslb.com. 227 IN      CNAME   c229846.edgekey.net.
c229846.edgekey.net.    139     IN      CNAME   agoda-dscx.tripgslb.akadns.net.
agoda-dscx.tripgslb.akadns.net. 77 IN   CNAME   e229846.dscx.akamaiedge.net.
e229846.dscx.akamaiedge.net. 27 IN      A       23.209.46.138
e229846.dscx.akamaiedge.net. 27 IN      A       23.209.46.141

;; Query time: 272 msec
;; SERVER: 172.20.10.1#53(172.20.10.1) (UDP)
;; WHEN: Wed Nov 01 10:39:23 +0530 2023
;; MSG SIZE  rcvd: 222
```

Fig.29.vcc.trip.com

```
┌──(malith㉿kali)-[~]
└─$ dig vn.trip.com

; <<>> DiG 9.18.16-1-Debian <<>> vn.trip.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9702
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;vn.trip.com.                   IN      A

;; ANSWER SECTION:
vn.trip.com.            1127    IN      CNAME   slb-trip-aws.ctripgslb.com.
slb-trip-aws.ctripgslb.com. 143 IN      CNAME   c229846.edgekey.net.
c229846.edgekey.net.    55      IN      CNAME   agoda-dscx.tripgslb.akadns.net.
agoda-dscx.tripgslb.akadns.net. 77 IN   CNAME   e229846.dscx.akamaiedge.net.
e229846.dscx.akamaiedge.net. 27 IN      A       23.209.46.141
e229846.dscx.akamaiedge.net. 27 IN      A       23.209.46.138

;; Query time: 208 msec
;; SERVER: 172.20.10.1#53(172.20.10.1) (UDP)
;; WHEN: Wed Nov 01 10:40:29 +0530 2023
;; MSG SIZE  rcvd: 221
```

Fig. 30. vn.trip.com

```
┌──(malith㉿kali)-[~]
└─$ dig tc.trip.com

; <<>> DiG 9.18.16-1-Debian <<>> tc.trip.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32386
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;tc.trip.com.                   IN      A

;; ANSWER SECTION:
tc.trip.com.            1127    IN      CNAME   base.trip.com.
base.trip.com.          1127    IN      CNAME   slb-05-xy5-rb5-osonly.ctripgslb.
slb-05-xy5-rb5-osonly.ctripgslb.com. 77 IN A    103.158.15.28
slb-05-xy5-rb5-osonly.ctripgslb.com. 77 IN A    103.143.160.200

;; Query time: 204 msec
;; SERVER: 172.20.10.1#53(172.20.10.1) (UDP)
;; WHEN: Wed Nov 01 10:40:53 +0530 2023
;; MSG SIZE  rcvd: 137
```

Fig. 31. tc.trip.com

```
┌──(malith㉿kali)-[~]
└─$ dig sin-im3.trip.com

; <<>> DiG 9.18.16-1-Debian <<>> sin-im3.trip.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11257
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sin-im3.trip.com.              IN      A

;; ANSWER SECTION:
sin-im3.trip.com.       1127    IN      CNAME   bbz-im-trip-82b54bed7d0ecac2.elb.ap-southeast-1.amazonaws.com.
bbz-im-trip-82b54bed7d0ecac2.elb.ap-southeast-1.amazonaws.com. 77 IN A 18.140.127.116
bbz-im-trip-82b54bed7d0ecac2.elb.ap-southeast-1.amazonaws.com. 77 IN A 54.179.124.5

;; Query time: 120 msec
;; SERVER: 172.20.10.1#53(172.20.10.1) (UDP)
;; WHEN: Wed Nov 01 10:41:19 +0530 2023
;; MSG SIZE  rcvd: 149
```

Fig. 32. Sin-im3.trip.com

```
┌──(malith㉿kali)-[~]
└─$ dig investors.trip.com

; <<>> DiG 9.18.16-1-Debian <<>> investors.trip.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43470
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;investors.trip.com.            IN      A

;; ANSWER SECTION:
investors.trip.com.     1127    IN      CNAME   ctripcominternationalltd.gcs-web.com.
ctripcominternationalltd.gcs-web.com. 377 IN CNAME leapfrog-ssl-21.gcs-web.com.edgekey.net.
leapfrog-ssl-21.gcs-web.com.edgekey.net. 4502 IN CNAME e26203.dsca.akamaiedge.net.
e26203.dsca.akamaiedge.net. 27  IN      A       23.209.46.163
e26203.dsca.akamaiedge.net. 27  IN      A       23.209.46.142

;; Query time: 264 msec
;; SERVER: 172.20.10.1#53(172.20.10.1) (UDP)
;; WHEN: Wed Nov 01 10:41:47 +0530 2023
;; MSG SIZE  rcvd: 216
```

Fig. 33. investors.trip.com

- ## Netcraft

Netcraft (https://sitereport.netcraft.com/) is an online web tool used to gather information related to technologies utilized in web application development. This tool is helping to identify out of date software modules used to develop the web application. These outdated software modules can be vulnerable to exploitation.


Fig. 34. https://sitereport.netcraft.com/

This is the main interface of the Netcraft tool. We have to enter the domain name to get the details from this tool.

- Gather details about the Network and Background of the targeted domain.


Fig. 35. Details about Network and Background

- Gather information regarded to IP Delegation of the targeted domain.

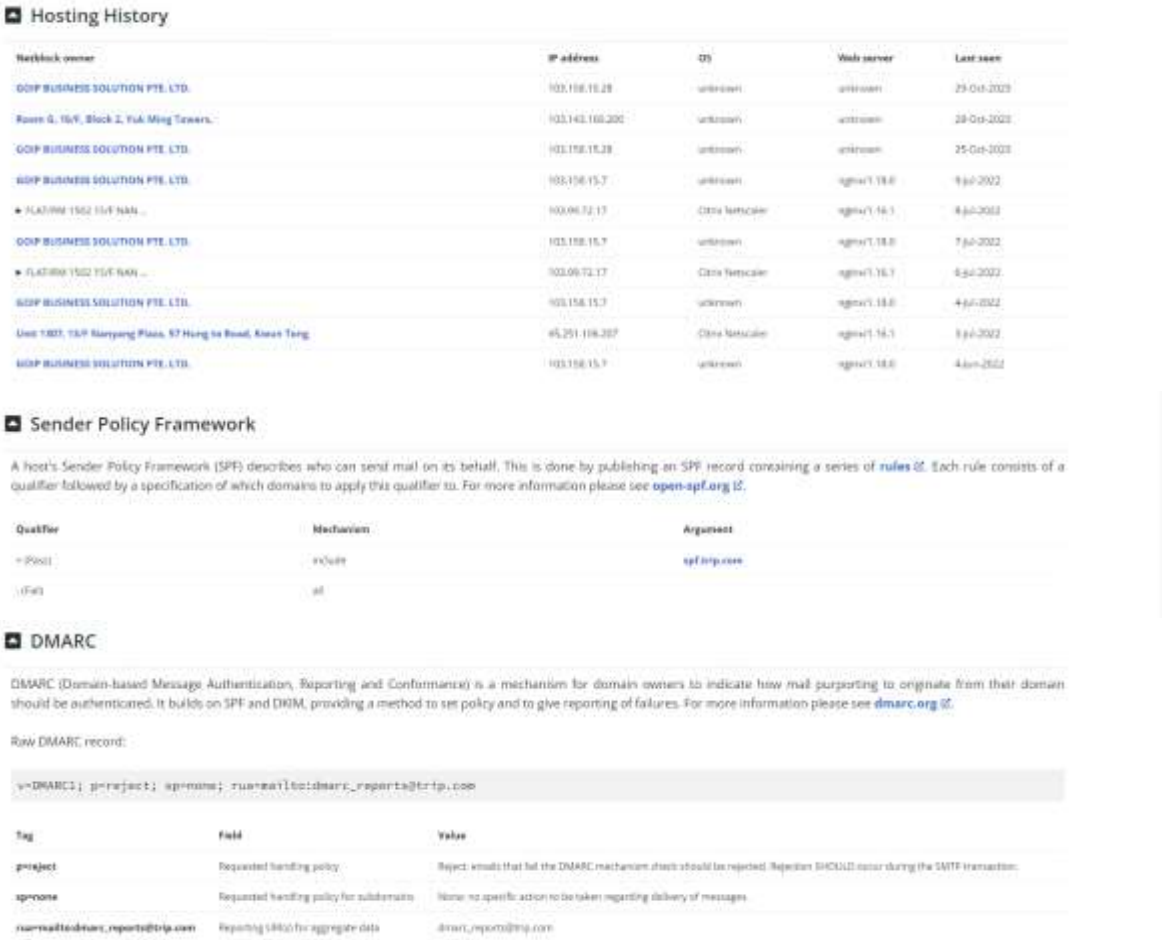
**IP delegation**

**IPv4 address (103.143.160.200)**

| IP range | Country | Name | Description |
|---|---|---|---|
| [illegible] | United States | IANA-IPV4-MAPPED-ADDRESS | Internet Assigned Numbers Authority |
| [illegible] | Australia | APNIC-AP | Asia Pacific Network Information Centre |
| [illegible] | Hong Kong | [illegible] | [illegible] Technology Co., Limited |
| [illegible] | Hong Kong | TWOWINCOLIMITED-HK | Room G, 16/F, Block 2, Yuk Ming Towers, |
| [illegible] | Hong Kong | TWOWINCOLIMITED-HK | Room G, 16/F, Block 2, Yuk Ming Towers, |

Fig. 36. information regarded to IP Delegation

- Gather the information about Hosting History, Sender Policy Framework, and DMARC of the targeted domain. And we can find the same older HTTP server founded using the whatweb command (Nginx version 1.20.1).



**Hosting History**

| Netblock owner | IP address | OS | Web server | Last seen |
|---|---|---|---|---|
| GOIP BUSINESS SOLUTION PTE. LTD. | 103.158.15.28 | unknown | unknown | 29-Oct-2023 |
| Room G, 16/F, Block 2, Yuk Ming Towers, | 103.143.160.200 | unknown | unknown | 28-Oct-2023 |
| GOIP BUSINESS SOLUTION PTE. LTD. | 103.158.15.28 | unknown | unknown | 25-Oct-2023 |
| GOIP BUSINESS SOLUTION PTE. LTD. | 103.158.15.7 | unknown | nginx/1.18.0 | 9-Jul-2022 |
| FLAT/RM 1502 15/F NAN ... | 103.99.72.17 | Citrix Netscaler | nginx/1.16.1 | 8-Jul-2022 |
| GOIP BUSINESS SOLUTION PTE. LTD. | 103.158.15.7 | unknown | nginx/1.18.0 | 7-Jul-2022 |
| FLAT/RM 1502 15/F NAN ... | 103.99.72.17 | Citrix Netscaler | nginx/1.16.1 | 6-Jul-2022 |
| GOIP BUSINESS SOLUTION PTE. LTD. | 103.158.15.7 | unknown | nginx/1.18.0 | 4-Jul-2022 |
| Unit 1807, 15/F Nanyang Plaza, 57 Hung to Road, Kwun Tong | 45.251.106.207 | Citrix Netscaler | nginx/1.16.1 | 3-Jul-2022 |
| GOIP BUSINESS SOLUTION PTE. LTD. | 103.158.15.7 | unknown | nginx/1.18.0 | 4-Jun-2022 |

**Sender Policy Framework**

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see open-spf.org.

| Qualifier | Mechanism | Argument |
|---|---|---|
| +(Pass) | include | spf.trip.com |
| -(Fail) | all | |

**DMARC**

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org.

Raw DMARC record:

