BUG BOUNTY START-UP

How I initiate my Bug Bounty Hunting journey using Hackerone Bug Bounty platform

NIPUN DILSHAN

Sri Lanka Institute of Information Technology

Bug Bounty Assignment

IE2062 – Web Security

https://www.oppo.com

Submitted by:

Student Registration Number	Student Name
IT20021870	Dilshan K. N

Date of submission

4th November 2021

Table of Content

Acknowledgement

I would like to express my sincere gratitude to Web Security module, lecture in charge Dr. Lakmal Rupasinghe and Miss Chethana Liyanapathirana for their valuable support and guidance in completing this assignment. Specially, Dr. Lakmal Rupasinghe's guidance and detailed explanations became vital in project initiation phase.

In the other hand, practical knowledge which gave by Miss Chathuri Udagedara and Miss Menaka Moonamaldeniya, was essentials for continuing this assignment. I also like to thank them in this occasion as well.

Purpose

It's essential to perform web audits and find all available security breachers and flows on the systems to ensure the system confidentiality, integrity, and availability. Based on that purpose, we were asked to conduct a web audit and bug bounty for the pre-selected platform.

I refer https://www.hackerone.com bug bounty platform to select suitable flatform for conduct the web audit. Eventually I choose the https://hackerone.com/oppo?type=team for conduct this second year second semester Web Security module assignment.

Introduction

Web applications are an essential component of any organization. An online company would be unable to archive their cooperative goals if they did not have proper web applications. As a result, in order to keep operations running smoothly and uninterruptedly, the company's web applications must be protected from cyberattacks and security loophole exploits.

Impartial cybersecurity experts can use bug bounty programs to report bugs to organizations and receive rewards or compensation. These bugs are typically security exploits and vulnerabilities, but they can also include process issues, hardware flaws, and other issues also.

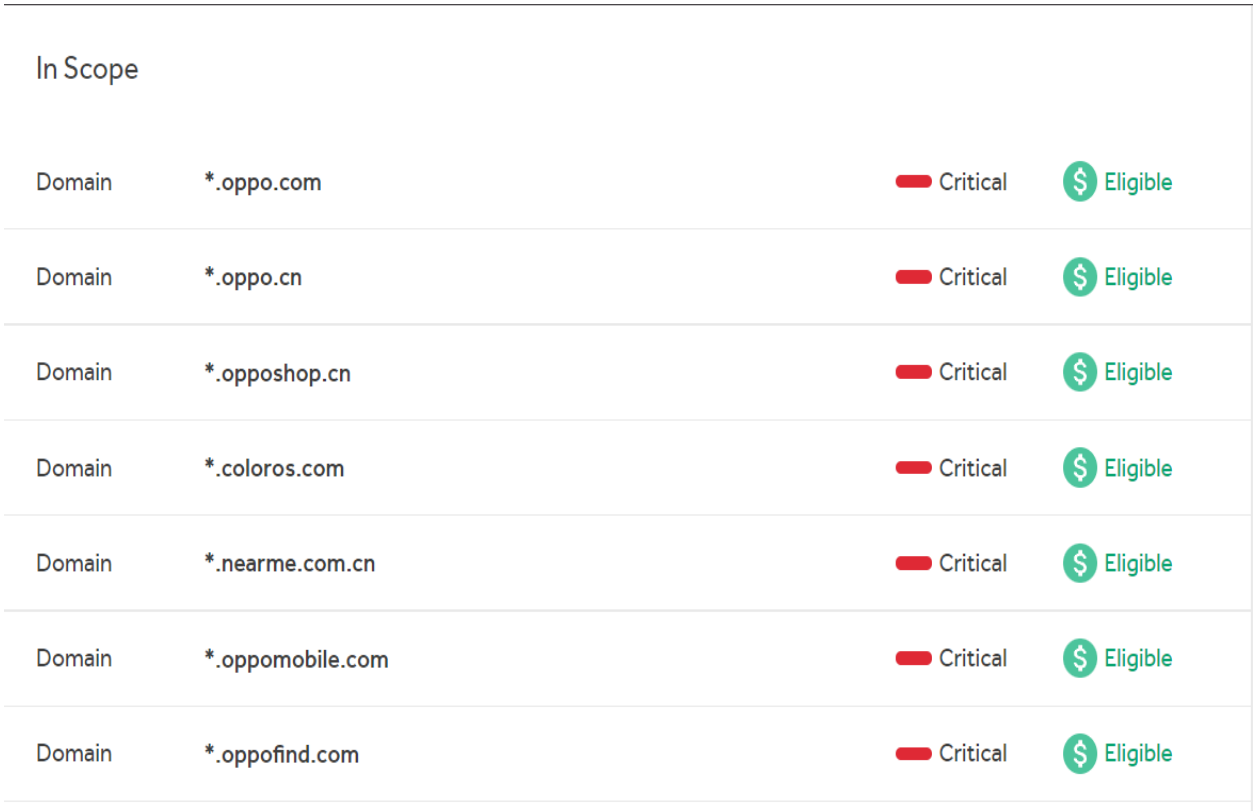
Normally, the reports are prepared through a program run by an independent third party. The organization will create a program that is tailored to the needs of the organization. Programs can be private, and reports are kept confidential to the organization or public. They can take place over a specific time period or without a set deadline.

Under this report I will demonstrate, how I began the bug bounty journey and my greatest failures same as the initial steps and which tools I used to in order to identify the flaw or a weakness in the web application. Under each section, complete guidelines provide with proper snaps and detailed descriptions as well.

Scope

In scope Domains

Since there are multiple domains available, under this report, I narrow down the in-scope domain count to seven domains. Bellow, screen shot shows the selected domains.



After selecting the domains, I create the text domain called “domain.txt” to store the selected domains. Having a text document always help to conduct efficient web audit.

Out scope Domains

Following domains are mentioned as out of scope.

- xiaoneng.oppo.com
- feedback.nearme.com.cn
- www.oppo.com.my
- http://opposimulator.com/
- i.feedback.oppomobile.com
- intl-feedback.oppomobile.com
- intl.feedback.oppomobile.com
- feedback.oppomobile.com
- *.myoas.com
- *.realmepaysa.com
- *.realme.com.tw
- community.coloros.com
- preview.myoas.com
- t-preview.myoas.com
- open.oppomobile.com **(**At present, the business is investigating security problems. We will not accept vulnerabilities during the time. Thank you for your attention)

Risk Level Information

Rewards			
Low	Medium	High	Critical
$70	$430	$1,440	$4,300
$50	$150	$720	$1,440

- **Critical Severity**

Critical vulnerabilities include but are not limited to:

- Vulnerabilities that result in arbitrary code execution on the affected system.
- Mass PII leakage of customers or employees
- Serious Business logic flaws

- **High Severity**

High-risk vulnerabilities include but are not limited to:

- Leakage of sensitive information, including but not limited to SQL injection in non-core databases, leak of compressed source code packages, using reversible encryption algorithm or storing in plaintext on the server, moving API access summary, hard coding, and disclosure of sensitive information caused by leakage of information on GitHub.
- Unauthorized access to sensitive information, including but not limited to bypassing authentication to directly access the management backend, weak backend passwords, and SSRF vulnerabilities that can be exploited to obtain a large amount of sensitive information from the internal network.
- Unauthorized manipulation of sensitive information, including but not limited to unauthorized account operations to modify important information, execute orders, modify important service configurations, etc.
- Other vulnerabilities that affect users on a large scale. These include but are not limited to Stored XSS and Blind XSS vulnerabilities on important pages that can automatically propagate themselves and obtain authentication credentials (Cookies).

- **Medium Severity**

Medium-risk vulnerabilities include but are not limited to:

- Vulnerabilities that require interaction to affect users. These include but are not limited to Stored XSS and Reflected XSS (including Reflected DOM-XSS) vulnerabilities on general web pages, JSON Hijacking, and critical CSRF vulnerabilities.
- General unauthorized operations, including but not limited to modifying user data and performing user operations by bypassing restrictions.
- General information leakage, including but not limited to web directory traversal, system directory traversal, and plain-text password transmission over the HTTP when a HeyTap account is used for sign-in.
- General flaws in logical design and process, including but not limited to logic flaws that can be exploited to bypass the verification code to access important systems, and bypassing restrictions to conduct credential stuffing attacks.
- Weak password discovered used to access management backend.

- **Low Severity**

Low-risk vulnerabilities include but are not limited to:

- Vulnerabilities that could be exploited only in certain non-mainstream browser environments (such as IE6) to obtain user identity information. These include but are not limited to Reflected XSS (including Reflected DOM-XSS) vulnerabilities, and Stored XSS vulnerabilities for general services.
- Minor information leakage, including but not limited to leakage of path information, SVN info, PHPinfo, detailed exception information, logs, configuration information, and error messages plain-text password transmission over HTTP when a non-HeyTap account is used for sign-in. Information that is trivial and cannot be directly misused will be deemed out of scope, examples of that would be generic application/server errors, or banner grabbing (showing server/software types and version number).
- Unauthorized access, including but not limited to bypassing the active defense system on the client.

- Open redirect vulnerabilities.
- Issues that cannot be exploited easily but have potential security risks, including but not limited to using CSRF to turn self-XSS into an exploited XSS, JSON Hijacking that has obtained sensitive information, clickjacking on input web pages containing sensitive information (a valid exploit must be provided in the vulnerability details), and remote code execution vulnerabilities that require man-in-the-middle attacks, with an effective PoC provided.
- Other vulnerabilities that can only cause minor damage, including but not limited to URL jumps, improper system/service O&M configurations, and component permission vulnerabilities.
- Lack of rate limiting on sensitive functionality.
- Brute-force/lack of rate limiting on One Time Passwords (OTPs).

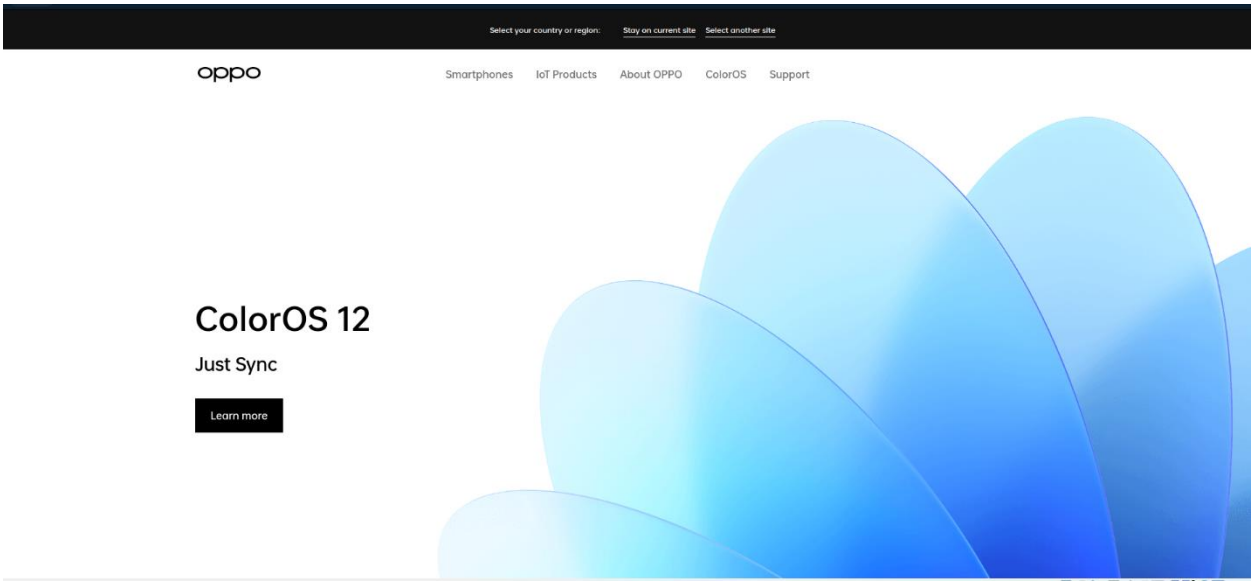
Out of scope vulnerabilities

- Denial of Service attacks.
- Recently disclosed 0-day vulnerabilities (a researcher should wait around 30 days of cool down period to report)
- Disclosure of known public files or directories.
- Use of a known-vulnerable library without a description of an exploit specific to our implementation
- **Other Out of scope vulnerabilities** list available in https://hackerone.com/oppo?type=team [1]

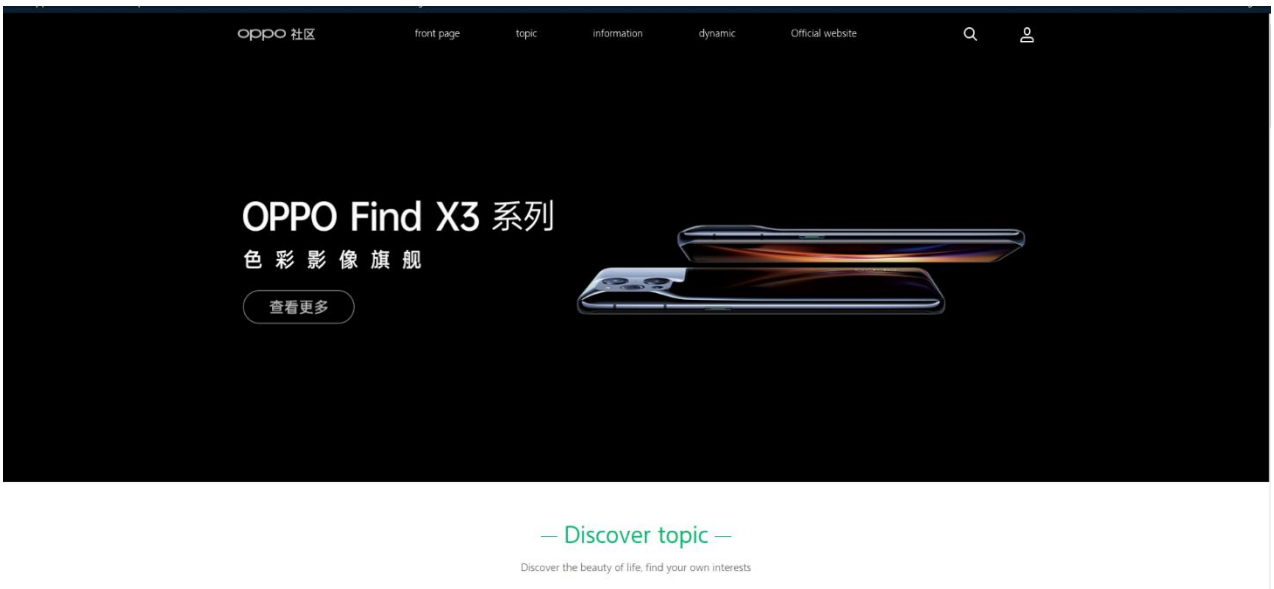
Information Gathering

Initially I brows in scope domains to render their webpages to identify the webpage contents and basic behaviors.

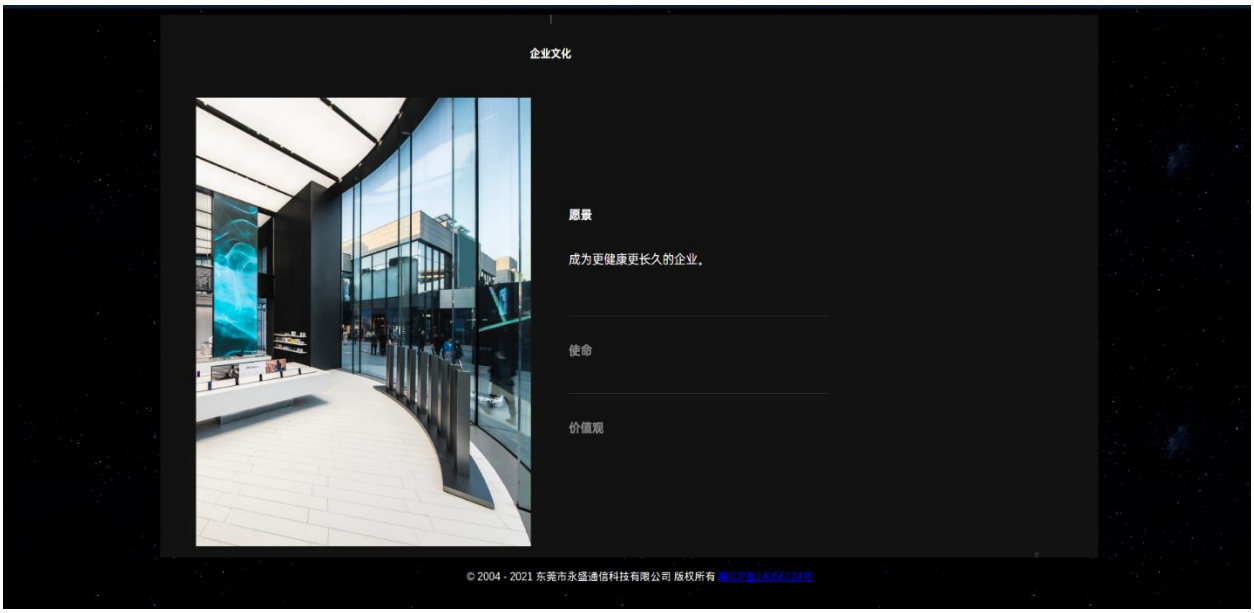
1. .oppo.com



2. .oppo.cn

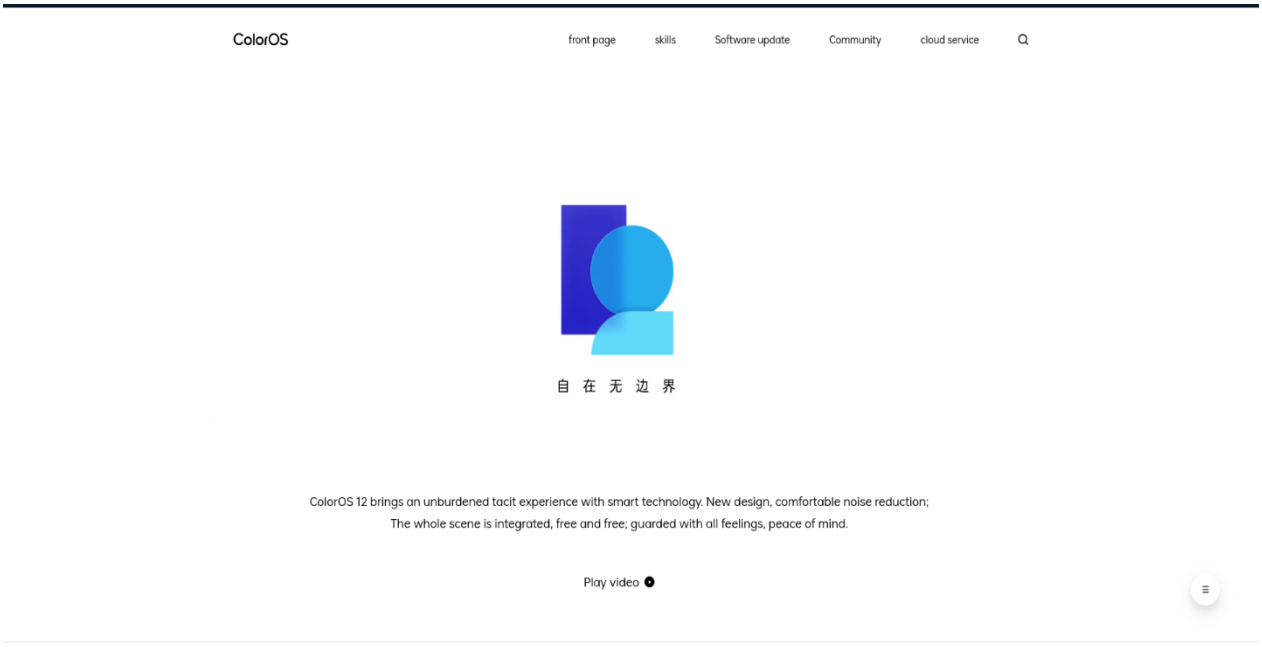


3. .opposhop.cn



When I request .**opposhop.cn,** request will internally redirect to **https://www.myoas.com/.**