```
v=DMARC1; p=reject; sp=none; rua=mailto:dmarc_reports@trip.com
```

| Tag | Field | Value |
|---|---|---|
| p=reject | Requested handling policy | Reject: emails that fail the DMARC mechanism check should be rejected. Rejection SHOULD occur during the SMTP transaction. |
| sp=none | Requested handling policy for subdomains | None: no specific action to be taken regarding delivery of messages |
| rua=mailto:dmarc_reports@trip.com | Reporting URI(s) for aggregate data | dmarc_reports@trip.com |

Fig. 37. Gather the information about Hosting History, Sender Policy Framework, and DMARC

- Gather the information about Site Technology.

netcraft

LEARN MORE | REPORT FRAUD

Site Technology (fetched 16 days ago)

**Server-Side**

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| SSL | A cryptographic protocol providing communication security over the Internet | |

**Client-Side**

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

| Technology | Description | Popular sites using this technology |
|---|---|---|
| JavaScript | Widely-supported programming language commonly used to power client-side dynamic content on websites | www.linkedin.com, www.twitch.com, t.co |

**Client-Side Scripting Frameworks**

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| Google Hosted Libraries | Google API to retrieve JavaScript libraries | www.roblox.com, www.binance.com, www.theguardian.com |

**Web Stats**

Web analytics is the measurement, collection, analysis and reporting of internet data for purposes of understanding and optimizing web usage.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| Google Webmaster Tools | Set of tools allowing webmasters to check indexing status and optimize visibility of their websites on Google | www.amazon.fr, www.ebay.com, www.aliexpress.com |

netcraft

LEARN MORE | REPORT FRAUD

**Character Encoding**

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| UTF8 | UCS Transformation Format 8 bit | |