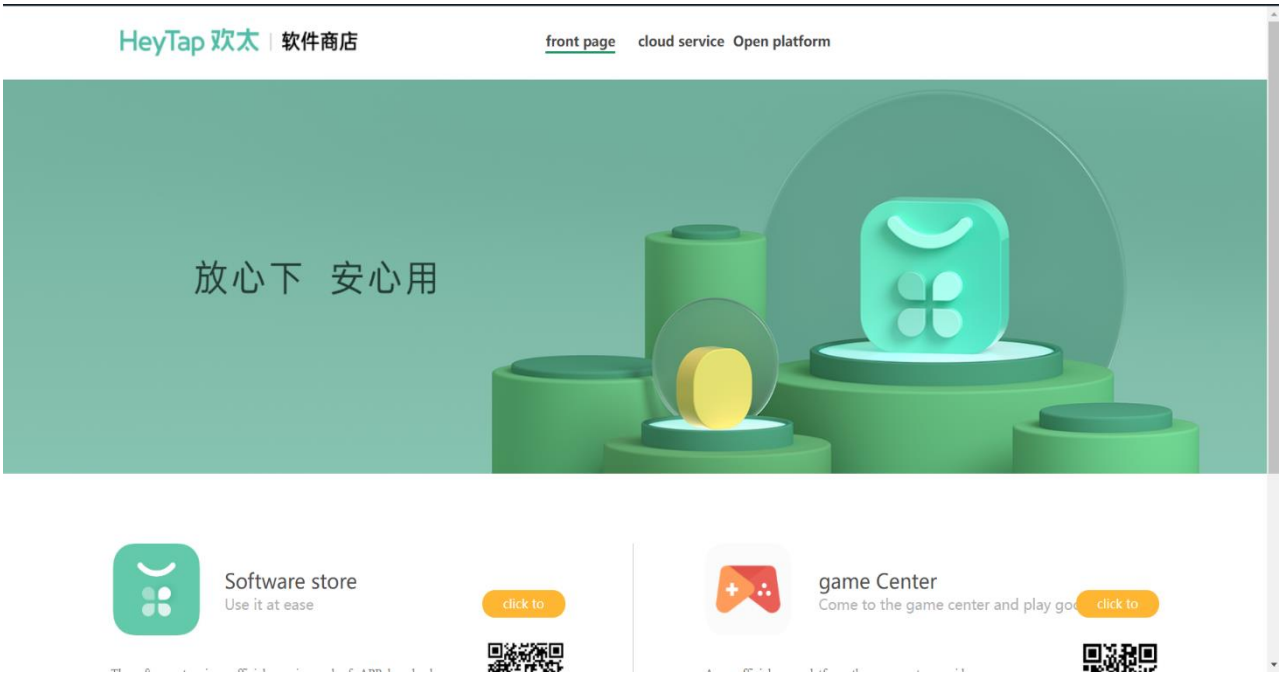
4. .coloros.com



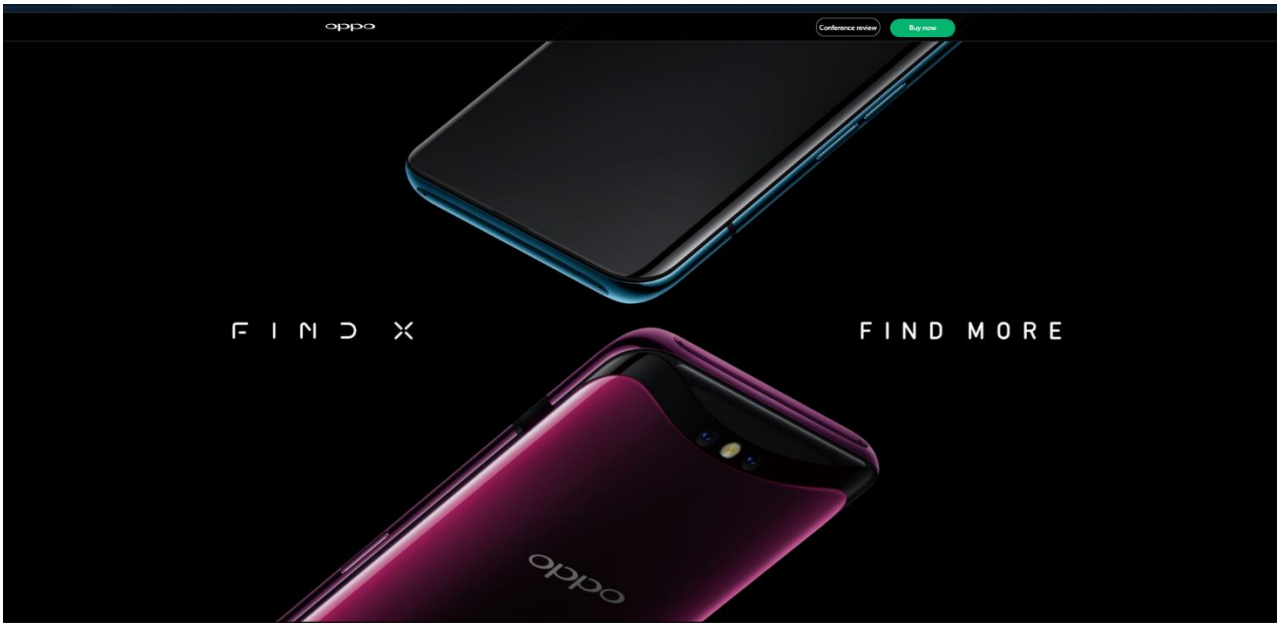
5. .nearme.com.cn

When I request **.nearme.com.cn,** request will internally redirect to **https://store.oppomobile.com**

6. .oppomobile.com



7. .oppofind.com



Subdomain Enumeration

1. Subfinder

Subfinder is a subdomain explore tool that uses passive online information to gather valid subdomains for websites. It has a simplistic modular architecture and is speed-optimized. Subfinder is designed for passive subdomain enumeration, and it complies with all passive source licenses and usage restrictions, while also maintaining a consistent passive model that makes it useful to both penetration testers and bug bounty hunters.

Followings are the key features of Subfinder tool,

- Fast and powerful resolution and wildcard elimination module
- Curated passive sources to maximize results
- Multiple output formats supported (Json, File, Stdout)
- Optimized for speed, very fast and lightweight on resources

Installation

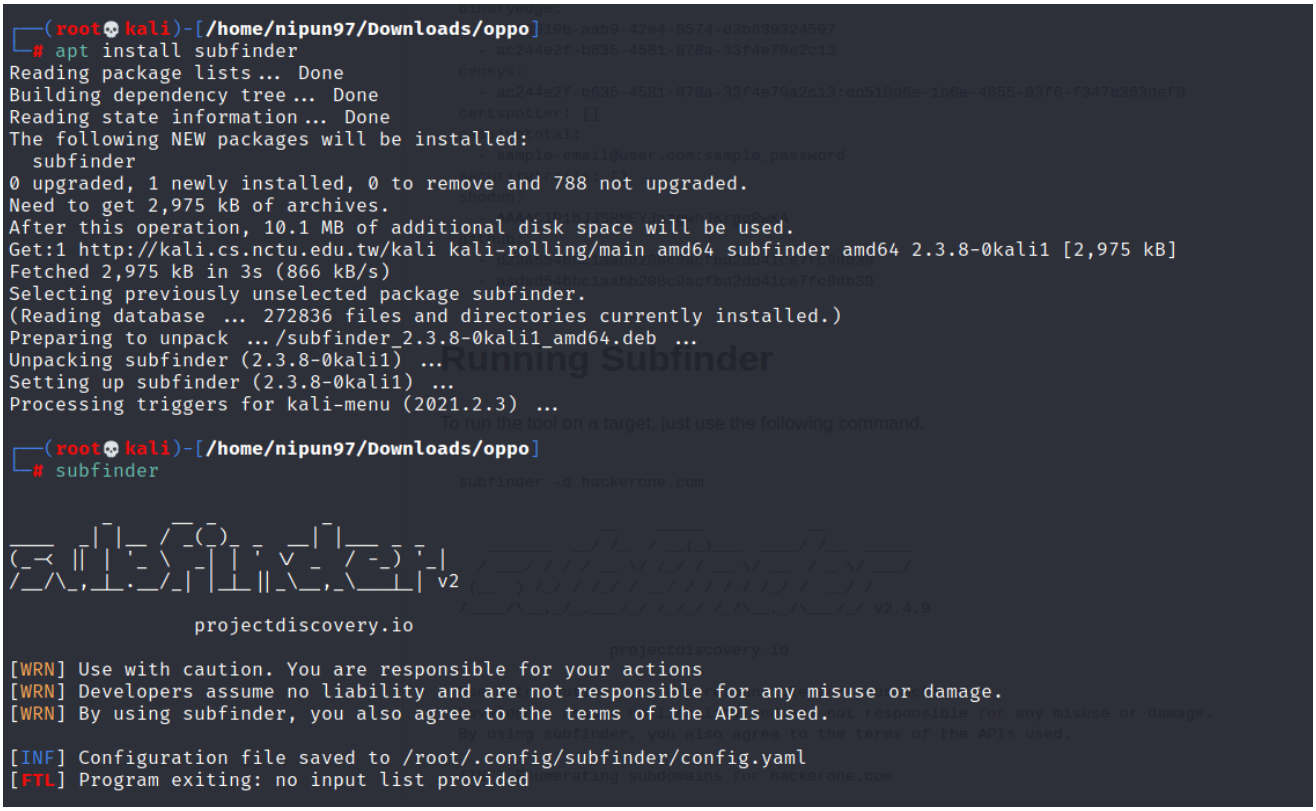
Sufinder can be install to Linux using bellow command

- apt install subfinder

Note :

If your system fails to execute “go” command, then install “golang” by using snap store

- snap install go –classic



2. HttpX

HttpX is a fast and multi-purpose HTTP toolkit that allows you to run multiple probers using the retryablehttp library. It is designed to maintain result reliability as the number of threads increases.

The following are the key features of the HttpX tool:

• A simple and modular code base that makes it simple to contribute.

• Quick and fully customizable flags for probing multiple elements.

• Allows for multiple HTTP-based probing.

• Intelligent auto-fallback from https to http as the default.

• Accepts hostnames, URLs, and CIDR as input.

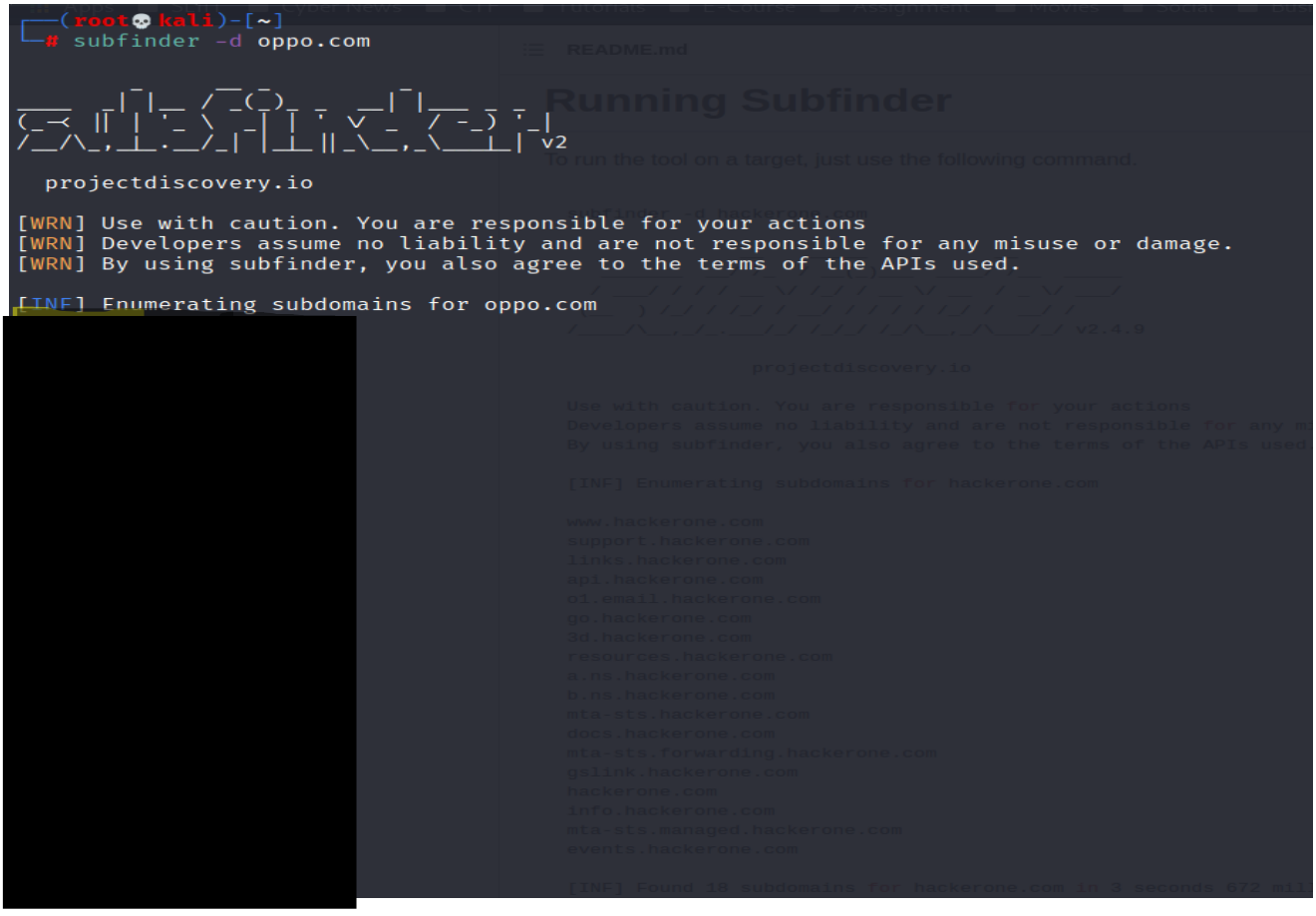
• Handles edge cases by performing retries, backoffs, and other operations in order to handle WAFs.

Initially I thought to concatenate both Subfinder and HttpX for efficient sub domain enumeration for “oppo.com”. I tried so many different ways to run HttpX tool but unfortunately, I fail to execute that tool.

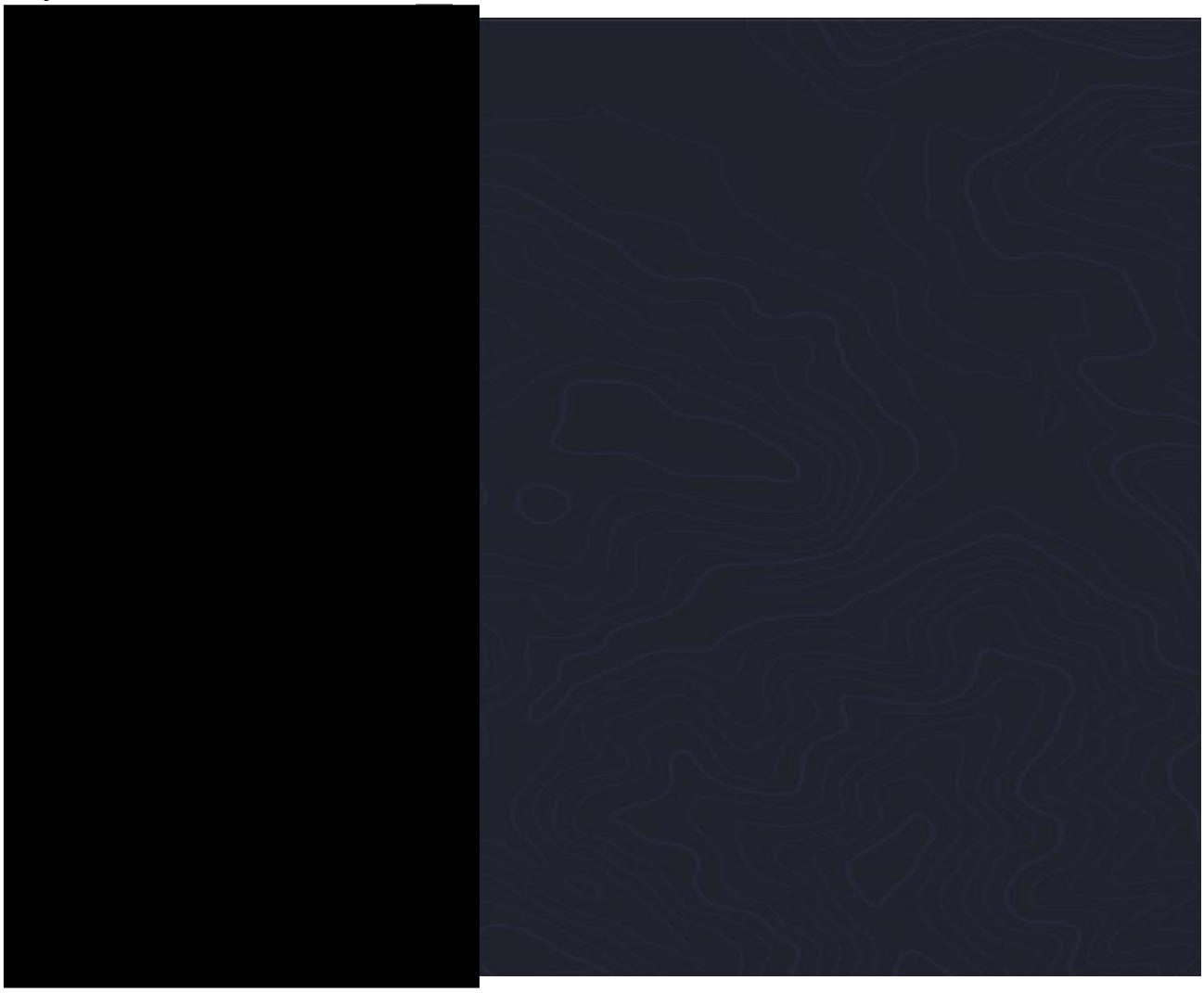
- subfinder -d oppo.com -silent | httpx -title -tech-detect -status-code [**helps to identify the subdomain takeover vulnerability as well]**

GitHub repository URL : https://github.com/projectdiscovery/httpx/tree/master

Afterwards, using the subfinder tool I did the subdomain enumeration as follows.



After completing successful subdomain Enumeration, resulted subdomains listed in this way.



3. Assertfinder

Assertfinder is a subdomain enumeration tool written in the "Go" programming language. Essentially, this tool searches for domains and subdomains that may be related to a given domain. The following default sources have been added to the Assertfinder tool.