**HTTP Compression**

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| Gzip Content Encoding | Gzip HTTP Compression protocol | www.amazon.com.br, www.virustotal.com, www.wildberries.ru |

**Web Browser Targeting**

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| X-Content-Type-Options | Browser MIME type sniffing is disabled | www.netflix.com, www.instagram.com, www.amazon.com |
| X-Frame-Options Same Origin | Do not allow this site to be rendered within an iframe | www.tiktok.com, www.reddit.com, www.stampede.com |
| Content Security Policy Report | Report attacks in the browser | www.amazon.in, www.amazon.ca, www.amazon.co.uk |
| X-XSS-Protection Block | Block pages on which cross-site scripting is detected | www.bbc.co.uk, teams.microsoft.com, accounts.google.com |

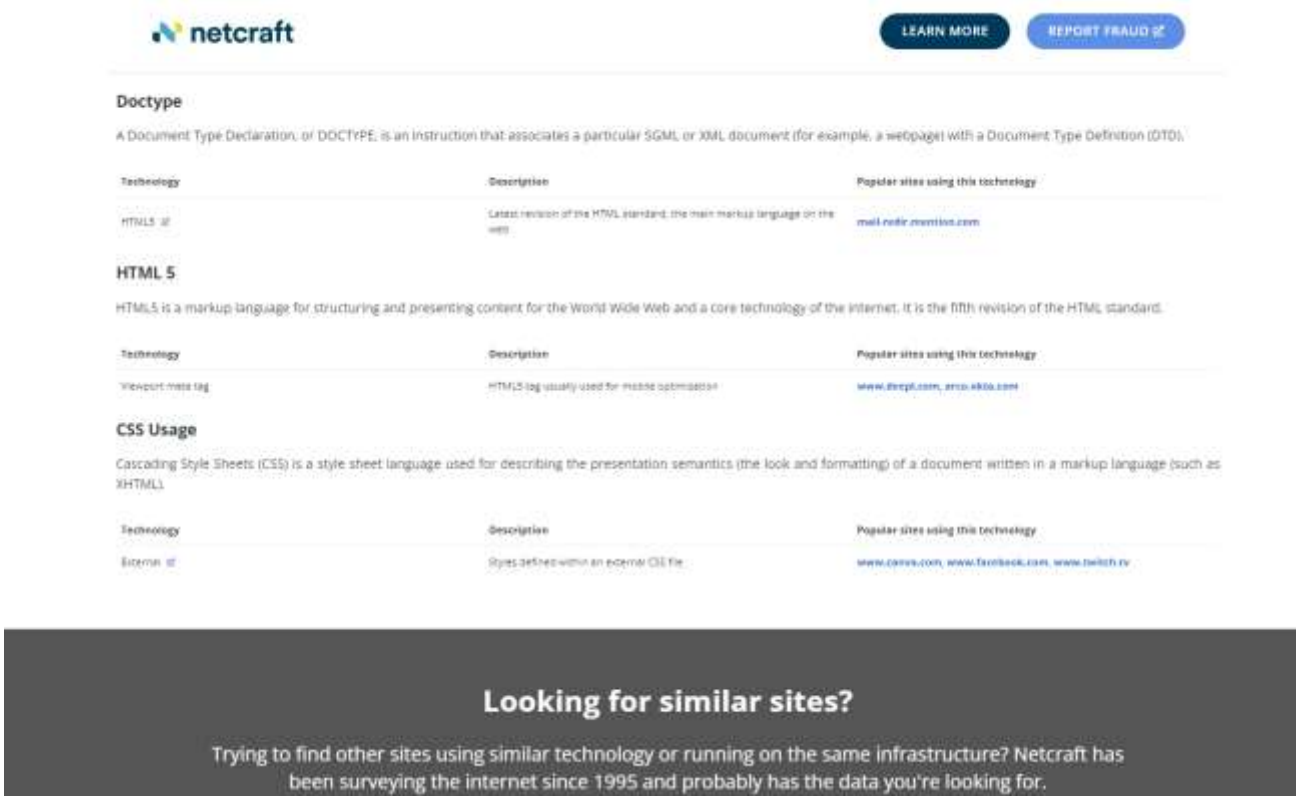


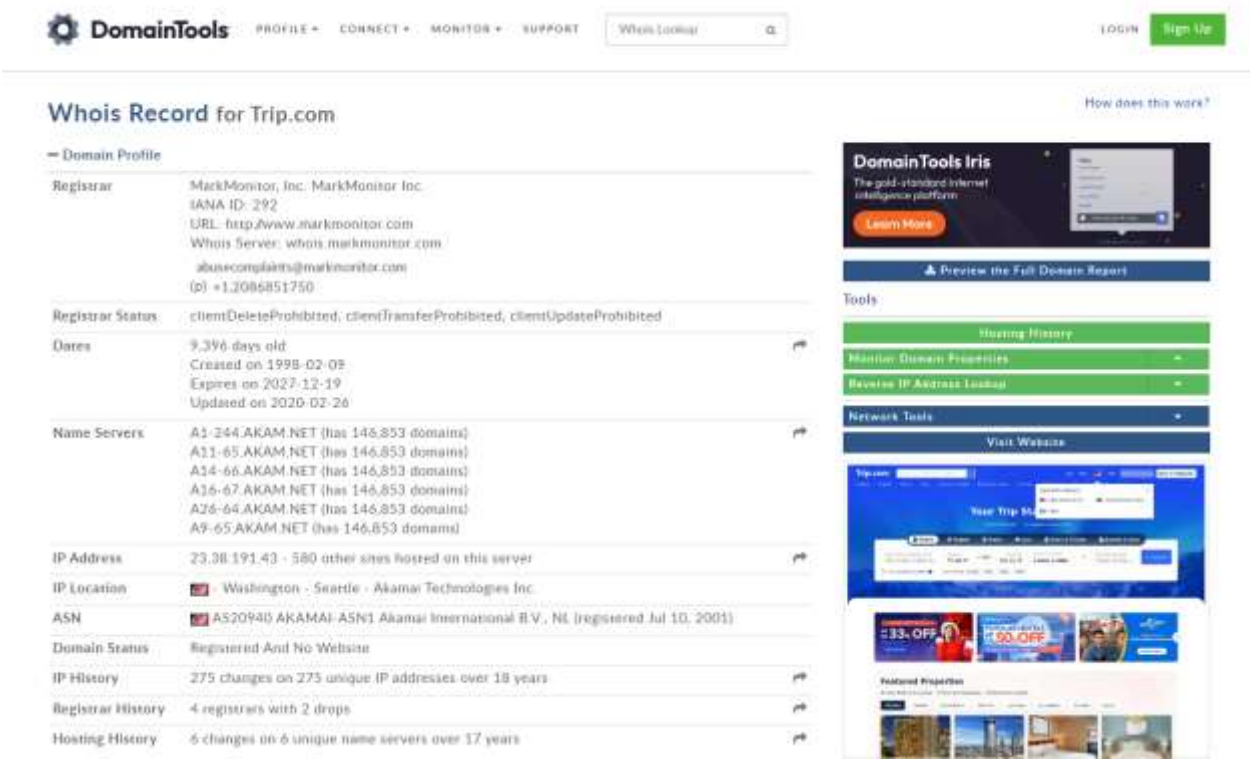
Fig. 38. Information about Site Technology.

## ▪ Whois Lookup

Whois Lookup (https://whois.domaintools.com/) is an online web tool used to gather information about the hosted company, owner of a target, Server Type, and location of servers.

Fig. 39. https://whois.domaintools.com/


- Gather the IP information using the targeted domain IP address.



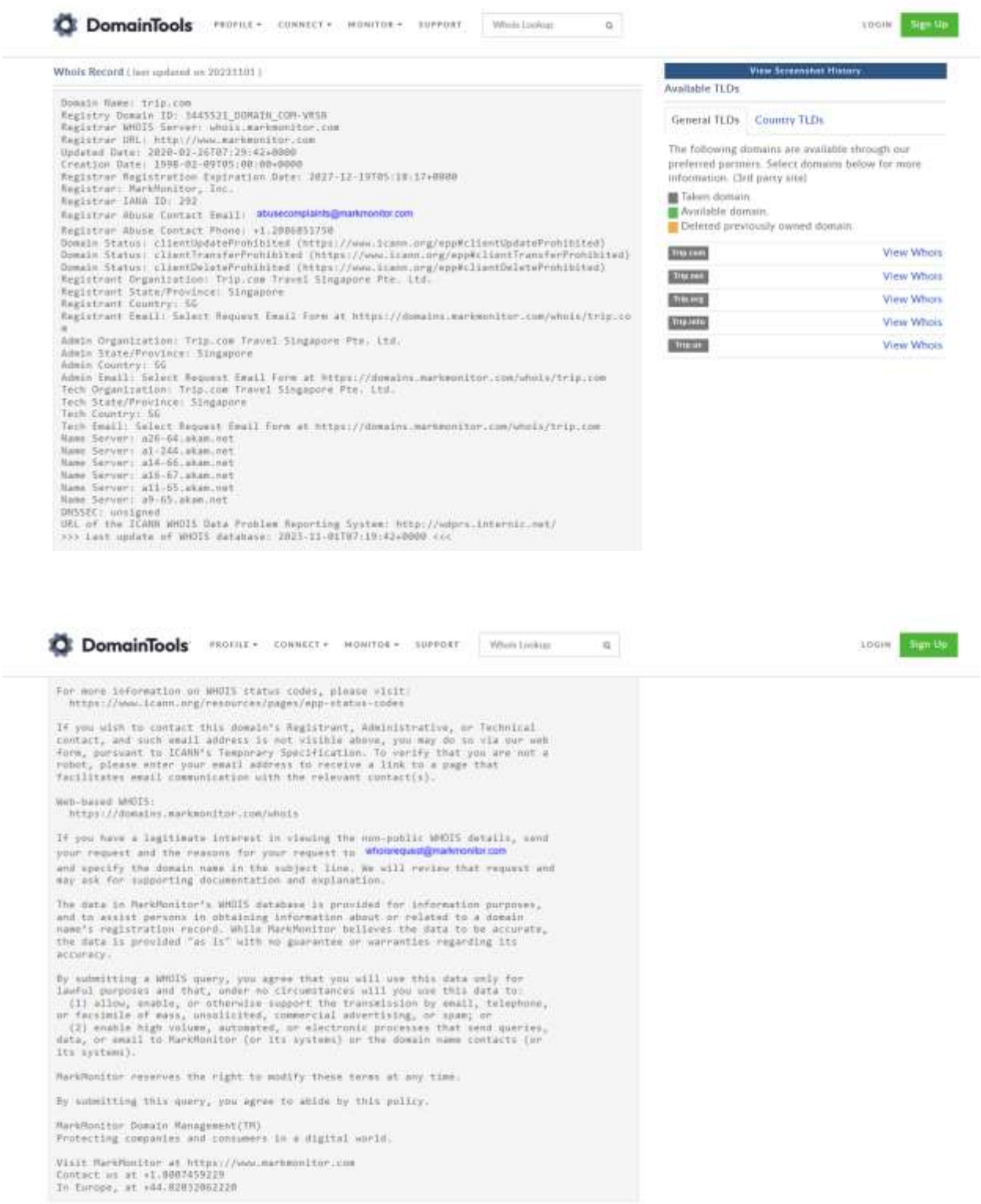



Fig. 40. Whois record

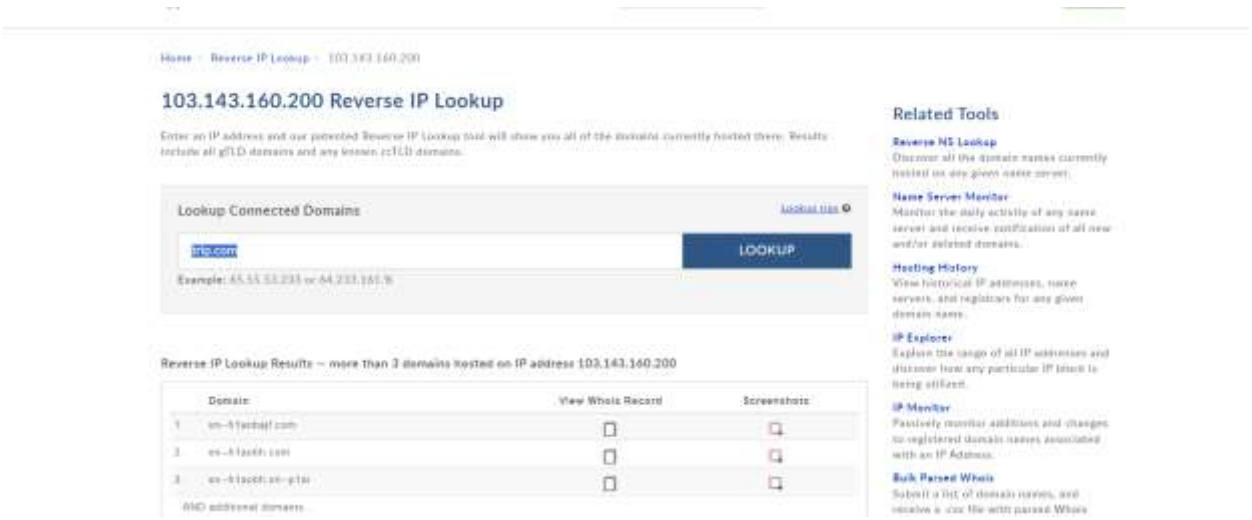



Fig. 41. Reverse IP Lookup

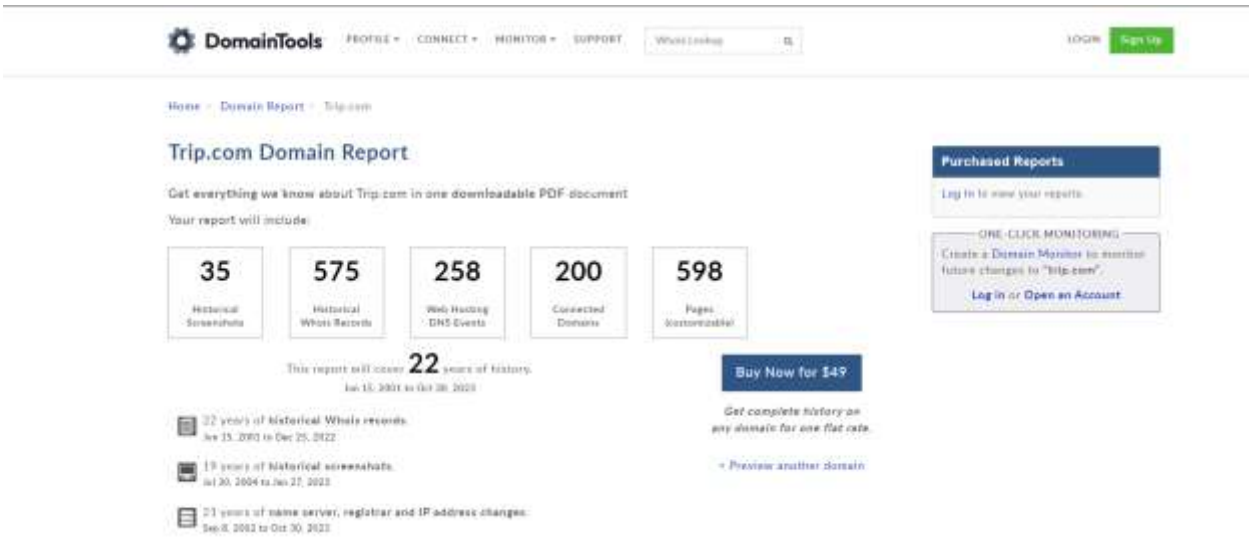



Fig. 42. Trip.com Domain Report

## 2. Active information gathering tools

### ▪ Nmap

Nmap is a tool used to recognize the state of ports, the host is up and running or not, and much other useful information can gather using this tool. Nmap tool also can be used to scan vulnerabilities inside the targeted domain. But now I use this tool only to gather information about the open ports or those ports are filtered, closed, or unfiltered. So, using the Nmap tool to execute SYN scan to gather the details about the open port of the targeted domains.

- Gather open port information about the www.trip.com web domain.

```
┌──(malith㉿kali)-[~/Documents]
└─$ sudo nmap -sS www.trip.com
[sudo] password for malith:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-01 13:42 +0530
Nmap scan report for www.trip.com (125.56.219.18)
Host is up (0.085s latency).
Other addresses for www.trip.com (not scanned): 23.32.29.91 2600:1417:75::17d5:1c9 2600:1417:75::17d5:1c3
rDNS record for 125.56.219.18: a125-56-219-18.deploy.static.akamaitechnologies.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
53/tcp  closed domain
80/tcp  open   http
443/tcp open   https

Nmap done: 1 IP address (1 host up) scanned in 12.69 seconds
```

Fig. 43. Open ports of the www.trip.com

- Gather open port information about the vcc.trip.com web domain.

```
┌──(malith㉿kali)-[~/Documents]
└─$ sudo nmap -sS vcc.trip.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-01 13:53 +0530
Nmap scan report for vcc.trip.com (23.52.40.163)
Host is up (0.10s latency).
Other addresses for vcc.trip.com (not scanned): 23.52.40.155 2600:1417:75::17d5:1c9 2600:1417:75::17d5:1c3
rDNS record for 23.52.40.163: a23-52-40-163.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 16.86 seconds
```

Fig. 44. Open ports of the vcc.trip.com

- Gather open port information about the vn.trip.com web domain.

```
┌──(malith㉿kali)-[~/Documents]
└─$ sudo nmap -sS vn.trip.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-01 13:55 +0530
Nmap scan report for vn.trip.com (23.32.29.91)
Host is up (0.18s latency).
Other addresses for vn.trip.com (not scanned): 125.56.219.18 2600:1417:75::17d5:1c9 2600:1417:75::17d5:1c3
rDNS record for 23.32.29.91: a23-32-29-91.deploy.static.akamaitechnologies.com
All 1000 scanned ports on vn.trip.com (23.32.29.91) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 185.03 seconds
```

Fig. 45. Open ports of the vn.trip.com

- Gather open port information about the tc.trip.com web domain.

```
┌──(malith㉿kali)-[~/Documents]
└─$ sudo nmap -sS tc.trip.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-01 14:02 +0530
Nmap scan report for tc.trip.com (103.143.160.200)
Host is up (0.17s latency).
Other addresses for tc.trip.com (not scanned): 103.158.15.28
rDNS record for 103.143.160.200: static-ip-200-117-229-43.TWOWINCOLIMITED-HK.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 16.08 seconds
```

- Fig. 46. Open ports of the tc.trip.com

- Gather open port information about the sin-im3.trip.com web domain.

```
┌──(malith㉿kali)-[~/Documents]
└─$ sudo nmap -sS sin-im3.trip.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-01 14:06 +0530
Nmap scan report for sin-im3.trip.com (18.140.127.116)
Host is up (0.075s latency).
Other addresses for sin-im3.trip.com (not scanned): 54.179.124.5
rDNS record for 18.140.127.116: ec2-18-140-127-116.ap-southeast-1.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 9.62 seconds
```

- Fig. 47. Open ports of the sin-im3.trip.com
- Gather open port information about the investors.trip.com web domain.

```
┌──(malith㉿kali)-[~/Documents]
└─$ sudo nmap -sS investors.trip.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-01 14:07 +0530
Nmap scan report for investors.trip.com (23.192.150.12)
Host is up (0.078s latency).
Other addresses for investors.trip.com (not scanned): 23.192.150.21 2600:1417:75::687c:3649 2600:1417:75::1
rDNS record for 23.192.150.12: a23-192-150-12.deploy.static.akamaitechnologies.com
All 1000 scanned ports on investors.trip.com (23.192.150.12) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 83.85 seconds
```

Fig. 48. Open ports of the investors.trip.com

## Dmitry

Dmitry is a collection of information-gathering tools. Because of that, this tool is a combination or package of tools. Using this tool, we can gather details related to Whois lookup web tool information, Netcraft information, and open port details. Because this tool gathers information about open ports, Dmitry is an Active information gathering tool.

```
┌──(malith㉿kali)-[~/Documents]
└─$ dmitry --help
Deepmagic Information Gathering Tool
"There be some deep magic going on"

dmitry: invalid option -- '-'
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o     Save output to %host.txt or to file specified by -o file
  -i     Perform a whois lookup on the IP address of a host
  -w     Perform a whois lookup on the domain name of a host
  -n     Retrieve Netcraft.com information on a host
  -s     Perform a search for possible subdomains
  -e     Perform a search for possible email addresses
  -p     Perform a TCP port scan on a host
* -f     Perform a TCP port scan on a host showing output reporting filtered ports
* -b     Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
```

Fig. 49. Dmitry filtering commands

- Gathering Information related to Inet-whois according to trip domain IP address.

```
┌──(malith㉿kali)-[~/Documents]
└─$ dmitry www.trip.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:23.32.29.91
HostName:www.trip.com

Gathered Inet-whois information for 23.32.29.91
---------------------------------


inetnum:        23.19.64.0 - 23.83.63.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        -------------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        -------------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2019-01-07T10:48:01Z
last-modified:  2019-01-07T10:48:01Z
source:         RIPE
```

```
role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.108 (SHETLAND)



Gathered Inic-whois information for trip.com
---------------------------------
   Domain Name: TRIP.COM
   Registry Domain ID: 3445521_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-06-13T03:46:10Z
   Creation Date: 1998-02-09T05:00:00Z
   Registry Expiry Date: 2027-12-19T05:18:17Z
   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
   Name Server: A1-244.AKAM.NET
   Name Server: A11-65.AKAM.NET
   Name Server: A14-66.AKAM.NET
   Name Server: A16-67.AKAM.NET
   Name Server: A26-64.AKAM.NET
   Name Server: A9-65.AKAM.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-11-02T04:43:53Z <<<

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

Fig. 50. Inet-whois information

- Gathering Information related to Netcraft according to trip domain.

```
Gathered Netcraft information for www.trip.com
----------------------------------

Retrieving Netcraft.com information for www.trip.com
Netcraft.com Information gathered

Gathered Subdomain information for trip.com
----------------------------------
Searching Google.com:80...
HostName:www.trip.com
HostIP:23.32.29.91
HostName:group.trip.com
HostIP:23.32.29.89
HostName:my.trip.com
HostIP:23.32.29.89
HostName:us.trip.com
HostIP:23.32.29.91
HostName:uk.trip.com
HostIP:23.32.29.91
HostName:sg.trip.com
HostIP:23.32.29.89
HostName:au.trip.com
HostIP:23.32.29.106
HostName:hk.trip.com
HostIP:23.32.29.91
HostName:ca.trip.com
HostIP:23.32.29.91
HostName:nz.trip.com
HostIP:23.32.29.89
HostName:it.trip.com
HostIP:23.32.29.106
HostName:id.trip.com
HostIP:23.32.29.89
HostName:ebooking.trip.com
HostIP:23.32.29.106
HostName:es.trip.com
HostIP:23.32.29.89
HostName:careers.trip.com
HostIP:23.32.29.106
HostName:investors.trip.com
HostIP:23.32.29.98
HostName:tw.trip.com
HostIP:23.32.29.106
HostName:pages.trip.com
HostIP:23.32.29.106
HostName:th.trip.com
HostIP:23.32.29.91
HostName:kr.trip.com
HostIP:23.32.29.106
Searching Altavista.com:80...
Found 20 possible subdomain(s) for host trip.com, Searched 0 pages containing 0 results
```

Fig. 51. Netcraft information

- Gathering Information related to E-mail and state of TCP port according to trip domain.

```
Gathered E-Mail information for trip.com
---------------------------------
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host trip.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 23.32.29.91
---------------------------------

 Port           State

80/tcp          open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed


All scans completed, exiting
```

Fig. 52. E-mail and TCP port information

- These are the Passive and Active tools I use to gather information about the www.trip.com domain.

# Planning and Analysis

After the information gathering stage, we need to analyze those details to plan what we focused on next stagers. The planning stage is very essential because vulnerability detection is a time-consuming process and with the plan, we can do vulnerability detection in a targeted way. So, we can save our time and vulnerability detection also can be done in a very efficient manner.

So, after the information gathering process that the collected data can be sorted down according to the technical details such as, Web server details, Application server details, and Database server details. And also, that the state of the ports and the HTTP protection methods are the details focused on to execute the vulnerability scan.

- Technical Details
  - Web server
    - ✓ HTTPS server is Nginx
      - ❖ www.trip.com
      - ❖ tc.trip.com
      - ❖ vcc.trip.com
    - ✓ HTTP server is Nginx
      - ❖ www.trip.com
      - ❖ vcc.trip.com
      - ❖ tc.trip.com
    - ✓ HTTP server is AkamaiGHost
      - ❖ vn.trip.com
      - ❖ www.trip.com
  - Application server
    - ✓ Python
    - ✓ PHP

- Database server
    - ✓ PostgresSQL
    - ✓ MySQL

- Open ports details are in the Nmap scan report done in the information gathering stage.
- HTTP security details are in the Wahtweb scan report done in the information gathering stage.

After that select vulnerability scanning tools according to the gathered information and plan the vulnerability scanning according to the information analysis details.

# Vulnerability Detection

Vulnerability Detection is a very important stage in Bug Bounty assessment. Because before moving to the penetration testing stage we need to identify vulnerabilities in the particular system. According to Balbix, “Vulnerability scanning is the process of identifying security weaknesses and flaws in the system.” [7].

There are two vulnerability detection methods. They are the automated scanning method and the manual scanning method. I use both of these methods to detect vulnerabilities in the targeted system. Most of the tools can scan vulnerabilities in the system for both of these two methods. Manual scanning is something like a filtered way of scanning and automated scanning is go through all subdomains in the system and scans all vulnerabilities in the system. The automated scanning method is very easy, but it is a time consuming method. Because that manual scanning is an efficient way of the vulnerability detection method.