- crt.sh
- certspotter
- hackertarget
- threatcrowd
- findsubdomains (optional)
- virustotal (optional)
- facebook (optional)
- dns.bufferover.run

- wayback machine

Installation

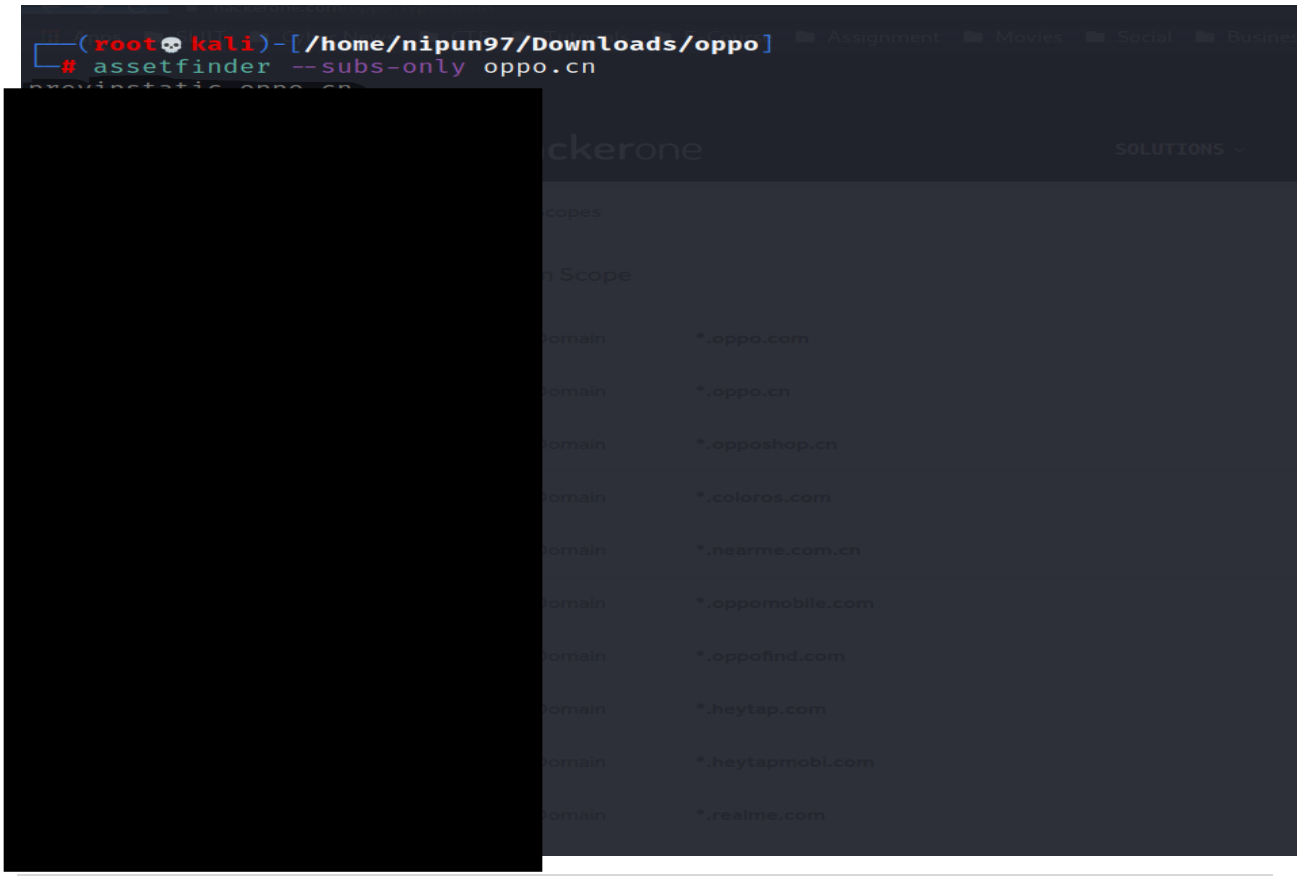
tool can be installed to Linux using below command

- git clone https://github.com/tomnomnom/assetfinder.git

Then I use,

- assertfinder –subs-only oppo.cn

to find subdomains under the oppo.un domain. This tool it efficient and gave results in quick time.



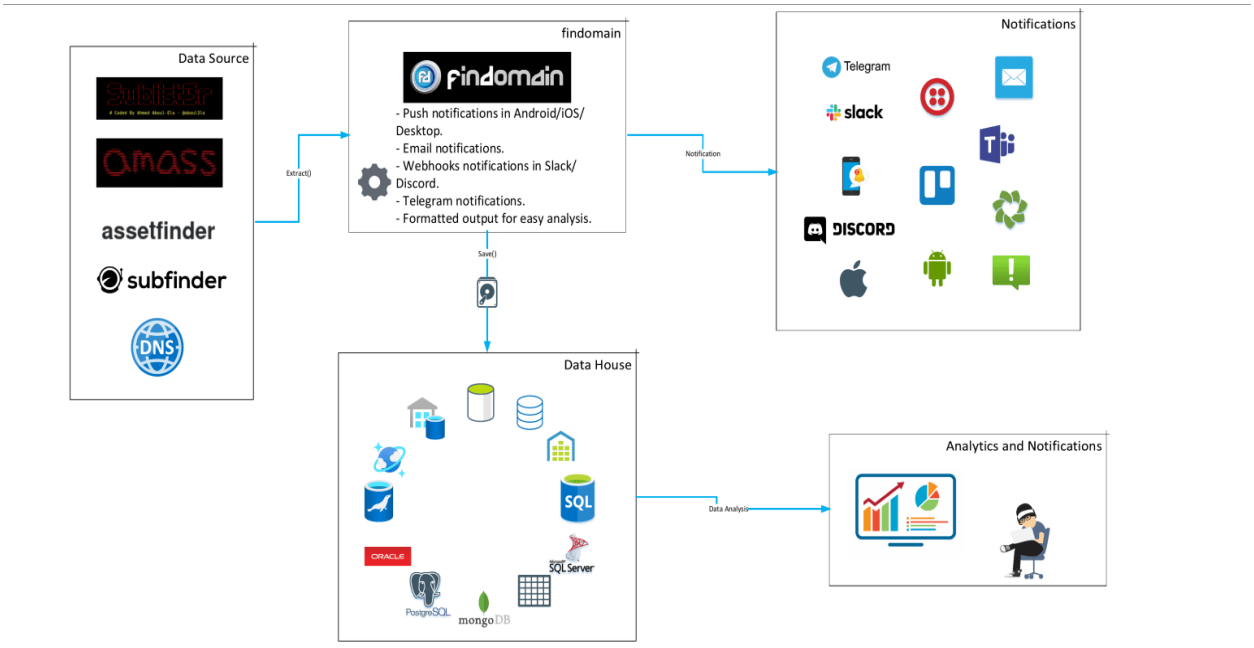
Note :

This tool also can concatenate with httpX and httprobe tools for gain more customized results.

4. Findomain

Findomain is a popular subdomain enumeration tool among bug bounty hunters and cybersecurity specialists all over the world. Findomain is a comprehensive recon framework that uses cutting-edge technology to send alerts about new subdomains, their HTTP status, open ports, IP addresses, and more to webhooks, emails, Telegram chats, and push notifications to Android, iOS, Desktop, and Smart Watches via Pushover. The tool is written in Rust and provides high performance, security, and dependability for large tasks.

Finddomain tool integrated the passive results of the top four tools like OWASP Amass, Sublist3r, Assetfinder and Subfinder in our process in order to provide efficient subdomain enumeration.



Installation

- URL : https://github.com/findomain/findomain.git

Tool can be installed to Linux by using bellow commands

- git clone https://github.com/findomain/findomain.git
- cd findomain
- cargo build --release
- sudo cp target/release/findomain /usr/bin/
- findomain

Note :

in order to install this tool “rust”, “make” and “perl” should be required

```
      Path to a file (or files) containing a list of DNS IP address. If no specified then Google, Cloudflare and
      Quad9 DNS servers are used.
  --exclude-sources <exclude-sources>...
      Exclude sources from searching subdomains in. [possible values: certspotter, crtsh, virustotal, sublist3r,
      facebook, spyse, bufferover, threatcrowd, virustotalapikey, anubis, urlscan, securitytrails, threatminer,
      archiveorg, c99, ctsearch]
-f, --file <files>...                       Use a list of subdomains writen in a file as input.
  --http-timeout <http-timeout>
      Value in seconds for the HTTP Status check of subdomains. Default 5.

  --import-subdomains <import-subdomains>...
      Import subdomains from one or multiple files. Subdomains need to be one per line in the file to import.

  --iport <initial-port>                    Initial port to scan. Default 0.
-j, --jobname <jobname>
      Use an database identifier for jobs. It is useful when you want to relate different targets into a same job
      name. To extract the data by job name identifier, use the query-jobname option.
  --lport <last-port>                       Last port to scan. Default 1000.
  --postgres-database <postgres-database>   Postgresql database.
  --postgres-host <postgres-host>           Postgresql host.
  --postgres-password <postgres-password>   Postgresql password.
  --postgres-port <postgres-port>           Postgresql port.
  --postgres-user <postgres-user>           Postgresql username.
  --rate-limit <rate-limit>                 Set the rate limit in seconds for each target during enumeration.
-s, --screenshots <screenshots-path>
      Path to save the screenshots of the HTTP(S) website for subdomains with active ones.

  --exclude <string-exclude>...             Exclude subdomains containing specifics strings.
  --filter <string-filter>...               Filter subdomains containing specifics strings.
-t, --target <target>                       Target host.
  --threads <threads>                       Number of threads to use to perform subdomains resolution.
-u, --unique-output <unique-output>
      Write all the results for a target or a list of targets to a specified filename.

  --ua <user-agents-file>                   Path to file containing user agents strings.
-w, --wordlist <wordlists>
      Wordlist file to use in the bruteforce process. Using it option automatically enables bruteforce mode.
```

To start the enumeration process, used the below command

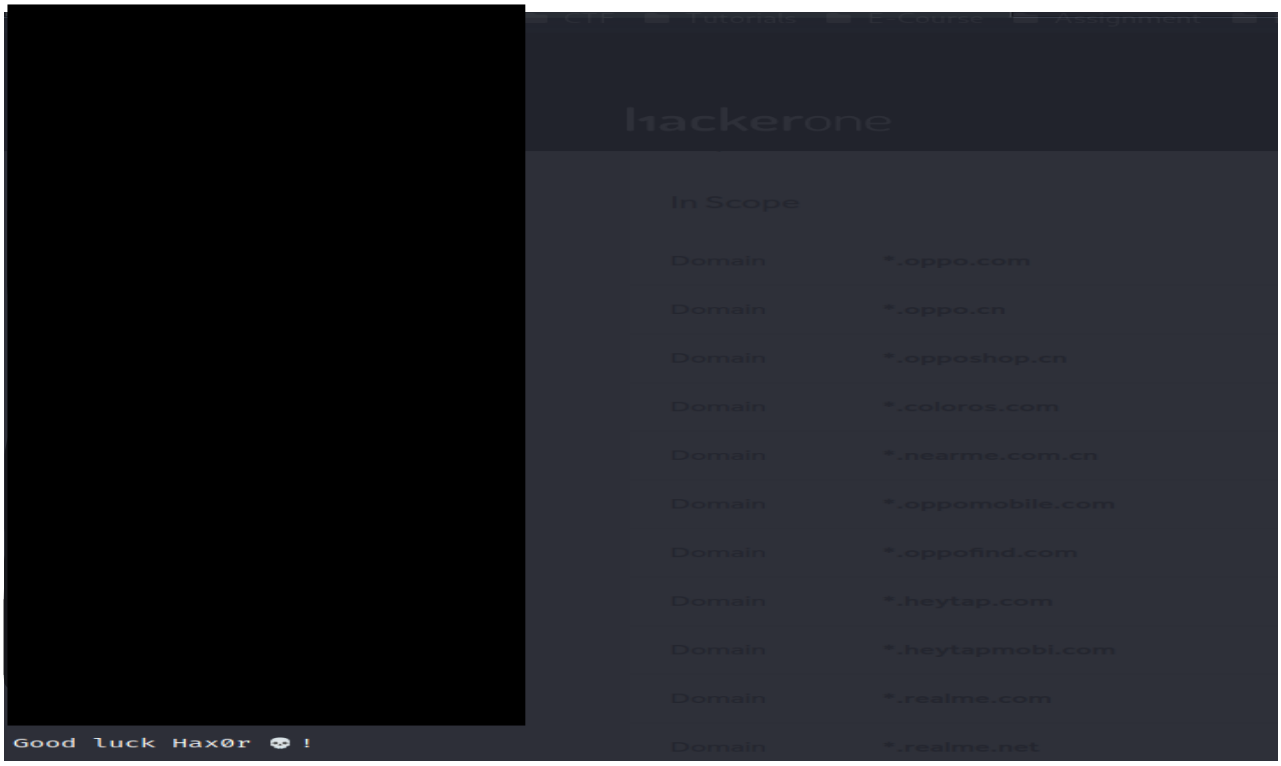
- findomain -t coloros.com

```
┌──(root💀kali)-[/home/nipun97/findomain]
└─# findomain -t coloros.com

Target ⟹ coloros.com

Searching in the CertSpotter API... 🔍
Searching in the Crtsh database API... 🔍
Searching in the Virustotal API... 🔍
Searching in the Sublist3r API... 🔍
Searching in the Facebook API... 🔍
Searching in the Spyse API... 🔍
Searching in the Bufferover API... 🔍
Searching in the AnubisDB API... 🔍
Searching in the Urlscan.io API... 🔍
Searching in the Threatcrowd API... 🔍
Searching in the Threatminer API... 🔍
Searching in the SecurityTrails API... 🔍
Searching in the Virustotal API using apikey... 🔍
Searching in the Archive.org API... 🔍
Searching in the C99 API... 🔍
Searching in the Ctsearch API... 🔍
```

- finally the results listed like this way



Note :

This tool also can concatenate with httpX and httprobe tools for gain more customized results.

5. Sublist3r

Sublist3r is a Python-based tool for enumerating subdomains of a specific website. This tool is based on the Open Source intelligence [OSINT] concept. This means that pen testers can use this tool to collect, analyze, and make decisions using freely and publicly available sources. Sublist3r primarily uses Google, Yahoo, Baidu, Bing, and Ask to enumerate subdomains, with Netcraft, Virustotal, ThreatCrowd, ReverseDNS, and DNSdumpster used in rare cases.

In recent upgrades “subbrute” tool was integrated with Sublist3r to increase the possibility of finding more subdomains using brute-force with an improved wordlist and compatibility increased to python 3 also.

Installation

URL : https://github.com/aboul3la/Sublist3r.git

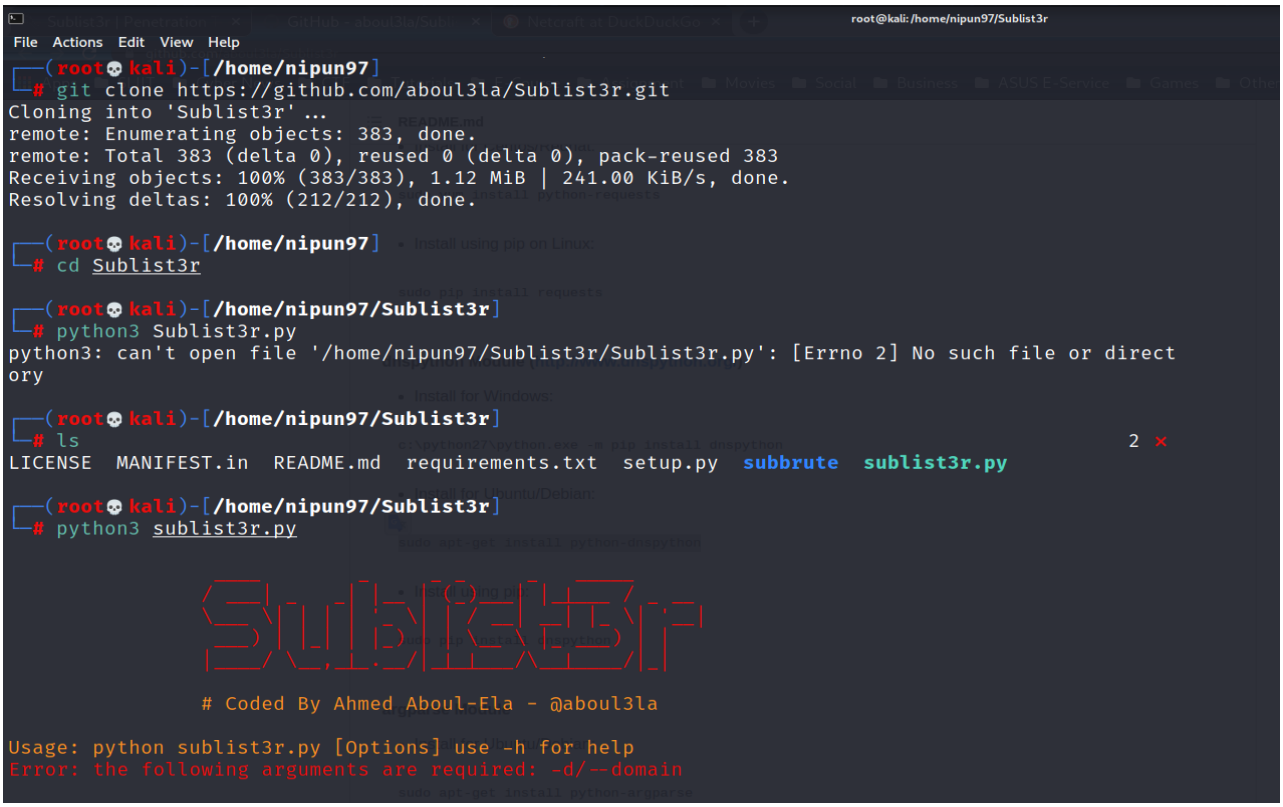
Sublist3r can be install to Linux using bellow command

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

Since this tool required additional dependencies like requests, dnspython and argparse python modules, users had to install either all dependencies at once using,

- sudo pip install -r requirements.txt

after successful GitHub cloning, I run the sublist3r.py by using python 3. Then tool interface will appear like this,