So, detecting those vulnerabilities can be done using the Vulnerability Detection tools. There is a lot of open source and paid tools. They are,

- Legion
- Nikto
- Nmap
- Uniscan
- Owasp Zap

So, I choose that the most suitable vulnerability detection tool according to the gathered information and the usability of those tools. Because some of those tools are not freeware. So, Legion, Nikto, Uniscan, , Owasp Zap are the tool chosen for use in this Bug Bounty assessment.

- ## Legion

Legion is an open source network vulnerability detection tool to discover online devices in a network, obtain useful information about targeted systems, and expose targeted system exploits. This tool is a combination of vulnerability detecting tools. Such as Nmap, Whatweb, sslyzer, vulners, SMBenum, and Shodan tools are used in the Legion tool. So, do not need to use Nmap and other tools to detect vulnerabilities in the targeted system.

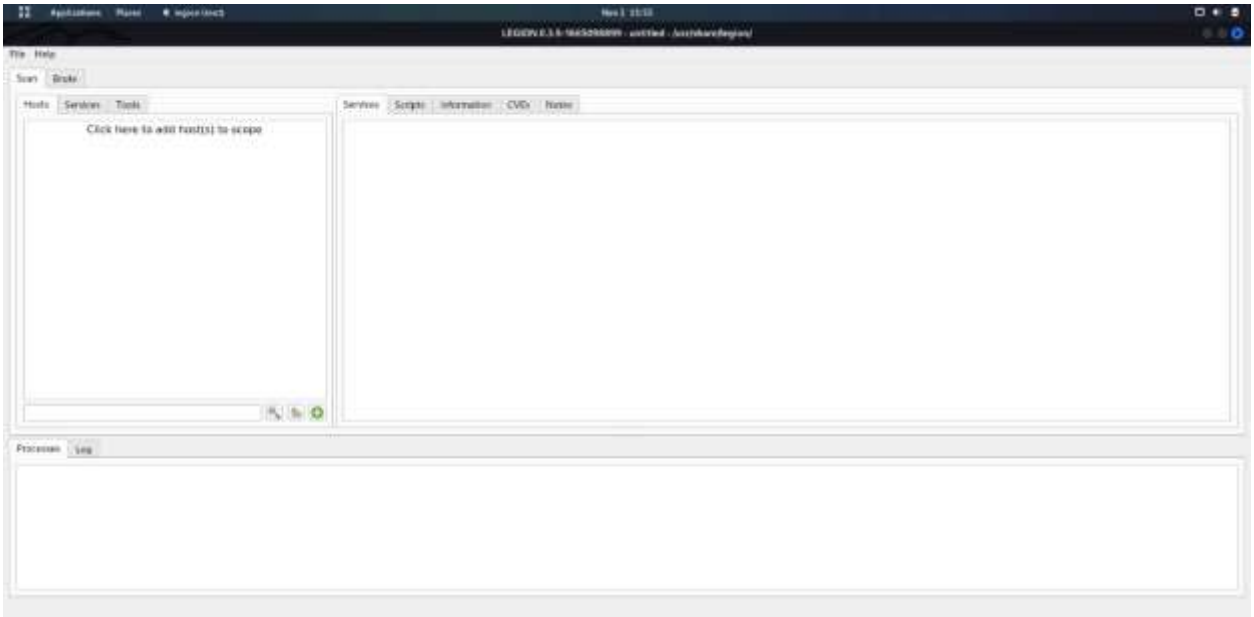


Fig. 53. Dashboard of the Legion Tool

This is the dashboard of the Legion tool. Using the green plus button we can do any type of customization to scan vulnerabilities and provide relevant subdomain links to this tool.

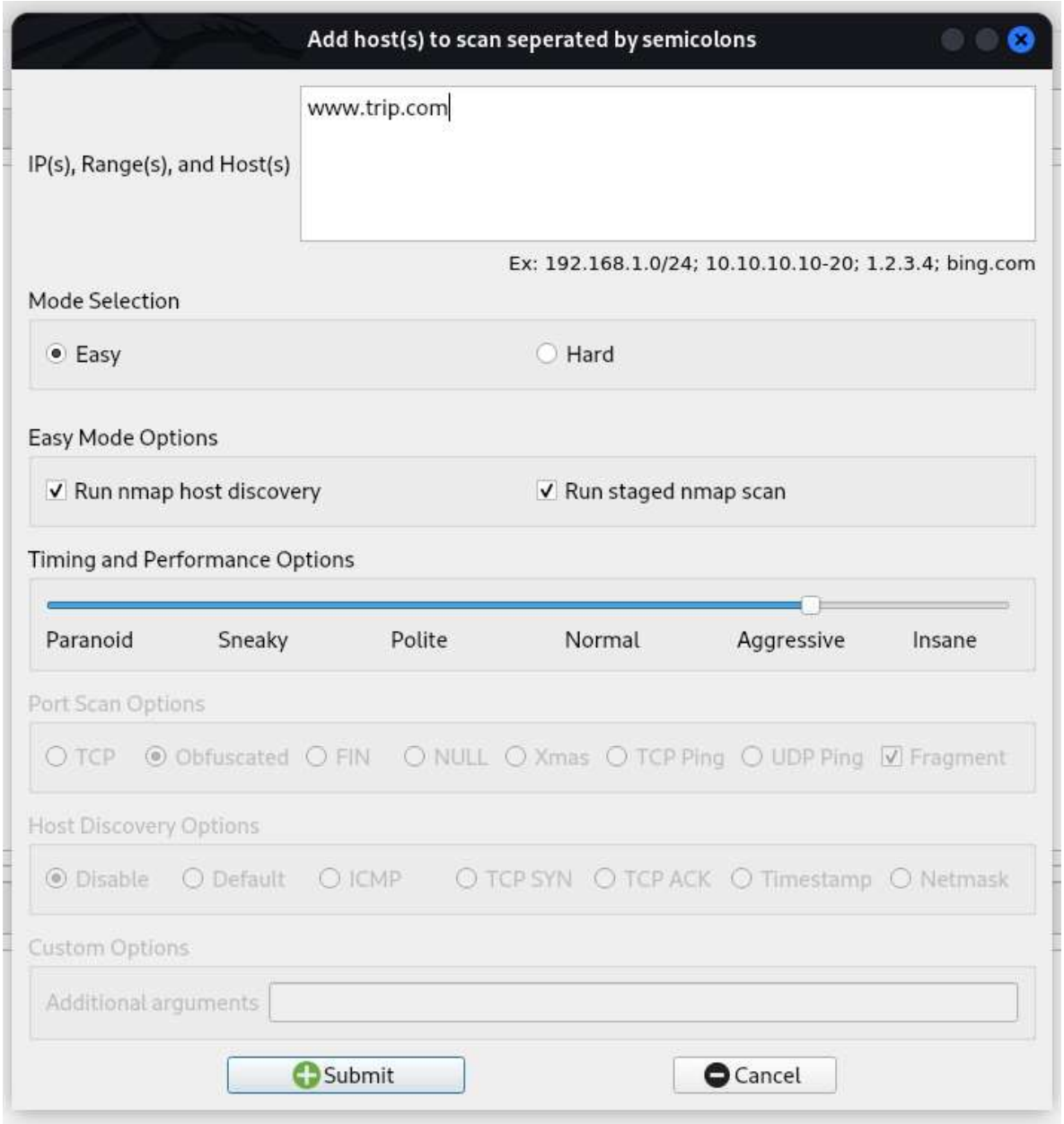



Fig. 54. Customization to scan vulnerabilities

So, I choose automated scan because I need a full scan report of targeted domains and this tool did not take much time to scan. Targeted domain IP address or hostname can use to identify the targeted system and even automated scan this tool provides some Nmap customization methods. After that the customization process is done, we need to submit to get the scanning result from this tool.

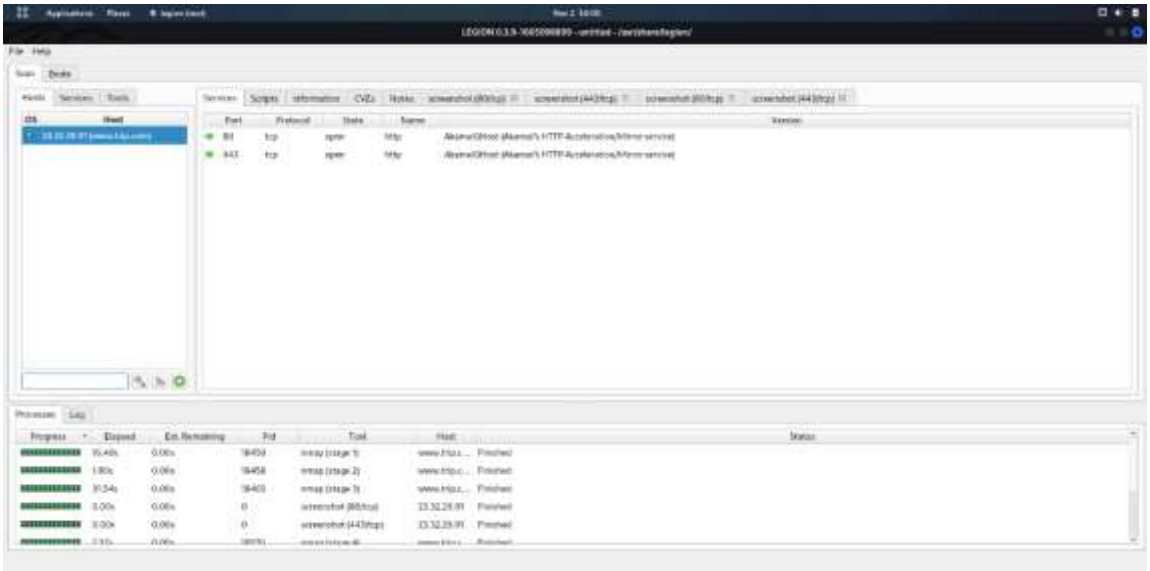


Fig. 55. Port scanning result

Port scanning also gives the same result given through the Nmap scanning done in the information gathering stage. Because that is the same tool used in this scan. 80 port and 443 port are the open port in the targeted domain. Port 80 can use to exploit vulnerabilities. Because that port is not a protected HTTP port.

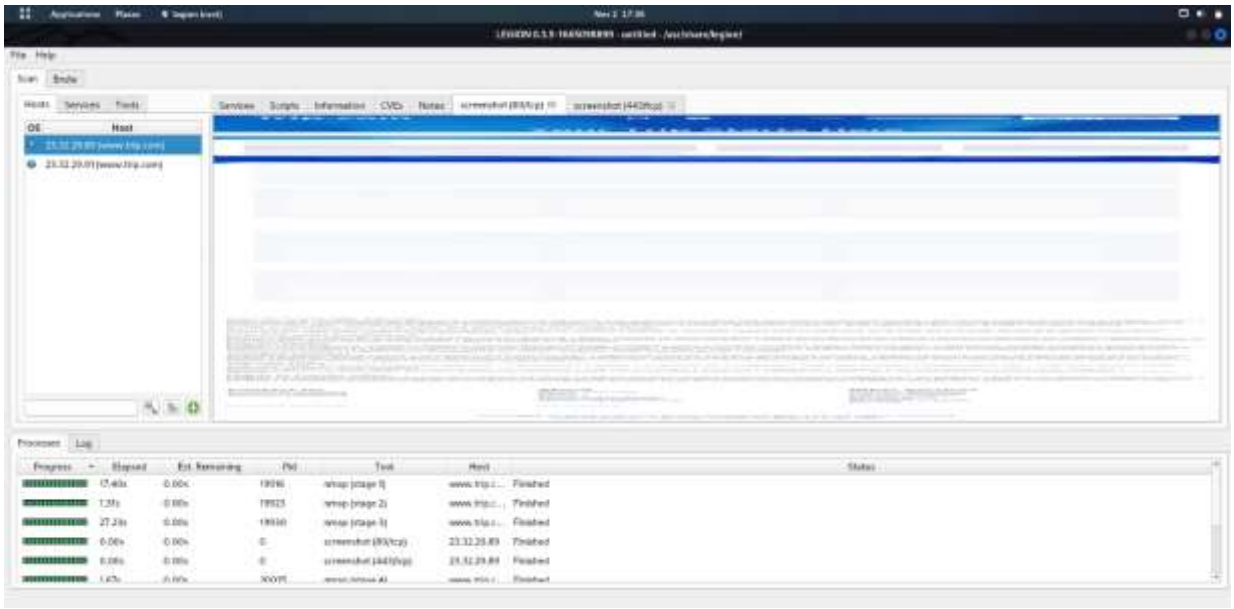


Fig. 56. Screenshot of the port 80

Other domains also give almost identical to the main domain result. And port 80 is an open port that is vulnerable to exploitation.

- ## Nikto

Nikto is a web vulnerability scanner that use to detect vulnerabilities on the targeted domain server. This tool actually detects that the server misconfiguration done by the developers. So, the Nikto tool can find misconfiguring ports in the targeted subdomain and output what type of vulnerabilities have in those subdomains.

- To get a better idea about the Nikto tool we can use the “nikto – help” command.

```
┌──(root㉿kali)-[~]
└─# nikto --help
Unknown option: help

   Options:
       -ask+               Whether to ask about submitting updates
                               yes   Ask about each (default)
                               no    Don't ask, don't send
                               auto  Don't ask, just send
       -check6             Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
       -Cgidirs+           Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
       -config+            Use this config file
       -Display+           Turn on/off display outputs:
                               1     Show redirects
                               2     Show cookies received
                               3     Show all 200/OK responses
                               4     Show URLs which require authentication
                               D     Debug output
                               E     Display all HTTP errors
                               P     Print progress to STDOUT
                               S     Scrub output of IPs and hostnames
                               V     Verbose output
       -dbcheck           Check database and other key files for syntax errors
       -evasion+          Encoding technique:
                               1     Random URI encoding (non-UTF8)
                               2     Directory self-reference (/./)
                               3     Premature URL ending
                               4     Prepend long random string
                               5     Fake parameter
                               6     TAB as request spacer
                               7     Change the case of the URL
                               8     Use Windows directory separator (\)
                               A     Use a carriage return (0x0d) as a request spacer
                               B     Use binary value 0x0b as a request spacer
        -followredirects   Follow 3xx redirects to new location
        -Format+           Save file (-o) format:
                               csv   Comma-separated-value
                               json  JSON Format
                               htm   HTML Format
                               nbe   Nessus NBE format
                               sql   Generic SQL (see docs for schema)
                               txt   Plain text
                               xml   XML Format
                               (if not specified the format will be taken from the file extension passed to -output)
```

Fig. 57. Nikto --help

So, now we need open ports scan details that were collected during the information gathering stage using the Nmap tool to get the scan result of the Nikto tool. According to the Nmap scan results, I scan all open ports use in all the targeted subdomains. So, we can use to input the hostname to the Nikto tool “-h” command and input the port address “-p” command.

```
┌──(malith㉿kali)-[~]
└─$ nikto -h www.trip.com -p 80
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 23.215.7.12, 23.215.7.26, 2600:1417:75::17d5:1c3, 2600:1417:75::17d5:1b2
+ Target IP:          23.215.7.12
+ Target Hostname:    www.trip.com
+ Target Port:        80
+ Start Time:         2023-11-05 08:08:51 (GMT5.5)
---------------------------------------------------------------------------
+ Server: AkamaiGHost
+ /: 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 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: ht
g-content-type-header/
+ Root page / redirects to: https://www.trip.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
D:Sun Nov  5 08:11:57 2023 'Request Hash' = {
        'Connection' => 'Keep-Alive',
        'Host' => '23.215.7.12',
        'User-Agent' => 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36',
        'whisker' => {
                'MAGIC' => 31339,
                'force_bodysnatch' => 0,
                'force_close' => 0,
                'force_open' => 0,
                'host' => '23.215.7.12',
                'http_eol' => "\r\n",
                'http_space1' => ' ',
                'http_space2' => ' ',
                'ignore_duplicate_headers' => 0,
                'include_host_in_uri' => 0,
                'invalid_protocol_return_value' => 1,
                'keep-alive' => 1,
                'lowercase_incoming_headers' => 1,
                'max_size' => 750000,
                'method' => 'GET',
                'normalize_incoming_headers' => 1,
                'port' => 80,
                'protocol' => 'HTTP',
                'require_newline_after_headers' => 0,
                'retry' => 0,
                'ssl' => 0,
                'ssl_certfile' => undef,
                'ssl_rsacertfile' => undef,
                'ssl_save_info' => 1,
                'timeout' => 10,
                'trailing_slurp' => 0,
                'uri' => '/www_trip_com.cer',
                'uri_param_sep' => '?',
                'uri_postfix' => '',
                'uri_prefix' => '',
                'version' => '1.1'
        }
};
```

```
D:Sun Nov  5 08:11:57 2023 'Result Hash' = {
        'connection' => 'close',
        'content-length' => 209,
        'content-type' => 'text/html',
        'date' => 'Sun, 05 Nov 2023 02:41:57 GMT',
        'expires' => 'Sun, 05 Nov 2023 02:41:57 GMT',
        'mime-version' => '1.0',
        'server' => 'AkamaiGHost',
        'whisker' => {
                'MAGIC' => 31340,
                'code' => 400,
                'data' => "<HTML><HEAD>\n<TITLE>Invalid URL</TITLE>\n</HEAD><BODY>\n<H1>Invalid URL</H1>\nThe requested URL \"6#91;no6#32;URL6#93;\", is invalid.<p>\
HTML>\n",
                'header_order' => {
                        'server',
                        'mime-version',
                        'content-type',
                        'content-length',
                        'expires',
                        'date',
                        'connection'
                },
                'http_data_sent' => 1,
                'http_eol' => "\r\n",
                'http_space1' => ' ',
                'http_space2' => ' ',
                'lowercase_incoming_headers' => 1,
                'message' => 'Bad Request',
                'protocol' => 'HTTP',
                'socket_state' => 0,
                'stats_reqs' => 228,
                'stats_syns' => 228,
                'uri' => '/www_trip_com.cer',
                'uri_requested' => '/www_trip_com.cer',
                'version' => '1.0'
        }
};
```

Fig. 58. nikto -h www.trip.com -p 80

- X-XSS-Protection is not defined. So, this protection is a must to have, and this website can be vulnerable to the Cross-Site Scripting (XSS) attack.

- And X-Content-Type-Option header also is not set. According to MDN Web Docs, “The X-Content-Type-Options response HTTP header is a marker used by the server to indicate that the MIME types advertised in the Content-Type headers should be followed and not be changed.” [8]. This also could have the risk of a Cross-Site Scripting (XSS) attack.

- Scan result of the www.trip.com using open port 443.

```
┌──(root㉿kali)-[~]
└─# nikto -h www.trip.com -p 443
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 125.56.219.18, 23.32.29.91, 2600:1417:75::17d5:1b2, 2600:1417:75::17d5:1c9
+ Target IP:          125.56.219.18
+ Target Hostname:    www.trip.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=SG/L=Singapore/O=Trip.com Travel Singapore Pte. Ltd./CN=Trip.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=DigiCert Inc/CN=DigiCert TLS RSA SHA256 2020 CA1
+ Start Time:         2023-11-02 17:08:19 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx/1.20.1
+ /: Cookie UBT_VID created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie UBT_VID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie kafka_result created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie kafka_result created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ibu_online_home_language_match created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ibu_online_home_language_match created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ; Path created without the secure 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
+ /: Cookie ibulanguage created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ibulanguage created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ibulocale created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ibulocale created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie cookiePricesDisplayed created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie cookiePricesDisplayed created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie _abtest_userid created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Uncommon header 'x-readtime' found, with contents: 125.
+ /: Uncommon header 'x-trip-app-version' found, with contents: 2.29.0.
+ /: Uncommon header 'x-trip-app-name' found, with contents: online-home.
+ /: Uncommon header 'x-trip-region' found, with contents: sg.
+ /: Uncommon header 'x-trip-app-idc' found, with contents: SIN-AWS.
+ /: 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-Transp
+ /TtNW0ckw.iso-ru: 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
bilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Hostname 'www.trip.com' does not match certificate's names: Trip.com. See: https://cwe.mitre.org/data/definitions/297.html
+ : Server banner changed from 'nginx/1.20.1' to 'AkamaiGHost'.
+ /: 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:0A000438:SSL routines::tlsv1 aler
 at /var/lib/nikto/plugins/LW2.pm line 5254.
;  at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 25 item(s) reported on remote host
+ End Time:          2023-11-02 17:11:38 (GMT5.5) (199 seconds)
---------------------------------------------------------------------------
```

Fig. 56. nikto -h www.trip.com -p 44

- ## Uniscan

Uniscan is an open-source vulnerability detection tool that can be used to scan vulnerabilities in the targeted web application, such as, cross-site scripting(XSS), remote file inclusion, web shell vulnerabilities, SQL injection, blind SQL injection, and hidden backdoors. Also, the Uniscan tool is capable to do a Bing and Google search for finding domains on shared IP addresses.