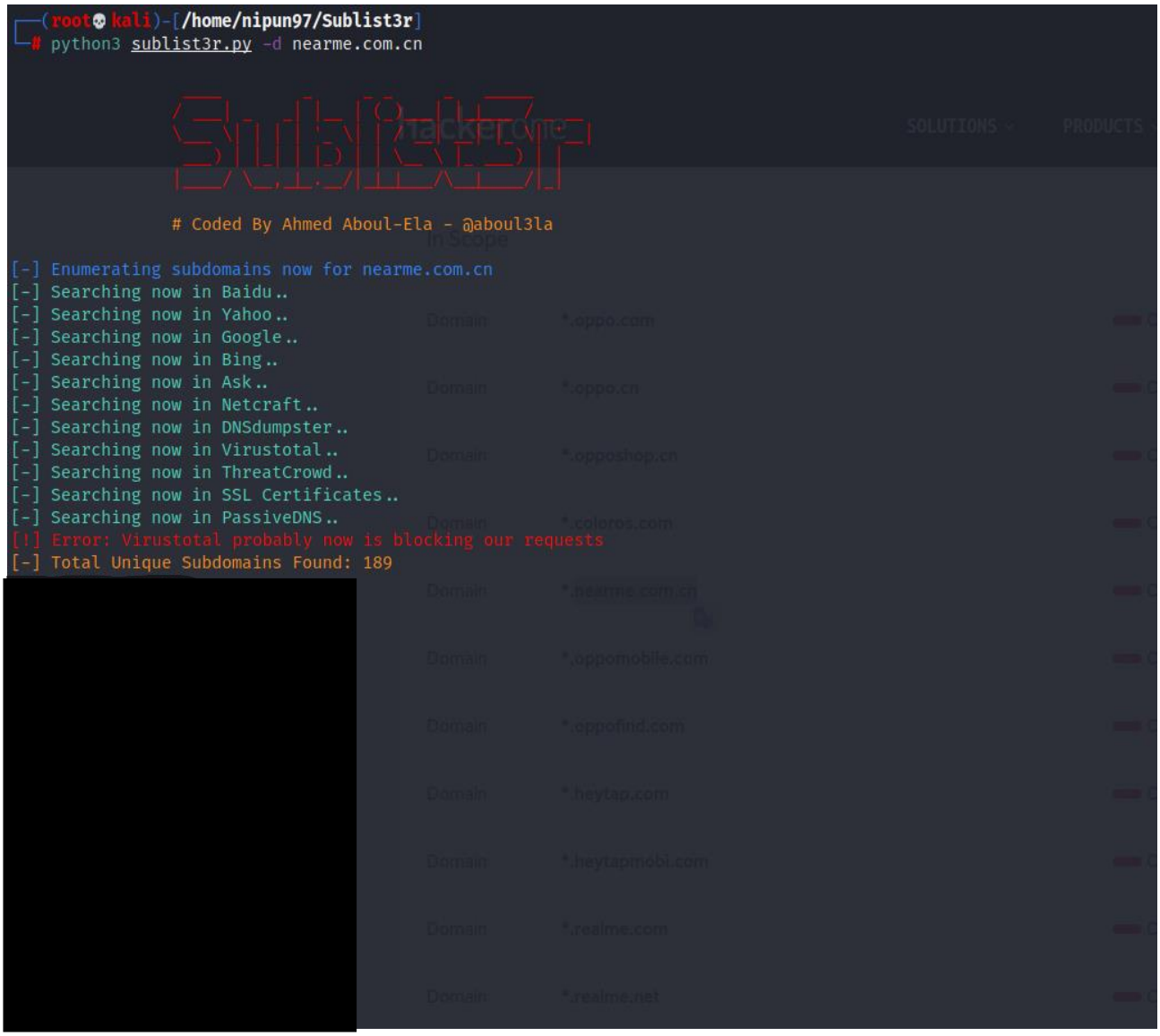


- -d flag used to specify the domain name

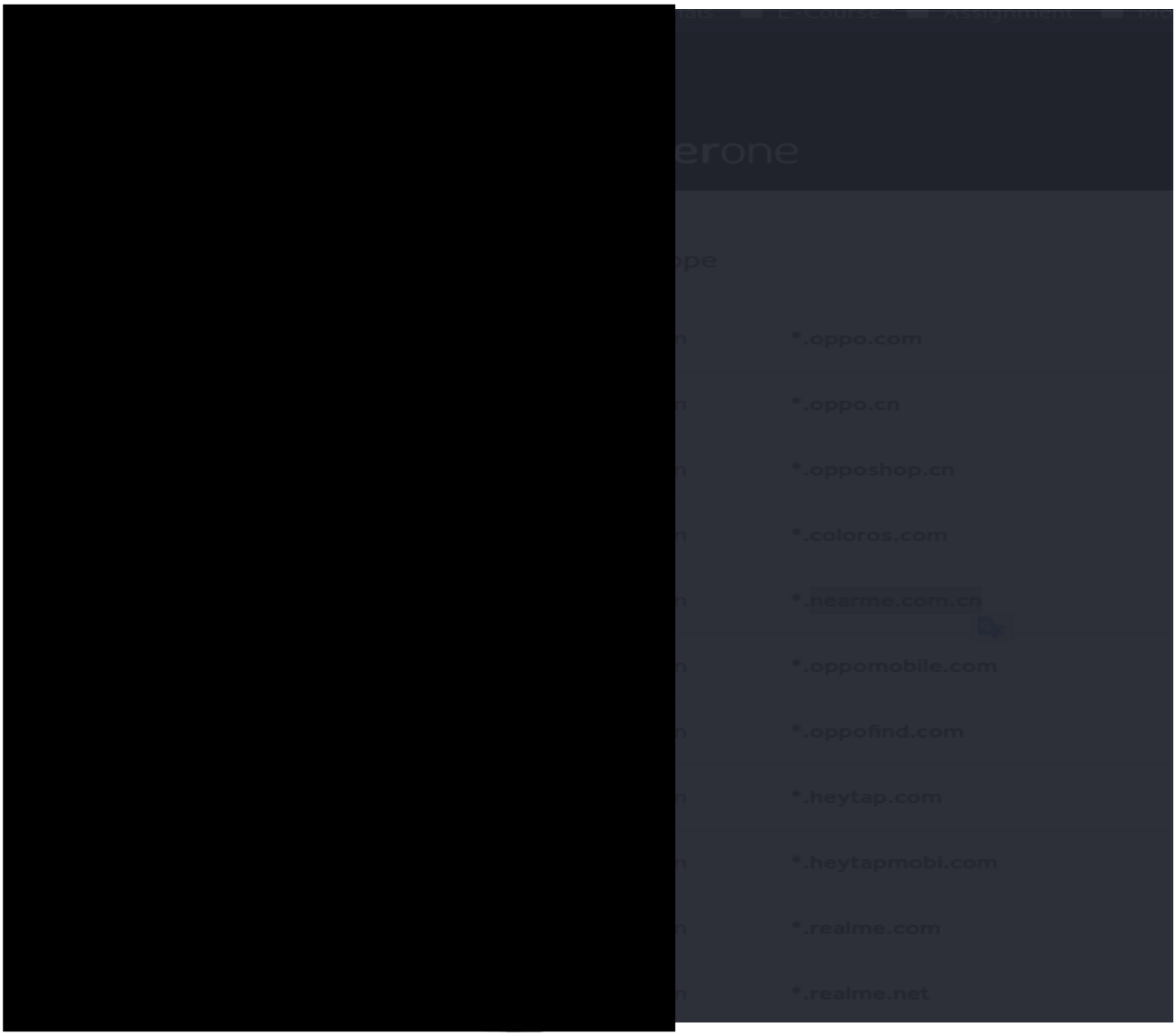
To observe the available subdomains in oppo.com, I use below command,

- python3 sublist3r.py -d opposhop.cn

After a successful scan I found 189 subdomains under the ***nearme.com.cn** domains.



- After successful enumeration final subdomains list figured as follows

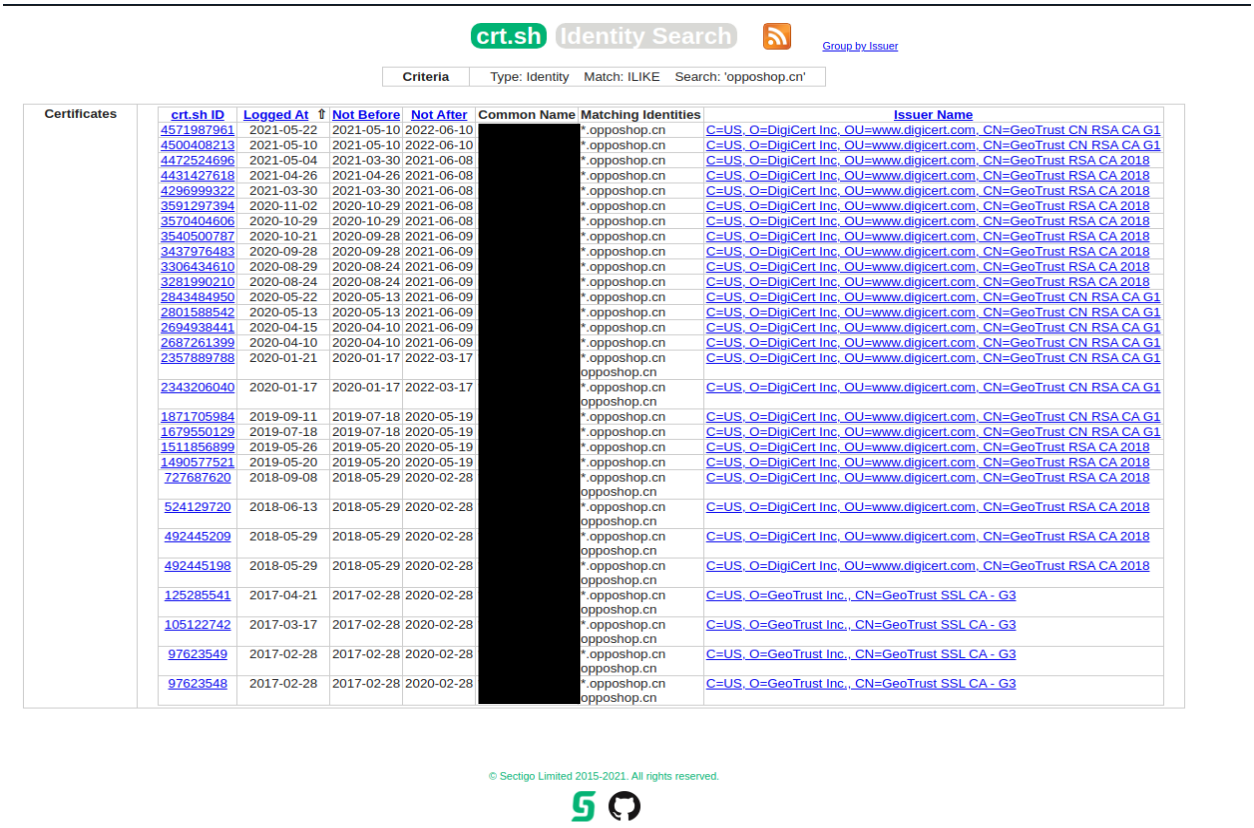


6. Crt.sh

Crt.sh is an abbreviation for "certificates.Saint Helena," and it is a website where users can find all of the SSL or TLS certificates for the specific targeted domain. To monitor the certificates, the site is open source. The site is in a graphical user interface format, and it is extremely simple to gather information. The site's goal is to keep the certificate logs as transparent as possible. Users can also access the certificate algorithms in ciphertext format.

URL : https://crt.sh/

- I used this site to find all the available subdomains for “opposhop.cn”



crt.sh Identity Search Group by Issuer

Criteria Type: Identity Match: ILIKE Search: 'opposhop.cn'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
4571987961	2021-05-22	2021-05-10	2022-06-10	[redacted]	*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust CN RSA CA G1
4500408213	2021-05-10	2021-05-10	2022-06-10		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust CN RSA CA G1
4472524696	2021-05-04	2021-03-30	2021-06-08		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
4431427618	2021-04-26	2021-04-26	2021-06-08		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
4296999322	2021-03-30	2021-03-30	2021-06-08		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
3591297394	2020-11-02	2020-10-29	2021-06-08		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
3570404606	2020-10-29	2020-10-29	2021-06-08		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
3540500787	2020-10-21	2020-09-28	2021-06-09		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
3437976483	2020-09-28	2020-09-28	2021-06-09		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
3306434610	2020-08-29	2020-08-24	2021-06-09		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
3281990210	2020-08-24	2020-08-24	2021-06-09		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
2843484950	2020-05-22	2020-05-13	2021-06-09		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust CN RSA CA G1
2801588542	2020-05-13	2020-05-13	2021-06-09		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust CN RSA CA G1
2694938441	2020-04-15	2020-04-10	2021-06-09		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust CN RSA CA G1
2687261399	2020-04-10	2020-04-10	2021-06-09		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust CN RSA CA G1
2357889788	2020-01-21	2020-01-17	2022-03-17		*.opposhop.cn opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust CN RSA CA G1
2343206040	2020-01-17	2020-01-17	2022-03-17		*.opposhop.cn opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust CN RSA CA G1
1871705984	2019-09-11	2019-07-18	2020-05-19		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust CN RSA CA G1
1679550129	2019-07-18	2019-07-18	2020-05-19		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust CN RSA CA G1
1511856899	2019-05-26	2019-05-20	2020-05-19		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
1490577521	2019-05-20	2019-05-20	2020-05-19		*.opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
727687620	2018-09-08	2018-05-29	2020-02-28		*.opposhop.cn opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
524129720	2018-06-13	2018-05-29	2020-02-28		*.opposhop.cn opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
492445209	2018-05-29	2018-05-29	2020-02-28		*.opposhop.cn opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
492445198	2018-05-29	2018-05-29	2020-02-28		*.opposhop.cn opposhop.cn	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
125285541	2017-04-21	2017-02-28	2020-02-28		*.opposhop.cn opposhop.cn	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
105122742	2017-03-17	2017-02-28	2020-02-28		*.opposhop.cn opposhop.cn	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
97623549	2017-02-28	2017-02-28	2020-02-28		*.opposhop.cn opposhop.cn	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
97623548	2017-02-28	2017-02-28	2020-02-28		*.opposhop.cn opposhop.cn	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3

- By accessing the provided list we can see the available subdomains for the given domain and subdomain SSL/TLS certificate issuer as well.

Find a live subdomain

7. Httprobe

Httprobe is a tool that searches for active http and https servers in a short period of time. If a user has a list of subdomains, he or she can use this tool to quickly determine which are active. Because this tool was created in Golang, users must be familiar with the language. To use httprobe, users must first print their list of domains and pipe them to httprobe. The following are some of httprobe's key features:

- By default, httprobe is probing for http on port 80 and https on port 443. We can add other ports by using the '-p' parameter.
- By adding '-s' parameter the default ports will be ignored.
- If user know that the response time on the target server might be high, then user can specify a custom timeout by using the '-t' parameter. The time is configured in milliseconds.
- Users can combine 'httprobe' with other tools such as 'assetfinder', 'subfinder' and etc.\

Installation

- URL : https://github.com/tomnomnom/httprobe

Using bellow commands tool can be clone to Linux with the help of GitHub

- git clone https://github.com/tomnomnom/httprobe
- cd httprobe
- go build main.go [compile executable using go]
- mv main httprobe [rename to httprobe]
- echo $path [echo the current path]
- mv httprobe /bin/ [move httprobe file to path]

```
┌──(root💀kali)-[/home/nipun97/Downloads/oppo]
└─# git clone https://github.com/tomnomnom/httprobe
Cloning into 'httprobe'...
remote: Enumerating objects: 69, done.
remote: Total 69 (delta 0), reused 0 (delta 0), pack-reused 69
Receiving objects: 100% (69/69), 15.91 KiB | 1.22 MiB/s, done.
Resolving deltas: 100% (28/28), done.

┌──(root💀kali)-[/home/nipun97/Downloads/oppo]
└─# cd httprobe

┌──(root💀kali)-[/home/nipun97/Downloads/oppo/httprobe]
└─# ls
Dockerfile  LICENSE  main.go  README.md  script

┌──(root💀kali)-[/home/nipun97/Downloads/oppo/httprobe]
└─# go build main.go

┌──(root💀kali)-[/home/nipun97/Downloads/oppo/httprobe]
└─# ls
Dockerfile  LICENSE  main  main.go  README.md  script

┌──(root💀kali)-[/home/nipun97/Downloads/oppo/httprobe]
└─# mv main httprobe

┌──(root💀kali)-[/home/nipun97/Downloads/oppo/httprobe]
└─# echo $path
/usr/local/sbin /usr/local/bin /usr/sbin /usr/bin /sbin /bin /snap/bin

┌──(root💀kali)-[/home/nipun97/Downloads/oppo/httprobe]
└─# mv httprobe /bin/
```

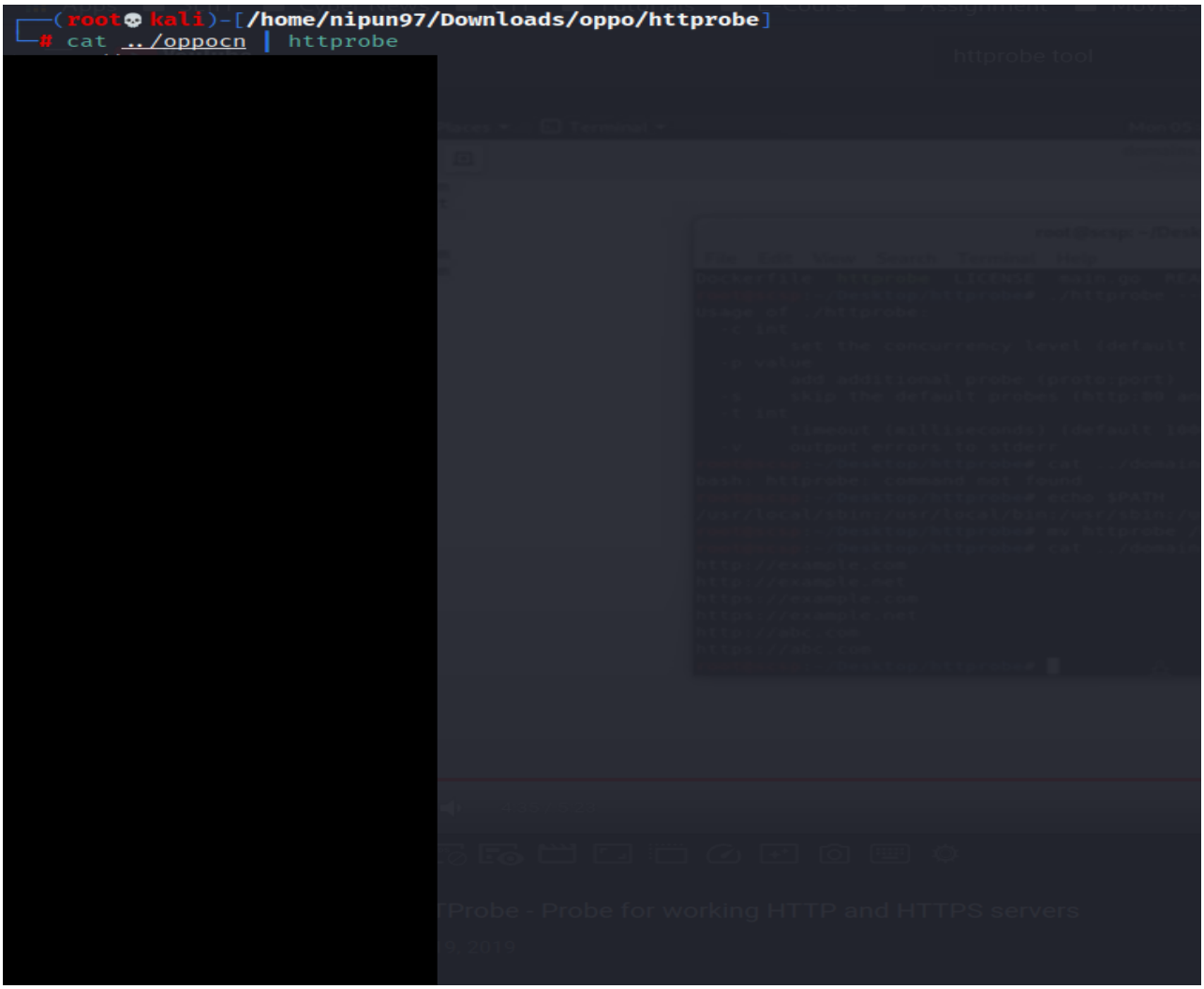
Since I stored all the enumerated subdomain into text files, I concatenate those files with httprobe to check the availability of subdomains.

I used bellow command to run a scan against the funded subdomains in ***oppo.cn**

- cat ../ oppocn | httprobe

after successful scan, all the subdomains categorized based on implemented protocol (whether HTTP or HTTPS).

Note : I run the httprobe for all 7 domains but bellow example show the results for ***oppo.cn** domain only.



.

DNS Enumeration

1. DNS Lookup

WHOIS is a protocol that is used to find the details of an internet resource such as a domain name, an IP address block or an autonomous system. This protocol is used to store the details in a database and deliver the details the database in a human readable format. Full documentation on WHOIS can be find on RFC 3912.

URL : https://whois.domaintools.com/

Once we input the domain name, site will simply produce the detailed list which contain,

- Domain owner details
- Ip address of the given domain
- Hosting server details and etc.

DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT Whois Lookup

Home > Whois Lookup > OppO.com

Whois Record for OppO.com

Domain Profile

Registrant Country	cn
Registrar	Alibaba Cloud Computing (Beijing) Co., Ltd. IANA ID: 420 URL: http://whois.aliyun.com,http://www.net.cn Whois Server: grs-whois.hichina.com domainabuse@service.aliyun.com (p) 8695187
Registrar Status	clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	8,338 days old Created on 1998-12-15 Expires on 2029-12-15 Updated on 2021-06-17
Name Servers	NS3.DNSV5.COM (has 1,030 domains) NS4.DNSV5.COM (has 1,030 domains)
Tech Contact	—
IP Address	[redacted] 3 other sites hosted on this server
IP Location	- California - Diamond Bar - Zenla-1
ASN	AS21859 ZEN-ECN, US (registered Apr 02, 2013)
Domain Status	Registered And Active Website
IP History	57 changes on 57 unique IP addresses over 16 years
Registrar History	2 registrars with 1 drop
Hosting History	12 changes on 11 unique name servers over 18 years

Website

Website Title	OPPO Official Site | OPPO Global
Server Type	NWS_Oversea_qdownload
Response Code	200
Terms	729 (Unique: 138, Linked: 405)
Images	1 (Alt tags missing: 1)
Links	149 (Internal: 148, Outbound: 1)

Whois Record (last updated on 2021-10-13)

```
Domain Name: oppo.com
Registry Domain ID: 2771331_DOMAIN_COM-VRSN
Registrar WHOIS Server: grs-whois.hichina.com
Registrar URL: http://whois.aliyun.com
Updated Date: 2021-06-17T11:23:23Z
Creation Date: 1998-12-16T05:00:00Z
Registrar Registration Expiration Date: 2029-12-16T05:00:00Z
Registrar: Alibaba Cloud Computing (Beijing) Co., Ltd.
Registrar IANA ID: 420
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Registrant City:
Registrant State/Province: Guangdong
Registrant Country: CN
Registrant Email:https://whois.aliyun.com/whois/whoisForm
Registry Registrant ID: Not Available From Registry
Name Server: NS3.DNSV5.COM
Name Server: NS4.DNSV5.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: domainabuse@service.aliyun.com
Registrar Abuse Contact Phone: +86.95187
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

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

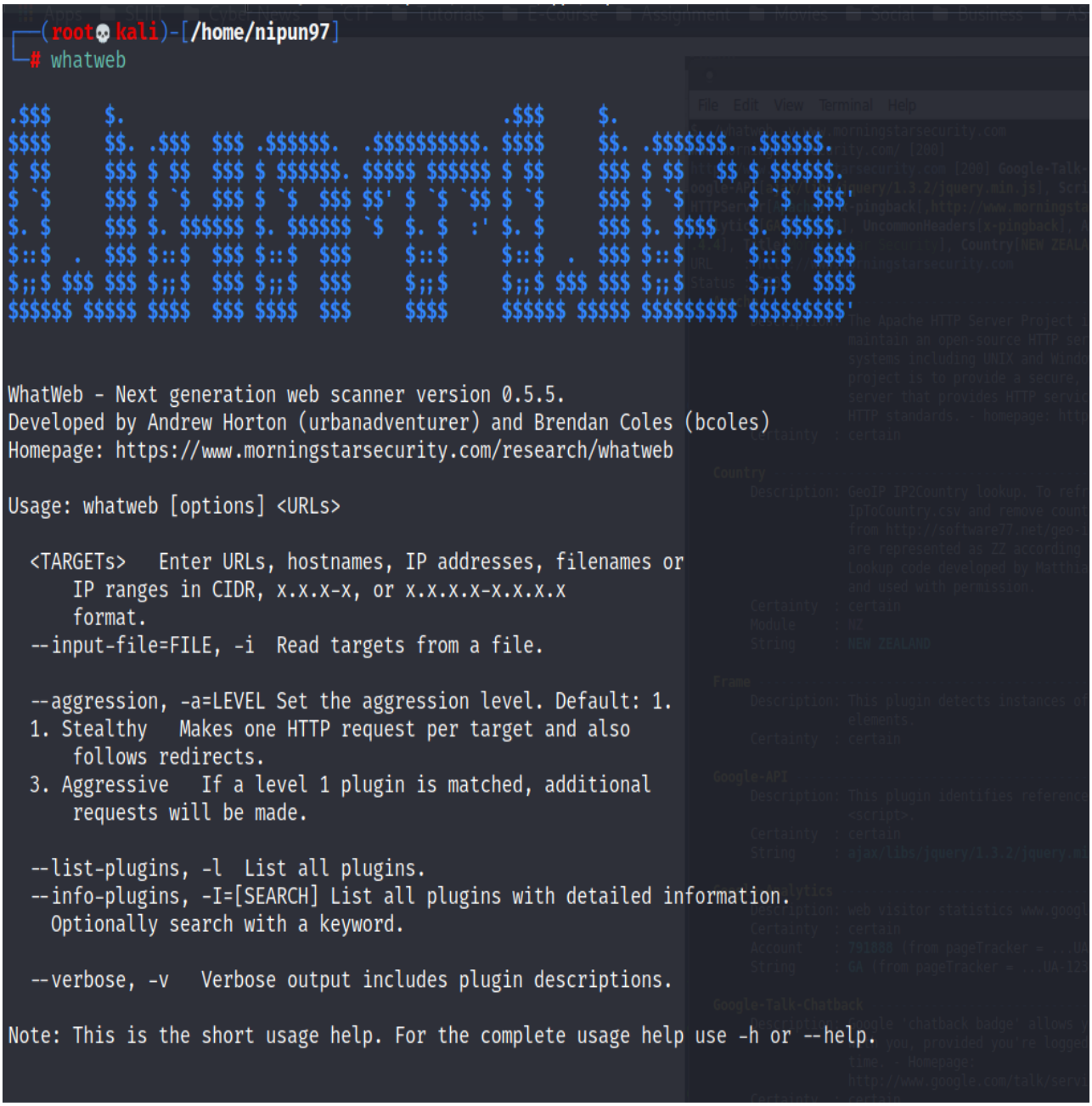
same as the ***oppo.com** I did the DNS Lookup for other 4 domains for gather basic information as well.

2. Whatweb

WhatWeb is an open source Kali Linux tool that recognizes web technologies such as content management systems (CMS), blogging platforms, statistical/analytics packages, JavaScript libraries, web servers, and embedded devices. WhatWeb has over 1700 plugins, each of which recognizes a different thing. WhatWeb can also recognize version numbers, email addresses, account IDs, web framework modules, SQL errors, and other information.

Whatweb primarily carries three types of aggressions, with the default level of aggression, known as'stealthy,' being the fastest and requiring only one HTTP request to a website. This is appropriate for scanning public websites. For use in penetration tests, more aggressive modes were developed. I've listed the key features of this tool below.

- Over 1700 plugins
- Control the tradeoff between speed/stealth and reliability
- Plugins include example URLs
- Performance tuning. Control how many websites to scan concurrently.
- Multiple log formats: Brief (greppable), Verbose (human readable), XML, JSON, MagicTree, RubyObject, MongoDB, SQL, and ElasticSearch.
- Proxy support including TOR
- Custom HTTP headers
- Basic HTTP authentication
- Control over webpage redirection
- Nmap-style IP ranges
- Fuzzy matching
- Result certainty awareness
- Custom plugins defined on the command line



Since all of domains are publicly available, I had to use default stealthy aggression mode.

I use bellow command to perform whatweb aggression for selected domains.

- whatweb -v < domain name >

```
┌──(root💀kali)-[/home/nipun97]
└─# whatweb -v oppo.com
WhatWeb report for http://oppo.com
Status    : 412 Precondition Failed
Title     : 您的访问被阻断！- 412错误
IP        : [redacted]
Country   : CHINA, CN

Summary   : HTML5, Script, HTTPServer[nginx], nginx

Detected Plugins:
[ 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 (from server string)

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


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

 Website     : http://nginx.net/

HTTP Headers:
 HTTP/1.1 412 Precondition Failed
 Server: nginx
 Date: Thu, 14 Oct 2021 08:51:21 GMT
 Content-Type: text/html
 Content-Length: 2681
 Connection: close
```

```
└─# whatweb -v oppo.cn
WhatWeb report for http://oppo.cn
Status    : 412 Precondition Failed
Title     : 您的访问被阻断！- 412错误
IP        : [redacted]
Country   : CHINA, CN

Summary   : HTML5, Script, HTTPServer[nginx], nginx

Detected Plugins:
[ 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 (from server string)

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


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

        Website     : http://nginx.net/

HTTP Headers:
        HTTP/1.1 412 Precondition Failed
        Server: nginx
        Date: Fri, 15 Oct 2021 19:05:12 GMT
        Content-Type: text/html
        Content-Length: 2681
        Connection: close
```

```
┌──(root💀kali)-[~]
└─# whatweb -v opposhop.cn
WhatWeb report for http://opposhop.cn
Status    : 412 Precondition Failed
Title     : 您的访问被阻断！- 412错误
IP        : [redacted]
Country   : CHINA, CN

Summary   : HTML5, Script, HTTPServer[nginx], nginx

Detected Plugins:
[ 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 (from server string)

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


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

        Website     : http://nginx.net/

HTTP Headers:
        HTTP/1.1 412 Precondition Failed
        Server: nginx
        Date: Fri, 15 Oct 2021 19:06:16 GMT
        Content-Type: text/html
        Content-Length: 2681
        Connection: close
```

```
┌──(root💀kali)-[~]
└─# whatweb -v coloros.com
WhatWeb report for http://coloros.com
Status    : 301 Moved Permanently
Title     : <None>
IP        : [redacted]
Country   : UNITED STATES, US

Summary   : RedirectLocation[http://www.coloros.com], HTTPServer[DNSPod URL V2.0]

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

        String       : DNSPod URL V2.0 (from server string)

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : http://www.coloros.com (from location)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Server: DNSPod URL V2.0
        Content-Length: 0
        Connection: close
        Date: Fri, 15 Oct 2021 19:07:20 GMT
        Cache-Control: max-age=600
        Expires: Fri, 15 Oct 2021 19:17:20 GMT
        Location: http://www.coloros.com

WhatWeb report for http://www.coloros.com
Status    : 412 Precondition Failed
Title     : 您的访问被阻断！- 412错误
IP        : [redacted]
Country   : CHINA, CN
```

```
Summary   : HTML5, Script, HTTPServer[nginx], nginx

Detected Plugins:
[ 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 (from server string)

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


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

        Website     : http://nginx.net/

HTTP Headers:
        HTTP/1.1 412 Precondition Failed
        Server: nginx
        Date: Fri, 15 Oct 2021 19:07:22 GMT
        Content-Type: text/html
        Content-Length: 2681
        Connection: close
```

```
┌──(root💀kali)-[~]
└─# whatweb -v nearme.com.cn
WhatWeb report for http://nearme.com.cn
Status    : 412 Precondition Failed
Title     : 您的访问被阻断！- 412错误
IP        : [redacted]
Country   : CHINA, CN

Summary   : HTML5, Script, HTTPServer[nginx], nginx

Detected Plugins:
[ 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 (from server string)

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


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

        Website     : http://nginx.net/

HTTP Headers:
        HTTP/1.1 412 Precondition Failed
        Server: nginx
        Date: Fri, 15 Oct 2021 19:10:01 GMT
        Content-Type: text/html
        Content-Length: 2681
        Connection: close
```

```
┌──(root💀kali)-[~]
└─# whatweb -v oppomobile.com
WhatWeb report for http://oppomobile.com
Status    : 412 Precondition Failed
Title     : 您的访问被阻断！- 412错误
IP        : [redacted]
Country   : CHINA, CN

Summary   : HTML5, Script, HTTPServer[nginx], nginx

Detected Plugins:
[ 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 (from server string)

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


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

        Website     : http://nginx.net/

HTTP Headers:
        HTTP/1.1 412 Precondition Failed
        Server: nginx
        Date: Fri, 15 Oct 2021 19:11:09 GMT
        Content-Type: text/html
        Content-Length: 2681
        Connection: close
```

```
┌──(root💀kali)-[~]
└─# whatweb -v oppofind.com
WhatWeb report for http://oppofind.com
Status    : 412 Precondition Failed
Title     : 您的访问被阻断！- 412错误
IP        : [redacted]
Country   : CHINA, CN

Summary   : HTML5, Script, HTTPServer[nginx], nginx

Detected Plugins:
[ 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 (from server string)

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


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

        Website     : http://nginx.net/

HTTP Headers:
        HTTP/1.1 412 Precondition Failed
        Server: nginx
        Date: Fri, 15 Oct 2021 19:12:11 GMT
        Content-Type: text/html
        Content-Length: 2681
        Connection: close
```

3. NS Lookup and Dig

Nslookup (name server lookup) is a useful for retrieving information from a DNS server. It is a network administration tool that queries the Domain Name System (DNS) to obtain domain name or IP address mapping information, as well as any other specific DNS record. It is also used to troubleshoot DNS issues.

Installation

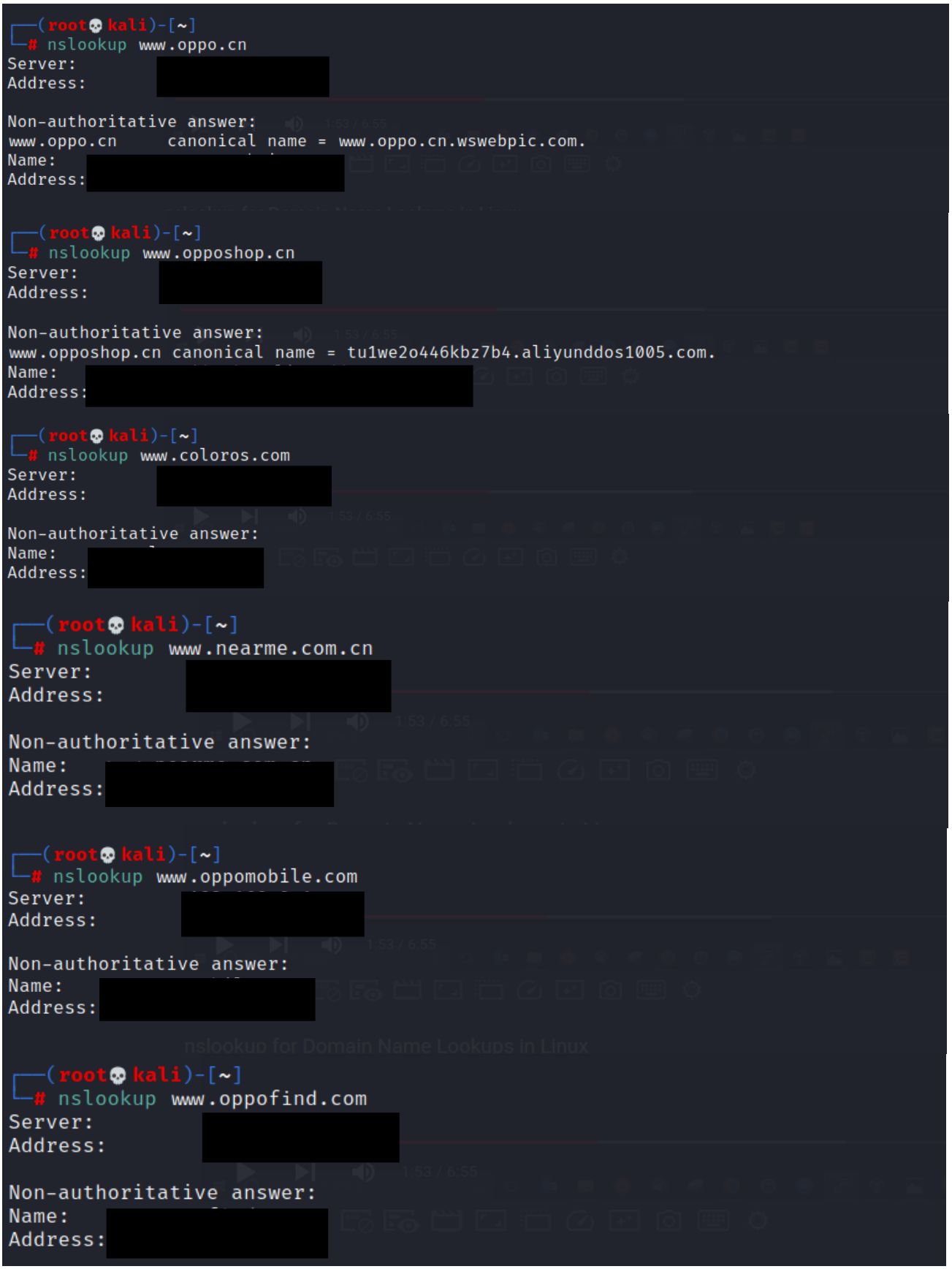
Since, “dig” is a command, Installation of NS Lookup can be done by using “apt” store.

```
┌──(root💀kali)-[~]
└─# apt-get install dnsutils
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  dnsutils
0 upgraded, 1 newly installed, 0 to remove and 950 not upgraded.
Need to get 255 kB of archives.
After this operation, 267 kB of additional disk space will be used.
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 dnsutils all 1:9.16.15-1 [255 kB]
Fetched 255 kB in 3s (84.3 kB/s)
Selecting previously unselected package dnsutils.
(Reading database ... 273764 files and directories currently installed.)
Preparing to unpack .../dnsutils_1%3a9.16.15-1_all.deb ...
Unpacking dnsutils (1:9.16.15-1) ...
Setting up dnsutils (1:9.16.15-1) ...
```

bellow snaps shows the results of each domain.

```
┌──(root💀kali)-[~]
└─# nslookup www.oppo.com
Server:
Address:

Non-authoritative answer:
www.oppo.com    canonical name = www.oppo.com.cdnx2.com.
www.oppo.com.cdnx2.com  canonical name = www.oppo.com.qdownload2.sched.ovscdns.com.
Name:
Address:
Name:
Address:
Name:
Address:
Name:
Address:
Name:
Address:
Name:
Address:
Name:
Address:
Name:
Address:
Name:
Address:
Name:
Address:
Name:
Address:
Name:
Address:
Name:
Address:
Name:
Address:
Name:
Address:
Name:
Address:
```


┌──(root💀kali)-[~]
└─# nslookup www.oppo.cn
Server:
Address:
Non-authoritative answer:
www.oppo.cn canonical name = www.oppo.cn.wswebpic.com.
Name:
Address:
┌──(root💀kali)-[~]
└─# nslookup www.opposhop.cn
Server:
Address:
Non-authoritative answer:
www.opposhop.cn canonical name = tu1we2o446kbz7b4.aliyunddos1005.com.
Name:
Address:
┌──(root💀kali)-[~]
└─# nslookup www.coloros.com
Server:
Address:
Non-authoritative answer:
Name:
Address:
┌──(root💀kali)-[~]
└─# nslookup www.nearme.com.cn
Server:
Address:
Non-authoritative answer:
Name:
Address:
┌──(root💀kali)-[~]
└─# nslookup www.oppomobile.com
Server:
Address:
Non-authoritative answer:
Name:
Address:
┌──(root💀kali)-[~]
└─# nslookup www.oppofind.com
Server:
Address:
Non-authoritative answer:
Name:
Address:

The “dig” command in Linux is used to gather DNS information. It stands for Domain Information Groper, and it collects data about Domain Name Servers. The “dig” command is helpful for diagnosing DNS problems, but is also used to display DNS information but in this time, it wasn’t provided much of an information about the target.

Gathering Achieved Information

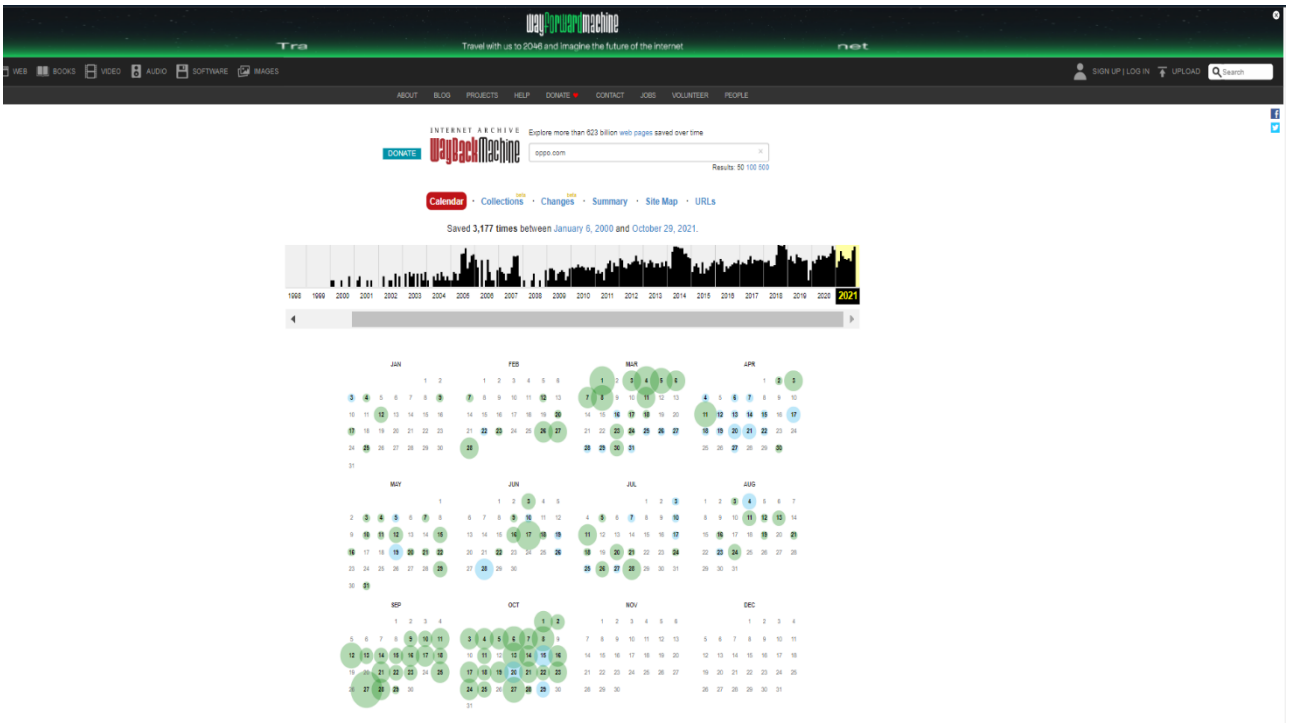
1. Wayback machine

URL : https://web.archive.org/

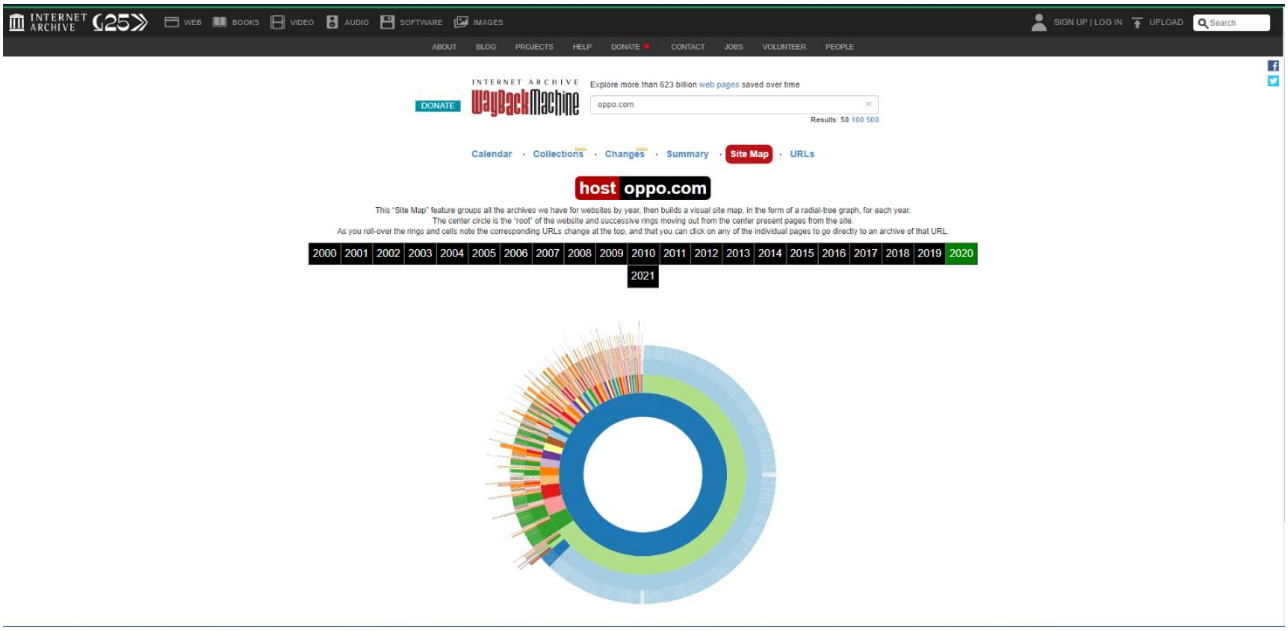
Brewster Kahle and Bruse Gillit funded the Wayback Machine, a digital archiver. It was first made available to the public in 2001, and it allows users to go "back in time" and see how websites looked in the past. Wayback Machine currently has over 613 billion archived web pages. So far, it has been designed to provide "universal access to all knowledge" by archiving copies of defunct web pages.

This site is very helpful for information gathering because, when it crawls, it finds some interesting data. Like,

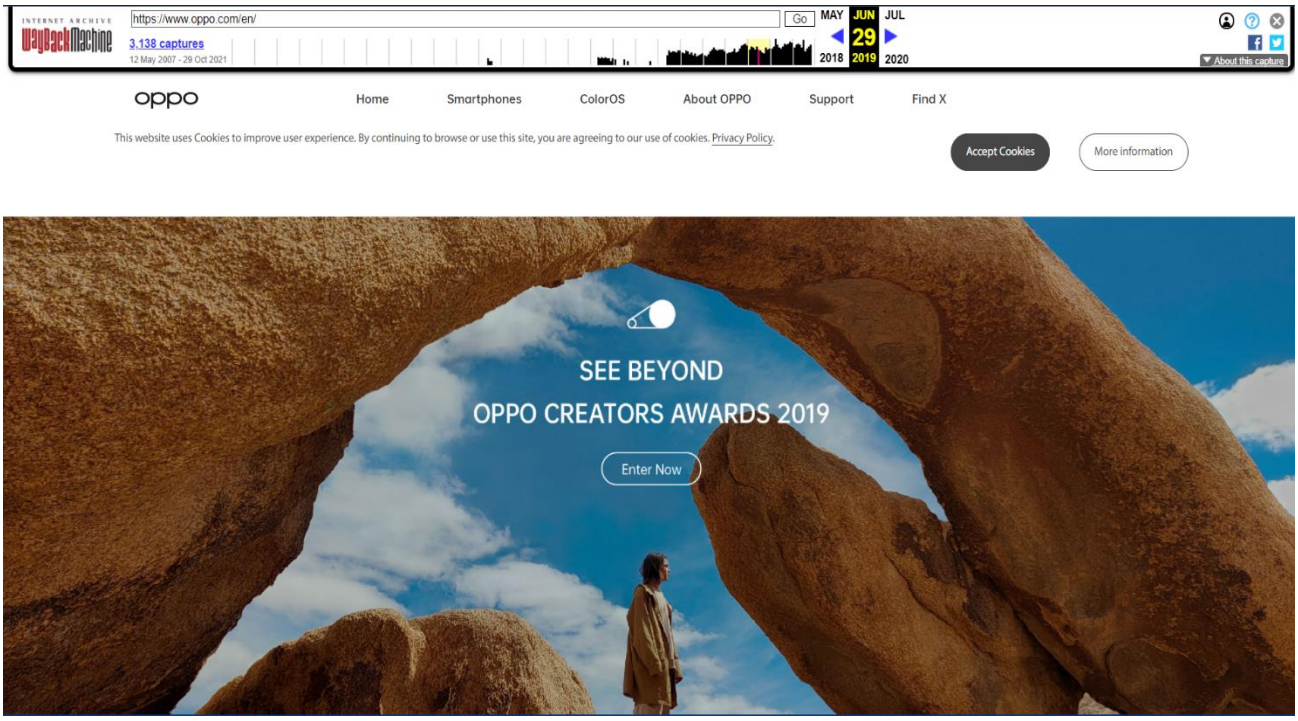
- Implemented new technologies
- Old forgotten endpoints
- Sensitive information (including JS files, php files)

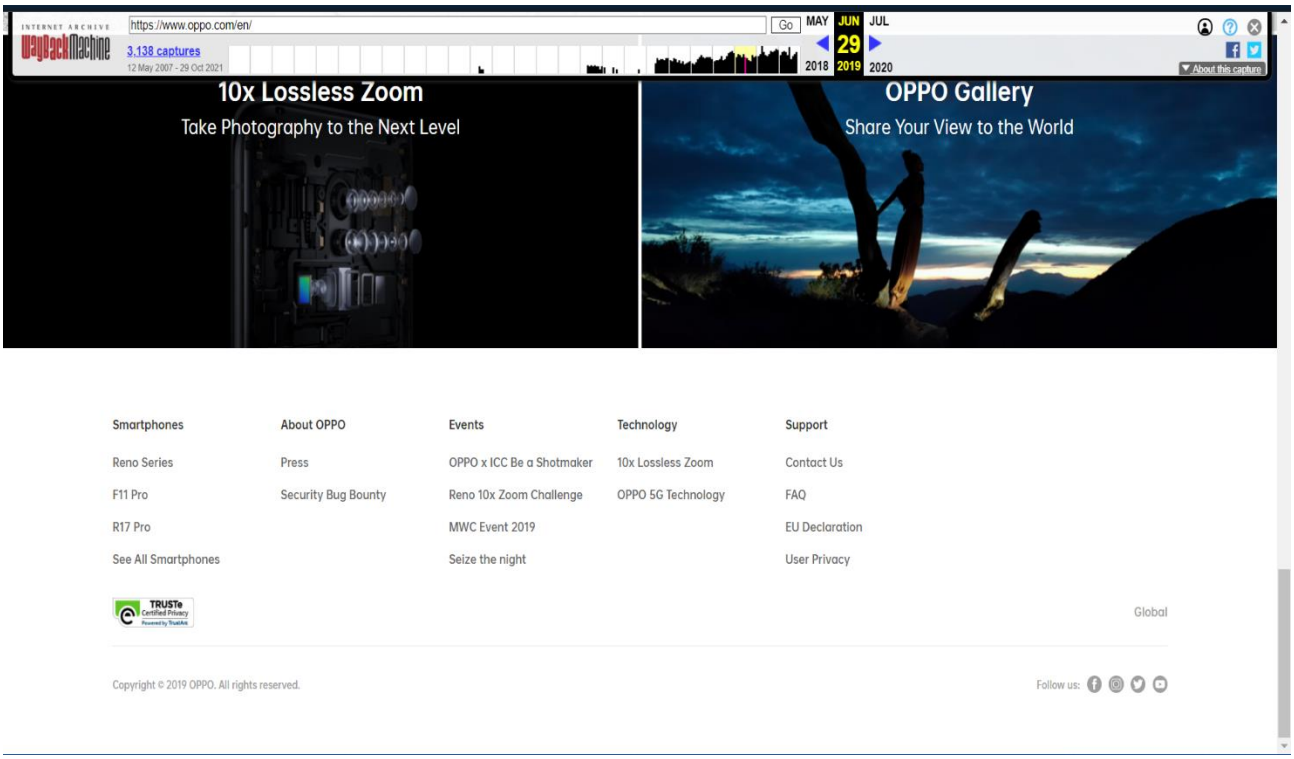


Under the site map, we can see the available subdomains and how the modified over the time.



Below snap shows how the oppo.com was appeared in 2019.





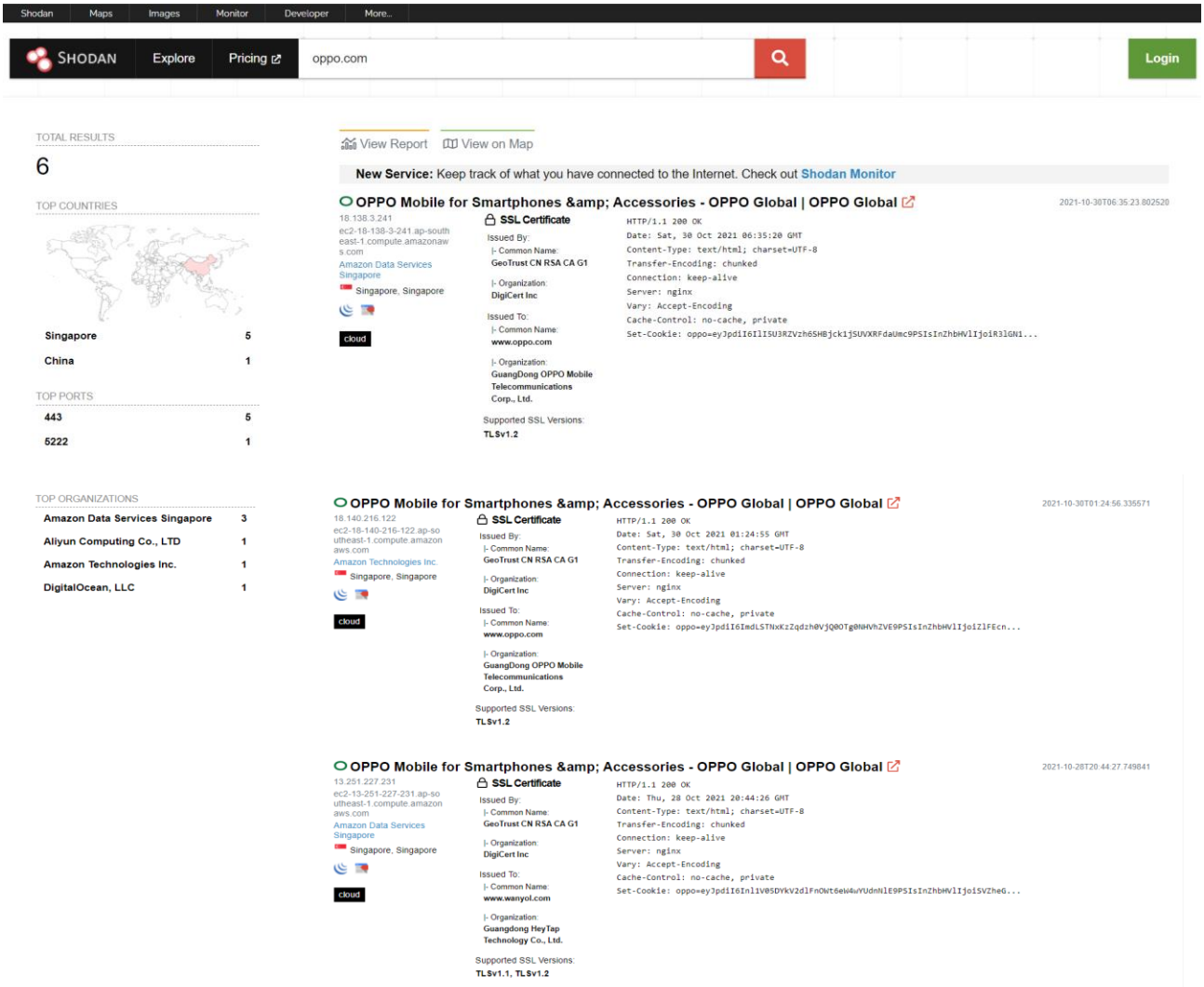
Same as I performed, wayback archive information gathering for other domains as well.

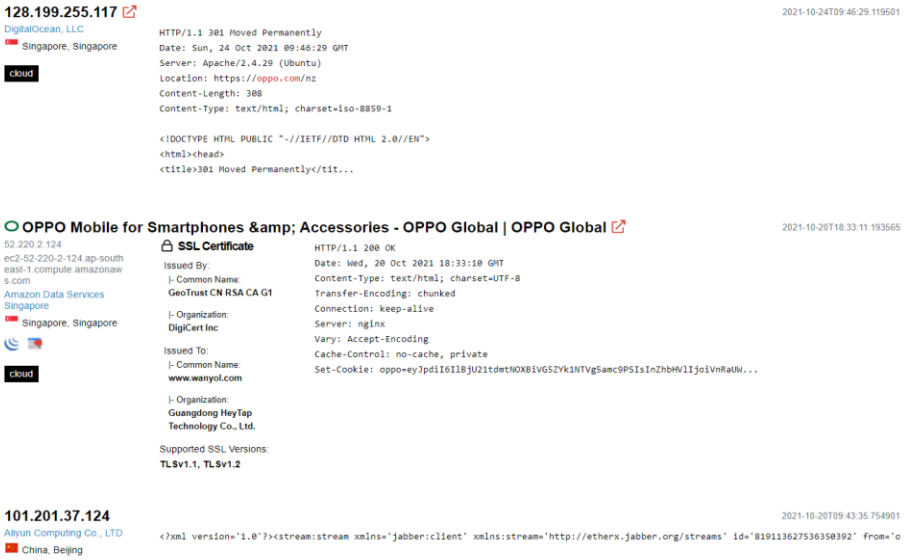
Public Device Enumeration

1. Shodan

URL : https://www.shodan.io/

Shodan is an internet-connected device search engine. Shodan, in essence, collects information about all devices that are directly connected to the Internet. When a device is directly connected to the Internet, Shodan queries it for a variety of publicly available information. If the target domain exposes any public IP address service on a specific port, it will be listed in Shodan. Not only can we obtain the IP address, but we can also obtain web server details, banners, Internet provider, Secure shell, File transfer protocol, and so on.





using this website, I performed same action for other domains as well.

Vulnerability Analyzing Phrase

OWASP Top 10 Security Risks and Vulnerabilities 2021

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. So, I used OWSAP top 10 list to identify the available vulnerabilities in the targeted domains.

- A01_2021-Broken_Access_Control/
- A02_2021-Cryptographic_Failures/
- A03_2021-Injection/
- A04_2021-Insecure_Design/
- A05_2021-Security_Misconfiguration/
- A06_2021-Vulnerable_and_Outdated_Components/
- A07_2021-Identification_and_Authentication_Failures/
- A08_2021-Software_and_Data_Integrity_Failures/

- A09_2021-Security_Logging_and_Monitoring_Failures/
- A10_2021-Server-Side_Request_Forgery_

1. Legion

Legion is an open source, user-friendly, super-extensible, and semi-automated network penetration testing tool that aids in information system discovery, reconnaissance, and exploitation. This tool integrated with NMAP, Shodan, whataweb, nikto, Vulners, Hydra, SMBenum, dirbuster, sslyzer, webslayer, and other tools automate recon and scanning (with almost 100 auto-scheduled scripts). Here are the some key features,

- Legion is Simple to use, Pentesters can quickly find and exploit attack vectors on hosts thanks to a graphical interface with rich context menus and panels.
- Users can easily customize Legion and automatically call their own scripts/tools using the modular functionality.
- Stage scanning with a high degree of customization for ninja-like IPS evasion CPEs (Common Platform Enumeration) and CVEs are automatically detected (Common Vulnerabilities and Exposures) and Project results.
- Tasks are automatically saved in real time.

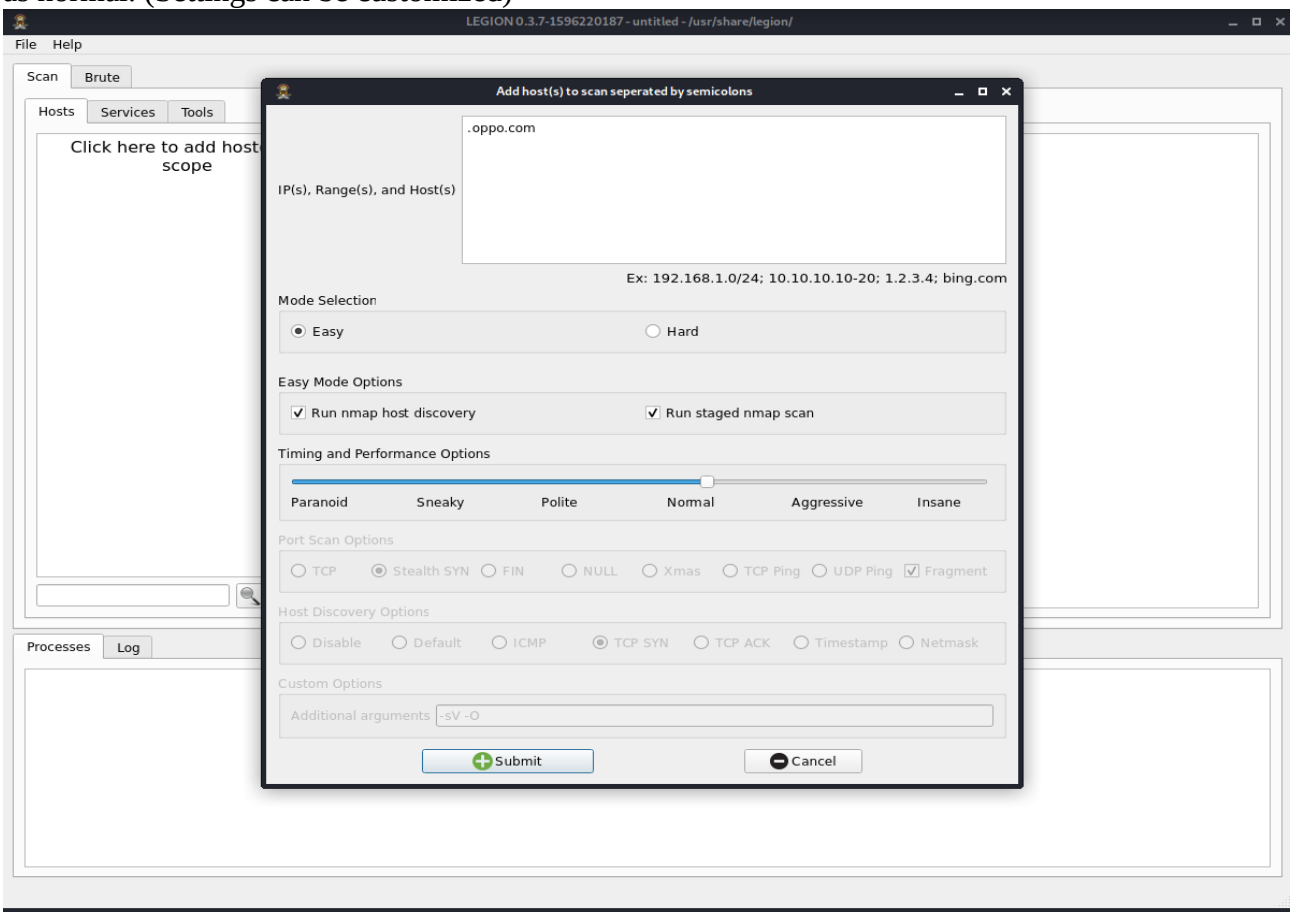
Installation

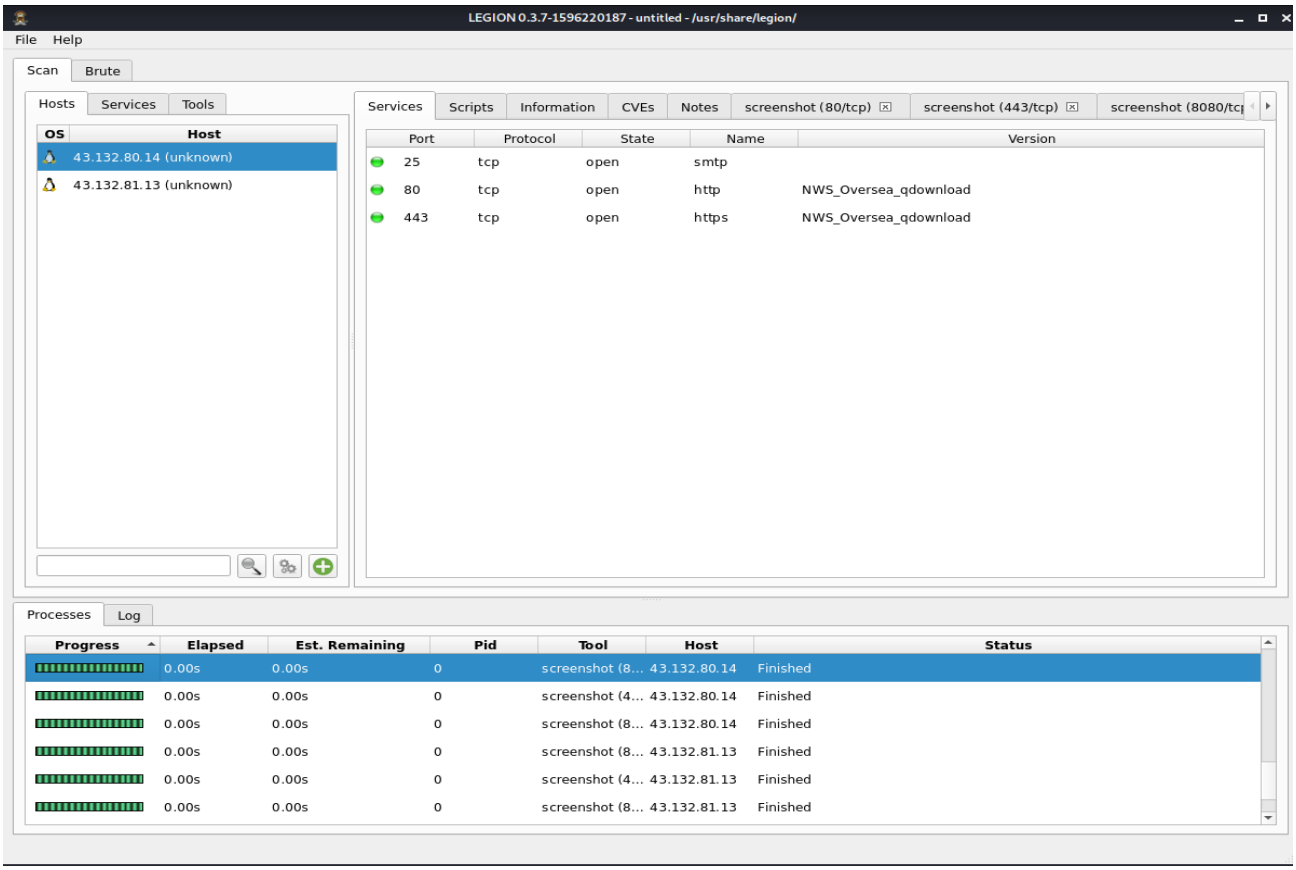
Legion tool also comes with as built in Kali Linux. Same as this tool can be install using apt store as well.