So, this tool is inbuilt in the Kali Linux operating system, and we need to give root permission to access this tool. Uniscan tool can be manually configurable. So, this tool is suitable for the filtered way of scanning.

```
┌──(root㉿kali)-[/home/malith]
└─# sudo apt-get install uniscan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libalgorithm-c3-perl libb-hooks-endofscope-perl libb-hooks-op-check-perl libclass-c3-perl libclass-c3-xs-perl libc
  libdevel-caller-perl libdevel-globaldestruction-perl libdevel-lexalias-perl libdevel-overloadinfo-perl libdevel-pa
  libmodule-implementation-perl libmodule-runtime-conflicts-perl libmodule-runtime-perl libmoose-perl libmro-compat-
  libpadwalker-perl libparams-classify-perl libparams-util-perl libsub-exporter-perl libsub-exporter-progressive-per
Suggested packages:
  libscalar-number-perl
The following NEW packages will be installed:
  libalgorithm-c3-perl libb-hooks-endofscope-perl libb-hooks-op-check-perl libclass-c3-perl libclass-c3-xs-perl libc
  libdevel-caller-perl libdevel-globaldestruction-perl libdevel-lexalias-perl libdevel-overloadinfo-perl libdevel-pa
  libmodule-implementation-perl libmodule-runtime-conflicts-perl libmodule-runtime-perl libmoose-perl libmro-compat-
  libpadwalker-perl libparams-classify-perl libparams-util-perl libsub-exporter-perl libsub-exporter-progressive-per
0 upgraded, 38 newly installed, 0 to remove and 1045 not upgraded.
Need to get 1611 kB of archives.
After this operation, 5398 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libalgorithm-c3-perl all 0.11-2 [10.8 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 libb-hooks-op-check-perl amd64 0.22-2+b1 [10.5 kB]
Get:3 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libdynaloader-functions-perl all 0.003-3 [12.7 kB]
Get:4 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libdevel-callchecker-perl amd64 0.008-2 [15.8 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 libparams-classify-perl amd64 0.015-2+b1 [23.1 kB]
Get:6 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libmodule-runtime-perl all 0.016-2 [19.6 kB]
Get:7 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libmodule-implementation-perl all 0.09-2 [12.6 kB]
Get:8 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libsub-exporter-progressive-perl all 0.001013-3 [7496
Get:9 http://http.kali.org/kali kali-rolling/main amd64 libvariable-magic-perl amd64 0.63-1+b1 [44.0 kB]
Get:10 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libb-hooks-endofscope-perl all 0.26-1 [19.6 kB]
Get:11 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libclass-c3-perl all 0.35-2 [21.0 kB]
Get:12 http://http.kali.org/kali kali-rolling/main amd64 libclass-c3-xs-perl amd64 0.15-1+b3 [17.0 kB]
```

Fig. 57. Install uniscan to kali

```
┌──(root㉿kali)-[/home/malith]
└─# uniscan
#####################################
# Uniscan project                   #
# http://uniscan.sourceforge.net/   #
#####################################
V. 6.3


OPTIONS:
        -h      help
        -u      <url> example: https://www.example.com/
        -f      <file> list of url's
        -b      Uniscan go to background
        -q      Enable Directory checks
        -w      Enable File checks
        -e      Enable robots.txt and sitemap.xml check
        -d      Enable Dynamic checks
        -s      Enable Static checks
        -r      Enable Stress checks
        -i      <dork> Bing search
        -o      <dork> Google search
        -g      Web fingerprint
        -j      Server fingerprint

usage:
[1] perl ./uniscan.pl -u http://www.example.com/ -qweds
[2] perl ./uniscan.pl -f sites.txt -bqweds
[3] perl ./uniscan.pl -i uniscan
[4] perl ./uniscan.pl -i "ip:xxx.xxx.xxx.xxx"
[5] perl ./uniscan.pl -o "inurl:test"
[6] perl ./uniscan.pl -u https://www.example.com/ -r
```

Fig. 58. Options that can use to filtered way of scanning

```
┌──(root㉿kali)-[/home/malith/Documents]
└─# uniscan -u http://trip.com/ -b
#####################################
# Uniscan project                   #
# http://uniscan.sourceforge.net/   #
#####################################
V. 6.3


Going to background with pid: [8063]
Scan date: 5-11-2023 11:48:13

┌──(root㉿kali)-[/home/malith/Documents]
└─# ==============================================================================================
| [*] http://trip.com/ redirected to http://www.trip.com/
| [*] New target is: http://www.trip.com/
==============================================================================================
| Domain: http://www.trip.com/
| Server: nginx/1.20.1
| IP: 125.56.219.18
==============================================================================================
==============================================================================================
Scan end date: 5-11-2023 11:48:20



HTML report saved in: report/www.trip.com.html
```

```
┌──(root㉿kali)-[/home/malith/Documents]
└─# uniscan -u http://trip.com/ -w
########################################
# Uniscan project                      #
# http://uniscan.sourceforge.net/      #
########################################
V. 6.3


Scan date: 5-11-2023 11:49:8
===============================================================================================
| [*] http://trip.com/ redirected to http://www.trip.com/
| [*] New target is: http://www.trip.com/
===============================================================================================
| Domain: http://www.trip.com/
| Server: nginx/1.20.1
| IP: 125.56.219.18
===============================================================================================
|
| File check:
| [+] CODE: 200 URL: http://www.trip.com/favicon.ico
| [+] CODE: 200 URL: http://www.trip.com/order/order_log.dat
| [+] CODE: 200 URL: http://www.trip.com/order/order_log_v12.dat
| [+] CODE: 200 URL: http://www.trip.com/robots.txt
===============================================================================================
===============================================================================================
Scan end date: 5-11-2023 11:52:25



HTML report saved in: report/www.trip.com.html
```

```
┌──(root㉿kali)-[/home/malith/Documents]
└─# uniscan -u http://trip.com/ -e
########################################
# Uniscan project                      #
# http://uniscan.sourceforge.net/      #
########################################
V. 6.3


Scan date: 5-11-2023 11:54:36
===============================================================================================
| [*] http://trip.com/ redirected to http://www.trip.com/
| [*] New target is: http://www.trip.com/
===============================================================================================
| Domain: http://www.trip.com/
| Server: nginx/1.20.1
| IP: 23.32.29.89
===============================================================================================
|
| Check robots.txt:
|
| Check sitemap.xml:
===============================================================================================
===============================================================================================
Scan end date: 5-11-2023 11:54:45



HTML report saved in: report/www.trip.com.html
```

```
┌──(root㉿kali)-[/home/malith/Documents]
└─# uniscan -u http://trip.com/ -d
#####################################
# Uniscan project                   #
# http://uniscan.sourceforge.net/   #
#####################################
V. 6.3


Scan date: 5-11-2023 11:55:13
===============================================================================================
| [*] http://trip.com/ redirected to http://www.trip.com/
| [*] New target is: http://www.trip.com/
===============================================================================================
| Domain: http://www.trip.com/
| Server: nginx/1.20.1
| IP: 23.209.46.138
===============================================================================================
|
| Crawler Started:
| Plugin name: Upload Form Detect v.1.1 Loaded.
| Plugin name: E-mail Detection v.1.1 Loaded.
| Plugin name: FCKeditor upload test v.1 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: phpinfo() Disclosure v.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| [+] Crawling finished, 1554 URL's found!
|
| File Upload Forms:
|
| E-mails:
| [+] E-mail Found: guanerzhounan@2x.png
|
| Timthumb < 1.33 vulnerability:
|
|
| Backup Files:
| Skipped because http://www.trip.com//testing123 did not return the code 404
|
|
| Blind SQL Injection:
|
|
| Local File Include:
|
|
| PHP CGI Argument Injection:
|
|
| Remote Command Execution:
|
|
| Remote File Include:
|
|
| SQL Injection:
|
|
| Cross-Site Scripting (XSS):
|
|
| Web Shell Finder:
===============================================================================================
Scan end date: 5-11-2023 20:7:41



HTML report saved in: report/www.trip.com.html
```

Fig. 59. Full scan report of www.trip.com

This is the scan result we can get from this tool. So, there are no vulnerabilities captured by this tool. But Nmap and other scan results are important to find vulnerabilities in the targeted system

- ## Owasp ZAP

The Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) is an open-source web application vulnerability detection tool. This is one of the best vulnerability detection tool and efficient than compared with most other tools. Owasp ZAP is also can be used as web application professional penetration testers. This tool work according to the OWASP top 10 security threats. Such as Cross-site scripting (XSS), Broken access control, SQL injection, Broken authentication and session management, Security misconfiguration and other security threats.

Consider that how does Owasp ZAP work, according to Srijan's Framework and Libraries, "ZAP creates a proxy server and makes your website traffic pass through that server. It comprises of auto scanners that help you intercept the vulnerabilities in your website." [9]. There is an automated or manual scanning option and for this assignment choose that the automated scan method because the automated method filter and scan only the in-scope subdomains. The automated scan is also customizable and if it is customized well, we can reduce that time taken for scanning the targeted subdomain.

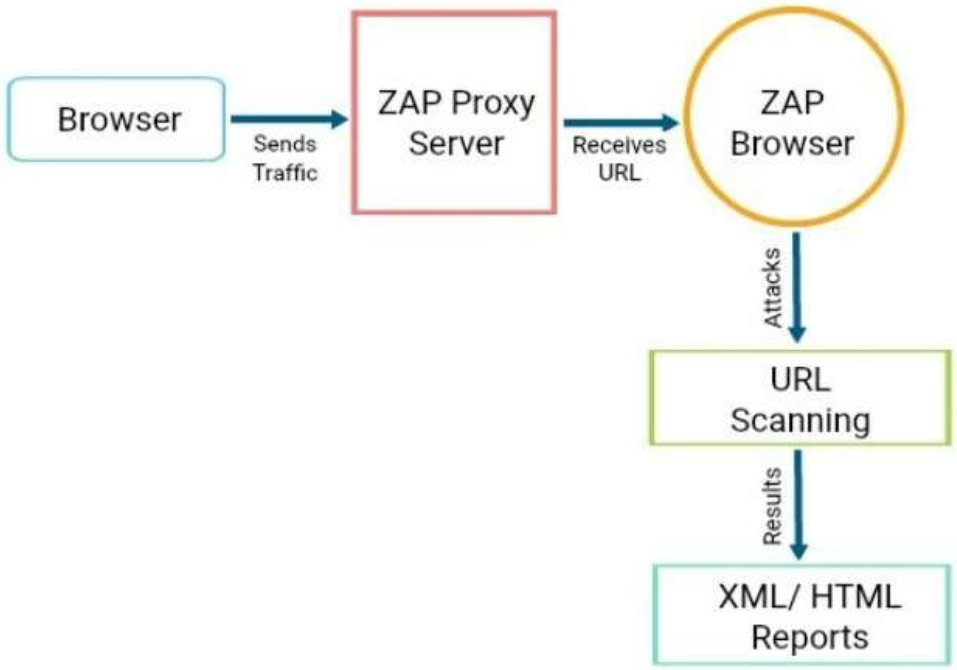



Fig. 60. How does Owasp ZAP work

- Install Owasp to kali


Fig. 61. install Owasp ZAP to kali

- Scanning process of www.trip.com

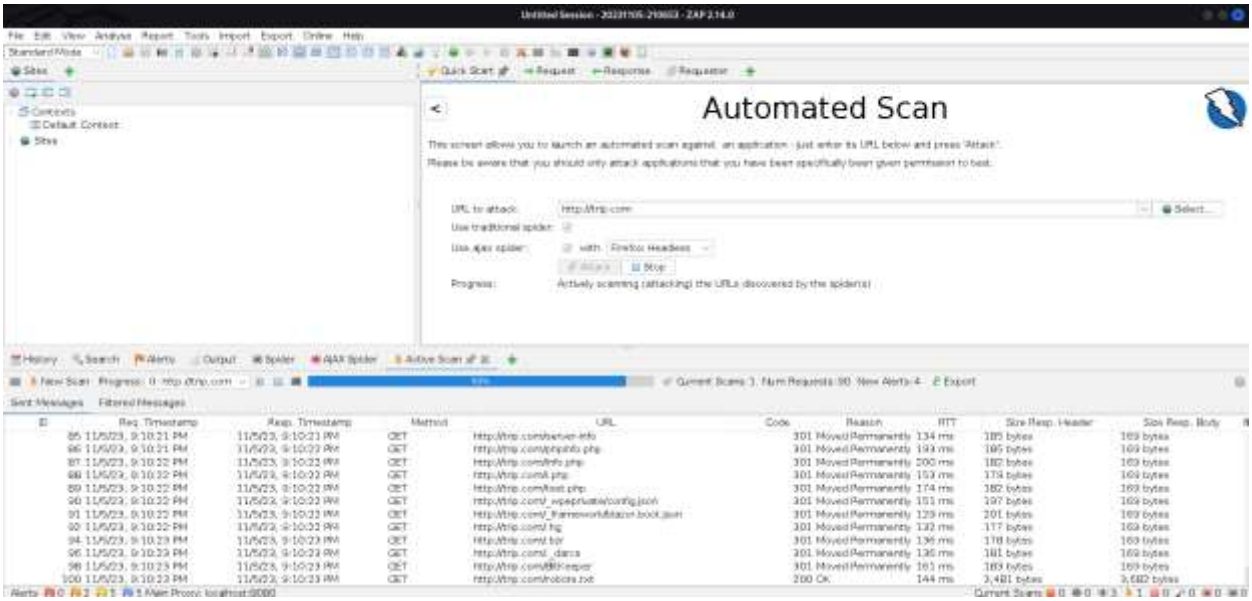



Fig. 62. Automated Scanning Process

- Scan results of www.trip.com

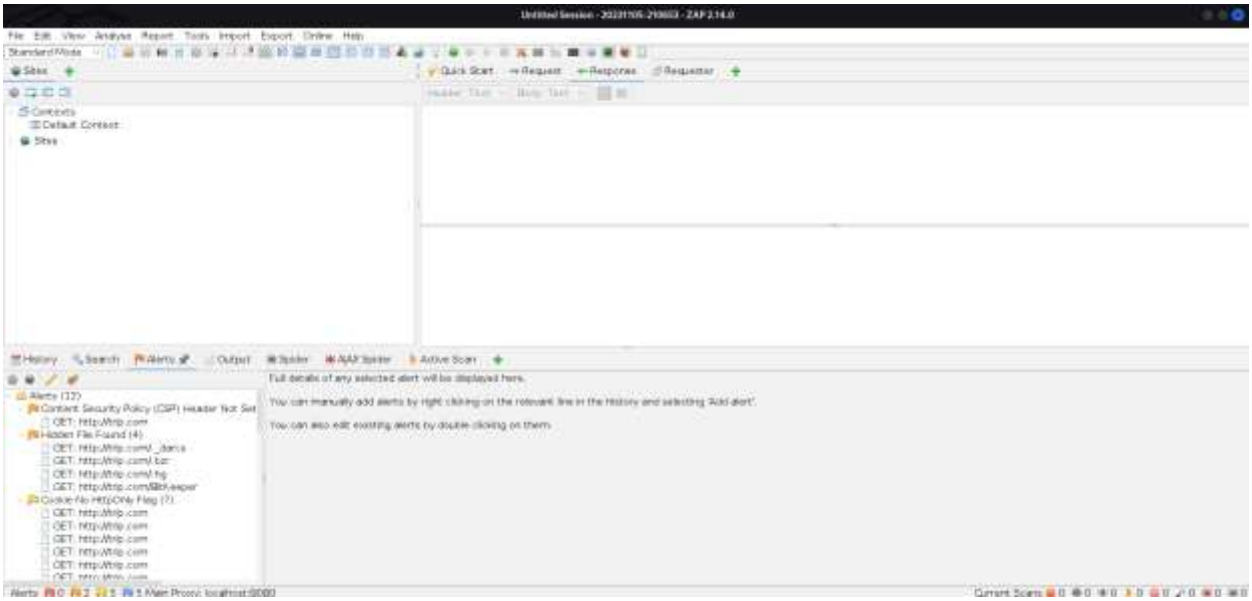


Fig. 63. Scan Results

Even this is a customized scan this tool consumes a lot of time to process the scan. Because of that, I had to abort the scan and get the result. So, these results are not the finalized result, and I already identified the vulnerabilities in the targeted system using the other tools.

## Penetration Testing

Penetration Testing is a really important stage in Bug Bounty Assessment. Because in this stage test the scanned vulnerabilities found in the targeted subdomain. So, we can find out that vulnerabilities are actually exploitable or not. According to the National Institute of Standards and Technology (NIST), "Penetration Testing is a method of testing where testers target individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited to compromise the application, its data, or its environment resources." [10]. Also, this process is named ethical hacking or pen-testing. So, this process can help to confirm the vulnerabilities in the targeted system.

Penetration testing is a crucial aspect in the confirmation of data security in every aspect of the data is used today. The necessity of it is highlighted due to the benefits it gives. Penetration tests allow us to identify new bugs and loopholes in existing software, test new software for existing bugs, and whether the implemented security controls are sufficient to handle the latest security threats. It enables us or our company to be able to stay up to standard with recognized international standards like General Data Protection Regulation (EU GDPR), Data Protection Act (DPA), Payment Card Industry Data Security Standard (PSI DSS), fix the identified bugs and loopholes in security controls that have already been implemented to assure our clients and stakeholders that their data is secure.

After confirming those vulnerabilities, we need to report these vulnerabilities and the protection methods to the relevant company belong the targeted system. And this process needs to be done before attackers exploit the system.

In the vulnerability detection stage, there are identified Critical level and High level vulnerabilities. In the penetration testing stage check, these identified vulnerabilities are impacting the targeted domains and suggest that the protection techniques secure the target domains.

# References


[1] OWASP Top 10 Security Risks & Vulnerabilities 2020 | Sucuri

[2] Information Gathering Techniques for Penetration Testing [Updated 2023] | All About Testing

[3] GitHub - aboul3la/Sublist3r: Fast subdomains enumeration tool for penetration testers

[4]whatweb | Kali Linux Tools

[5]Clickjacking Defense - OWASP Cheat Sheet Series

[6]X-XSS-Protection - HTTP | MDN (mozilla.org)

[7] What is Vulnerability Scanning | Balbix

[8] X-Content-Type-Options - HTTP | MDN (mozilla.org)

[9]An intro to OWASP Zed Attack Proxy (srijan.net)

[10] penetration testing - Glossary | CSRC (nist.gov)