```
sudo apt install legion
```

after lunching the tool, it will look like as bellows,

then I input the domain name to perform the scan. Initially, I set the mode as easy and performance as normal. (Settings can be customized)





after few rounds of scanning, tool provide the open ports details and basic information about the domain, but it fails to identify the any basic vulnerabilities.

2. Nikto

Nikto is an Open-Source tool. which can be used as web server scanner and it runs tests against known vulnerabilities on web servers for a range of things, likes potentially hazardous file system, outdated versions of over servers, and version-specific problems on servers. Nikto also identify the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Here are some key features,

- Checks database in CSV format that is easily updatable
- Reports can be output in plain text or HTML, with automatic switching between HTTP versions.

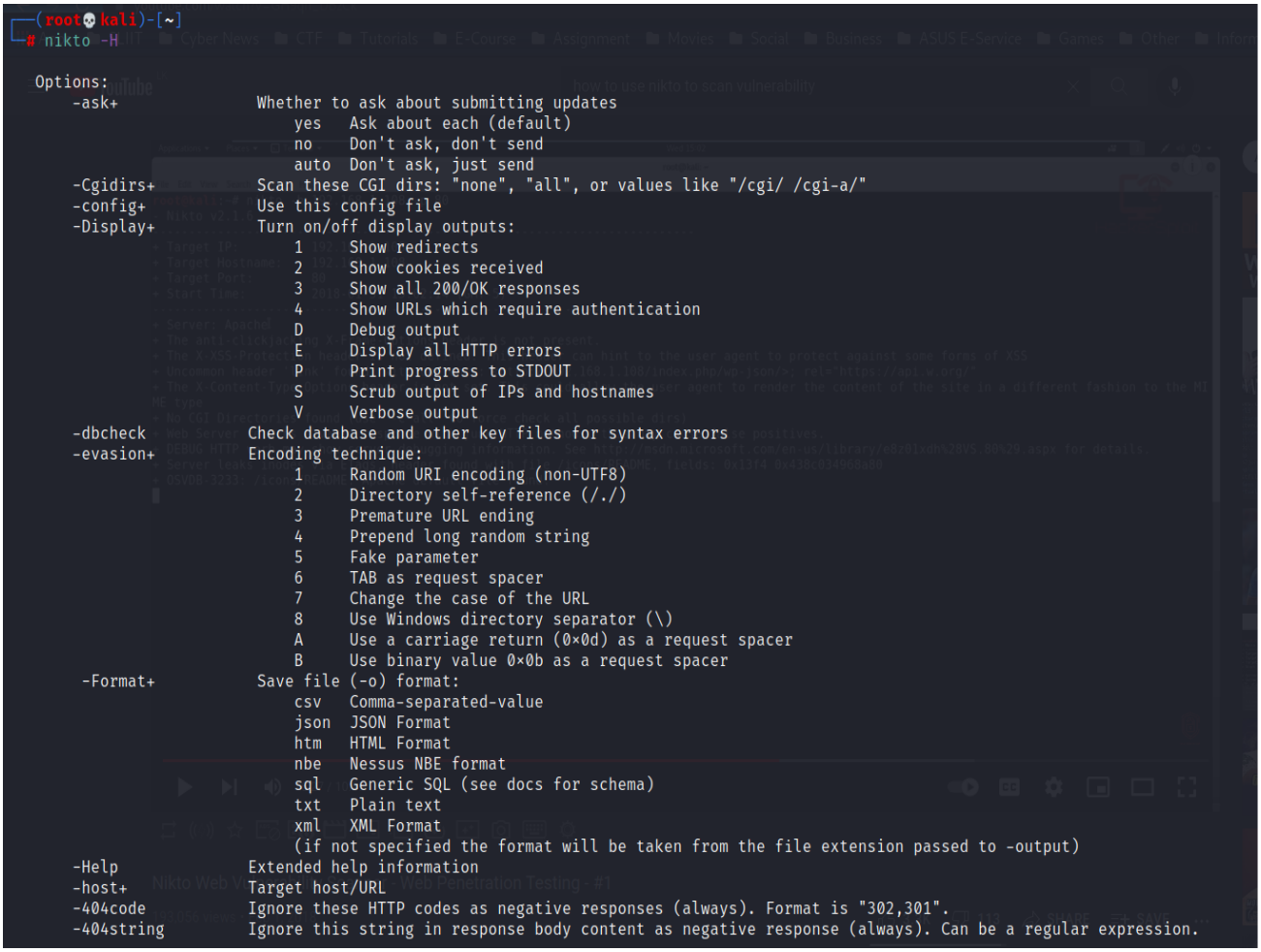
- Server software checks, both generic and specific
- SSL compatibility (through libnet-ssleay-perl)
- Proxy assistance (with authentication)
- Cookies are accepted.

Installation

Nikto tool also comes with as built in Kali Linux. Same as this tool can be install using apt store as well.

sudo apt install nikto

after lunching the tool with flag -h, it will show the available options as bellows,



```
    -id+                Host authentication to use, format is id:pass or id:pass:realm
    -key+               Client certificate key file
    -list-plugins       List all available plugins, perform no testing
    -maxtime+           Maximum testing time per host (e.g., 1h, 60m, 3600s)
    -mutate+            Guess additional file names:
                             1     Test all files with all root directories
                             2     Guess for password file names
                             3     Enumerate user names via Apache (/~user type requests)
                             4     Enumerate user names via cgiwrap (/cgi-bin/cgiwrap/~user type requests)
                             5     Attempt to brute force sub-domain names, assume that the host name is the parent domain
                             6     Attempt to guess directory names from the supplied dictionary file
    -mutate-options     Provide information for mutates
    -nointeractive      Disables interactive features
    -nolookup           Disables DNS lookups
    -nossl              Disables the use of SSL
    -no404              Disables nikto attempting to guess a 404 page
    -Option             Over-ride an option in nikto.conf, can be issued multiple times
    -output+            Write output to this file ('.' for auto-name)
    -Pause+             Pause between tests (seconds, integer or float)
    -Plugins+           List of plugins to run (default: ALL)
    -port+              Port to use (default 80)
    -RSAcert+           Client certificate file
    -root+              Prepend root value to all requests, format is /directory
    -Save               Save positive responses to this directory ('.' for auto-name)
    -ssl                Force ssl mode on port
    -Tuning+            Scan tuning:
                             1     Interesting File / Seen in logs
                             2     Misconfiguration / Default File
                             3     Information Disclosure
                             4     Injection (XSS/Script/HTML)
                             5     Remote File Retrieval - Inside Web Root
                             6     Denial of Service
                             7     Remote File Retrieval - Server Wide
                             8     Command Execution / Remote Shell
                             9     SQL Injection
                             0     File Upload
                             a     Authentication Bypass
                             b     Software Identification
                             c     Remote Source Inclusion
                             d     WebService
                             e     Administrative Console
                             x     Reverse Tuning Options (i.e., include all except specified)
    -timeout+           Timeout for requests (default 10 seconds)
    -Userdbs            Load only user databases, not the standard databases
                             all   Disable standard dbs and load only user dbs
```

then I perform some scans with basic as well as advance configurations, but tool doesn't provide much accurate results.

```
┌──(root💀kali)-[~]
└─# nikto -h www.oppo.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          [redacted]
+ Target Hostname:    [redacted]
+ Target Port:        80
+ Message:           Multiple IP addresses found: [redacted]
+ Start Time:         2021-10-16 01:31:28 (GMT5.5)
---------------------------------------------------------------------------
+ Server: NWS_Oversea_qdownload
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ Root page / redirects to: https://www.oppo.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7897 requests: 8 error(s) and 3 item(s) reported on remote host
+ End Time:           2021-10-16 01:52:22 (GMT5.5) (1254 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(root💀kali)-[~]
└─# nikto -h www.oppo.cn
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          [redacted]
+ Target Hostname:    [redacted]
+ Target Port:        80
+ Start Time:         2021-10-16 02:07:27 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-ws-request-id' found, with contents: 6169e688_xiaogan43_21537-7798
+ Uncommon header 'x-via' found, with contents: 1.1 xg29:6 (Cdn Cache Server V2.0)
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  20 error(s) and 5 item(s) reported on remote host
+ End Time:           2021-10-16 02:09:25 (GMT5.5) (118 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

3. Netsparker

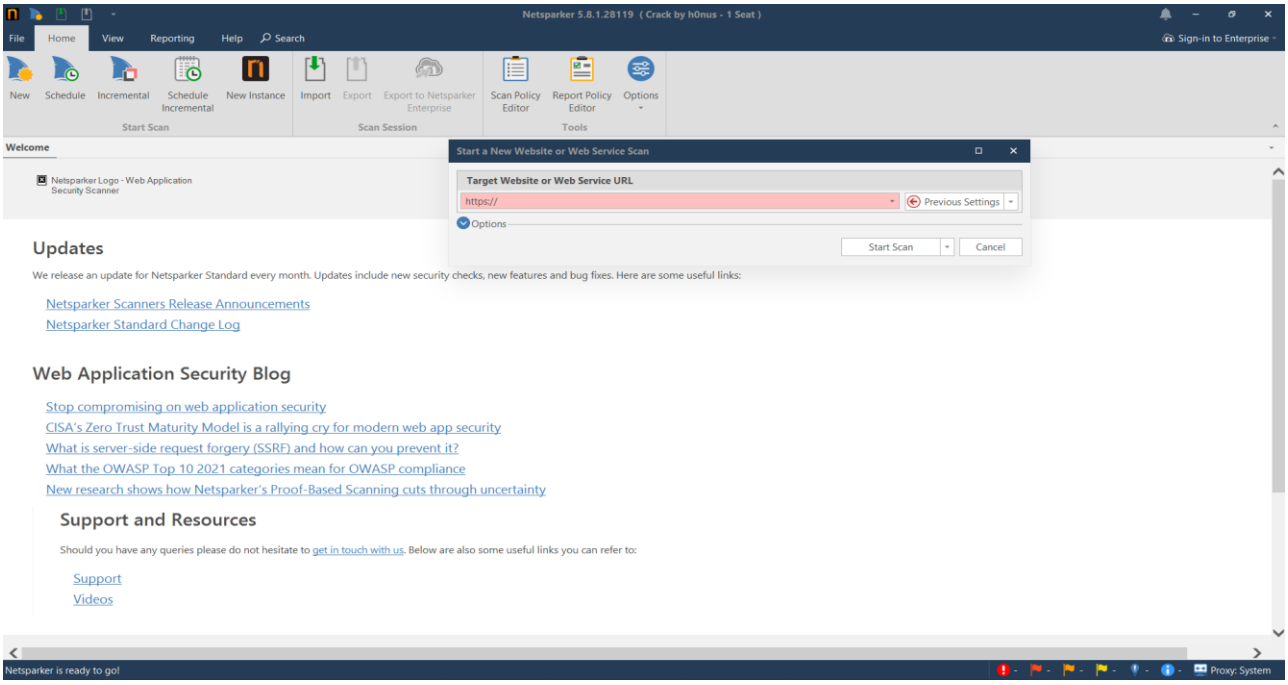
Netsparker is a commercial, fully automated web application security scanner. It scans websites, web applications, and web services, and identify security flaws. This tool is an online web application security scanner that automatically exploits identified vulnerabilities in a read-only and safe way, in order to confirm identified issues. Below are some key features of the Netsparker tool.

- Highly accurate
- Proof- based scanning
- Proof of concept
- Proof of exploit
- Fully details reporting

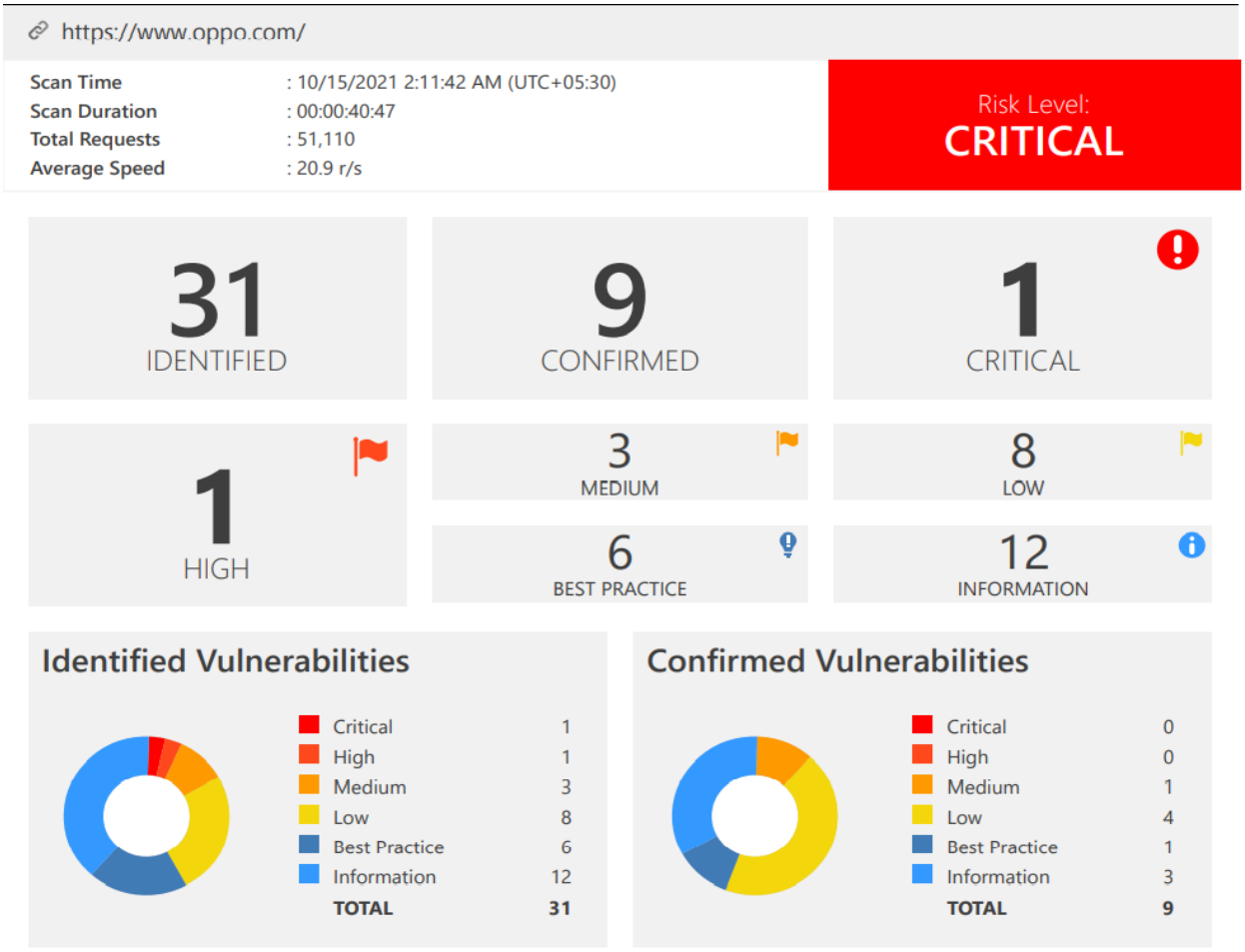
Installation

In order to perform real time, accurate scanning, users need to purchase the Netsparker pro versions.

URL : https://www.netsparker.com/



1. Target Domain: **https://www.oppo.com/**



A. Out-of-date Version (Lodash)

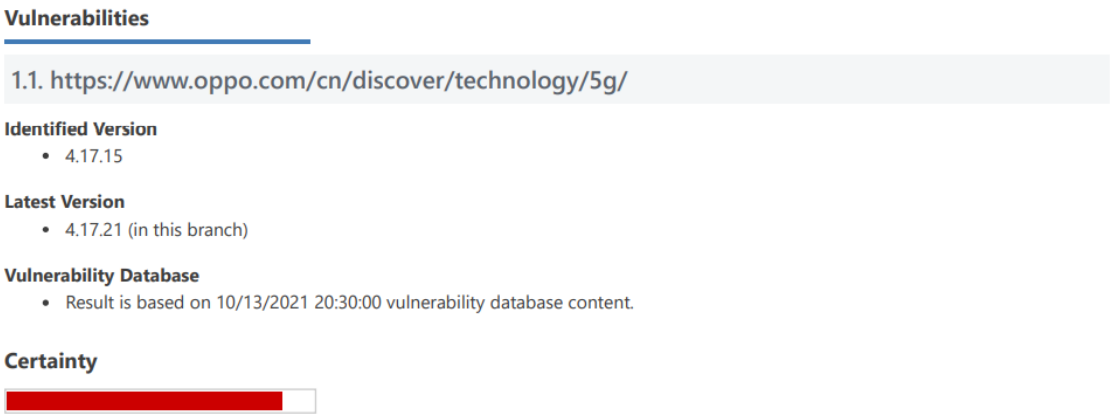
Severity : Critical
Method : GET
OWASP : No 06 Type

Impact

Because this is an older version of the software, it could be vulnerable to attacks. Improper Neutralization of Special Elements in a Command ('Command Injection') by Lodash Vulnerability All versions of the lodash package; all versions of the org.fujion.webjars:lodash package are vulnerable to Command Injection via template.

Affected Versions - 4.17.9 to 4.17.20

External References - CVE-2021-23337



Lodash Other Vulnerability

- Lodash versions prior to 4.17.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the toNumber, trim and trimEnd functions.
- **Lodash Prototype Pollution (CVE-2020-28500)**

  Affected versions of this package are vulnerable to Prototype Pollution in zipObjectDeep due to an incomplete fix for CVE-2020-8203. https://snyk.io/vuln/SNYK-JS-LODASH-590103

  Affected Versions (4.17.9 to 4.17.20)
- **Lodash Prototype Pollution**

  Affected versions of this package are vulnerable to Prototype Pollution via the setWith and set functions.https://snyk.io/vuln/SNYKJS-LODASH-608086

  Affected Versions (0.1.0 to 4.17.19)
- **Lodash Prototype Pollution**

  Affected versions of this package are vulnerable to Prototype Pollution via the setWith and set functions.https://snyk.io/vuln/SNYKJS-LODASH-608086

  Affected Versions (0.1.0 to 4.17.16)
- **lodash Allocation of Resources Without Limits or Throttling Vulnerability**

Prototype pollution attack when using .zipObjectDeep in lodash before 4.17.20. Affected Versions 4.17.9 to 4.17.19

- **CVE-2021-23337**

Description

Prior to 4.17.21, Lodash versions are vulnerable to Command Injection via the template function. Lodash is used in a number of NetApp products. All versions of package lodash are vulnerable to vulnerabilities that, if exploited successfully, could result in the disclosure of sensitive information, the addition or modification of data, or a Denial of Service (DoS).

Impact

disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). Affected products are follows,

Affected Products

- Active IQ Unified Manager for Linux
- Active IQ Unified Manager for Microsoft Windows
- Active IQ Unified Manager for VMware vSphere
- Cloud Manager
- System Manager 9.x

Exploit / Payload

org.fujion.webjars:lodash is a modern JavaScript utility library delivering modularity, performance, & extras. Affected versions of this package are vulnerable to Command Injection via template.

PoC

```
var _ = require('lodash');

_.template('', { variable: '){console.log(process.env)}; with(obj' })()
```

Recommended Actions / Remedy

Since this occurs based on outdated version, administrators should need to update to current Lodash utility 4.17.21.

Classification

B. Out-of-date Version (GSAP)

Severity : HIGH
Method : GET
OWASP : No 06 Type

Netsparker discovered that the target website is using the GreenSock Animation Platform (GSAP) and that it is out of date. GSAP is a JavaScript library that allows you to create high-performance animations that work in all major browsers. CSS, SVG, canvas, React, Vue, WebGL, colors, strings, motion paths, generic objects...anything JavaScript can touch can be animated! ScrollTrigger is a plug-in.

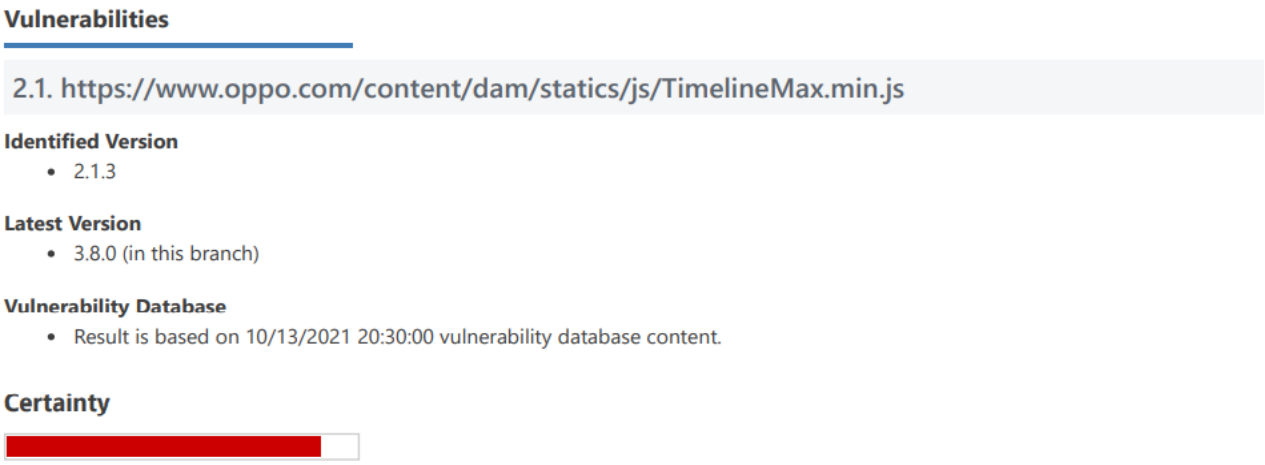
Impact

Since this is an old version of the software, it may be vulnerable to attacks.

- GSAP Insufficient Information Vulnerability
- This affects the package gsap before 3.6.0.
- Affected versions of this package are vulnerable to Prototype Pollution.

Affected Versions - 1.18.2 to 3.5.1

External References - CVE-2020-28478



Recommended Actions / Remedy

Since this occurs based on outdated version, administrators should need to update to current GSAP utility 3.8.0.

Since this outdated version vulnerable for prototype pollution attacks, its essentials to follow the bellow actions for more security.

- Freeze the prototype— use Object.freeze (Object.prototype).
- Require schema validation of JSON input.
- Avoid using unsafe recursive merge functions.
- Consider using objects without prototypes (for example, Object.create(null)), breaking the prototype chain and preventing pollution.

- As a best practice use Map instead of Object.

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
SANS Top 25	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

2. Target Domain: **https://www.oppo.cn/**

https://www.oppo.cn/

Scan Time	: 10/15/2021 1:10:05 AM (UTC+05:30)
Scan Duration	: 00:00:11:25
Total Requests	: 10,816
Average Speed	: 15.8 r/s

Risk Level: **CRITICAL**

22 IDENTIFIED	8 CONFIRMED	1 CRITICAL
0 HIGH	3 MEDIUM	7 LOW
	7 BEST PRACTICE	4 INFORMATION

Identified Vulnerabilities

Critical	1
High	0
Medium	3
Low	7
Best Practice	7
Information	4
TOTAL	**22**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	4
Best Practice	1
Information	2
TOTAL	**8**

A. Out-of-date Version (PHP)

Severity : Critical
Method : GET
OWASP : No 06 Type

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

- **PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability**

  An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.

  Affected Versions - 7.0.1 to 7.1.19

  External References - CVE-2019-9641

- **PHP Out-of-bounds Write Vulnerability**

  In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution.

  Affected Versions - 7.0.1 to 7.1.32

  External References - CVE-2019-11043

- **PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability.**

  In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the php_stream_url_wrap_http_ex function in ext/standard/http_fopen_wrapper.c. This subsequently results in copying a large string.

  Affected Versions - 7.1.0 to 7.1.14

  External References - CVE-2018-7584

- **PHP Use After Free Vulnerability**

  An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c.

  Affected Versions - 7.0.1 to 7.1.25
  External References - CVE-2019-9020

- **PHP Out-of-bounds Read Vulnerability**

  An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.

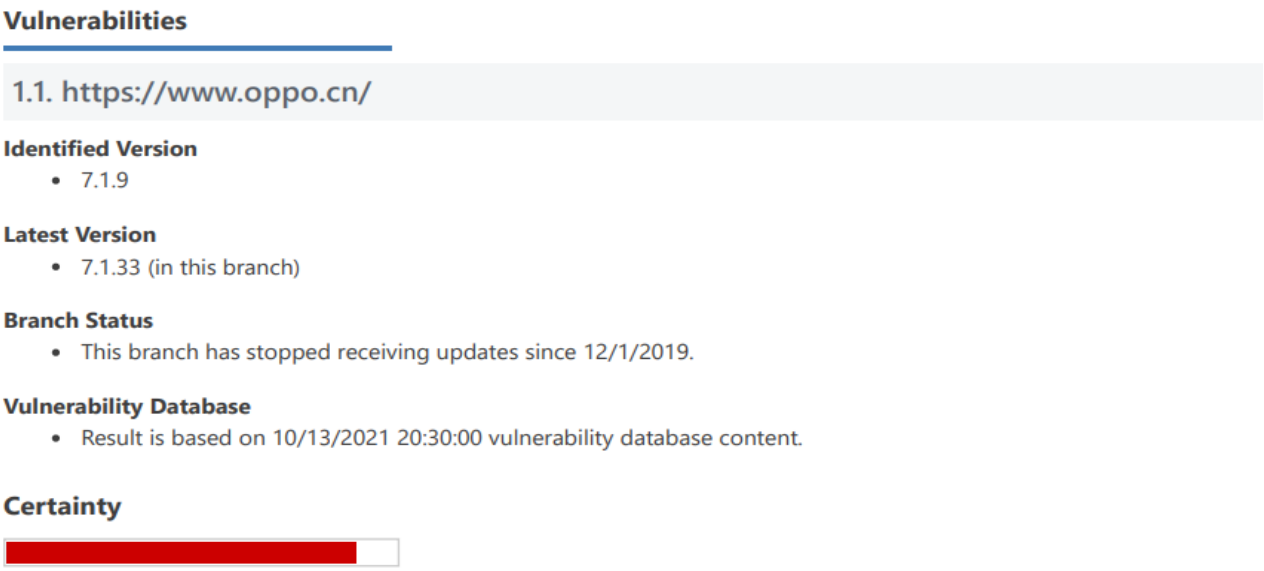
  Affected Versions - 7.0.1 to 7.1.25

  External References - CVE-2019-9023

Other Vulnerabilities related to Outdated PHP Versions

- PHP Out-of-bounds Read Vulnerability
- PHP Uncontrolled Resource Consumption Vulnerability
- PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability
- PHP Permissions, Privileges, and Access Controls Vulnerability
- PHP Integer Overflow or Wraparound Vulnerability
- PHP NULL Pointer Dereference Vulnerability
- PHP Deserialization of Untrusted Data Vulnerability

- PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability
- PHP Loop with Unreachable Exit Condition ('Infinite Loop') Vulnerability
- PHP Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') Vulnerability and so on.

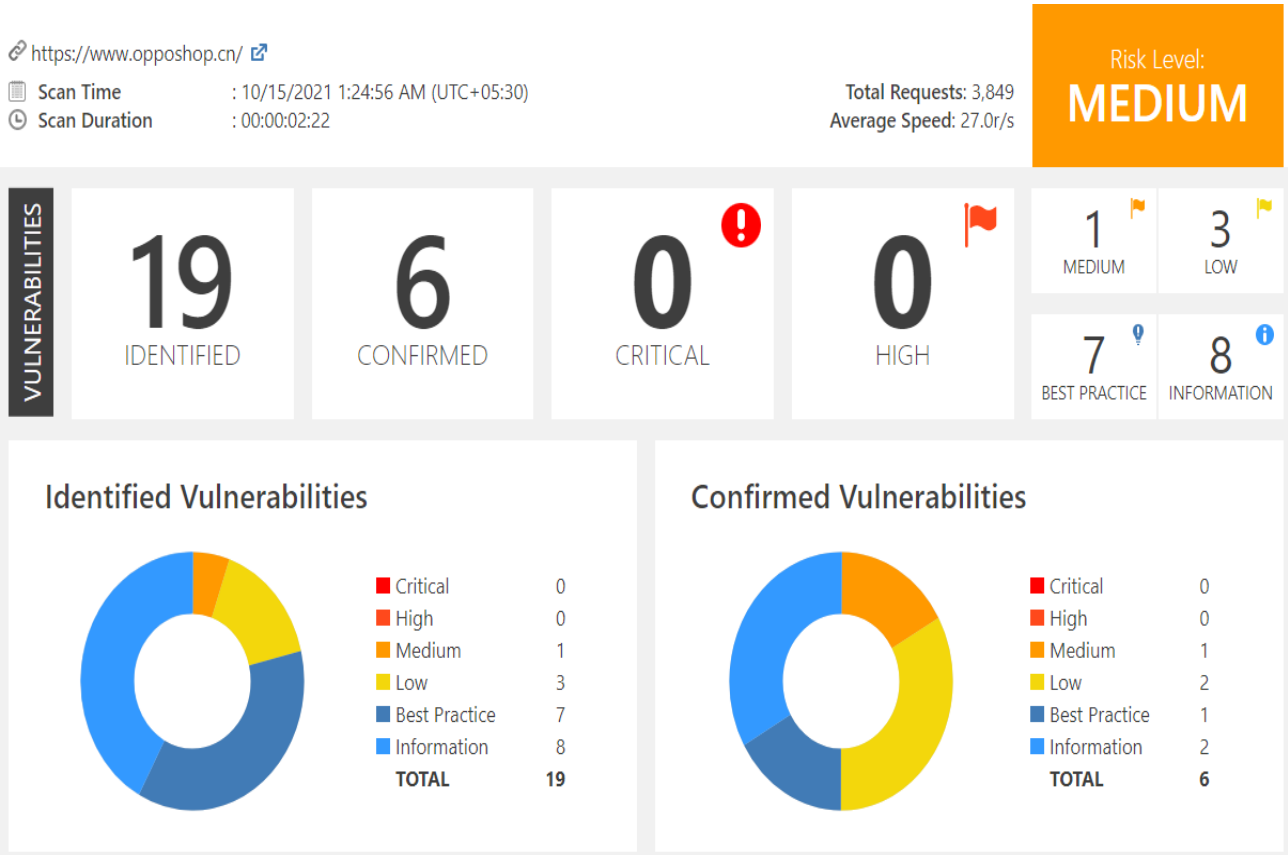


Recommended Actions / Remedy

Since this occurs based on outdated version, administrators should need to update to current PHP version 7.1.33

Classification

3. Target Domain: **https://www.opposhop.cn/**



A. Weak Ciphers Enabled

Method : GET
Severity : Medium

Netsparker detected that weak ciphers are enabled during secure communication (SSL). You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between server and client.

Recommended Actions / Remedy

- Configure the web server to disallow using weak ciphers and bellow actions can be perform for mitigations.

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

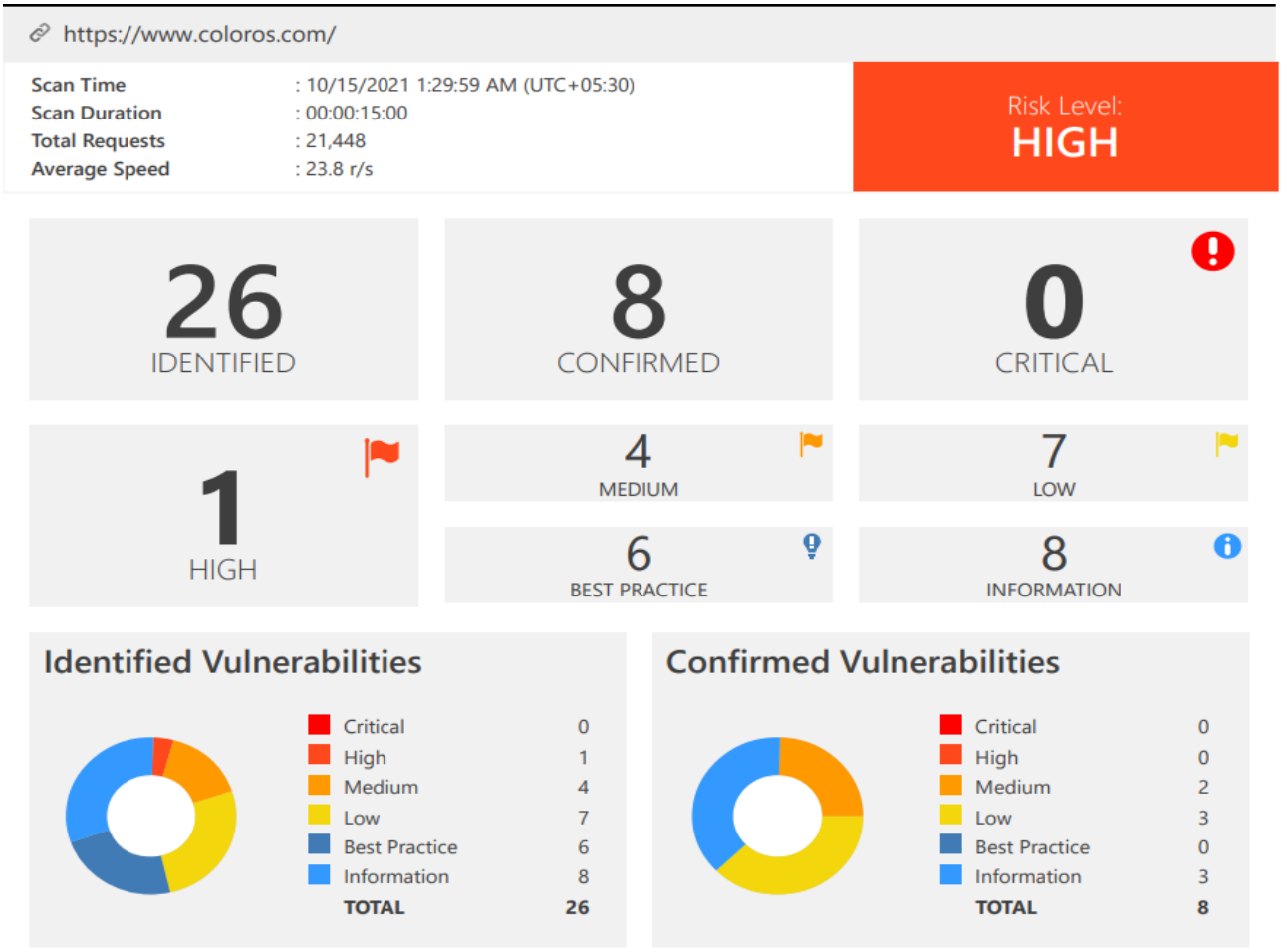
a.Click Start, click Run, type `regedt32`or type `regedit`, and then click OK.
b.In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
c.Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Classification

CLASSIFICATION	
PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

4. Target Domain: **https://www.coloros.com/**



A. Out-of-date Version (AngularJS)

Severity : HIGH
Method : GET
OWASP : No 06 Type

Netsparker identified the target web site is using AngularJS and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

- **AngularJS Improper Input Validation Vulnerability**

  In AngularJS before 1.7.9 the function `merge()` could be tricked into adding or modifying properties of `Object.prototype` using a `__proto__` payload.

  Affected Versions 0.9.0 to 1.7.8 External References

  Affected Versions - 0.9.0 to 1.7.8

  External References - CVE-2019-10768

- **AngularJS Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**

  angular.js prior to 1.8.0 allows cross site scripting. The regex-based input HTML replacement may turn sanitized code into unsanitized one. Wrapping "<option>" elements in "<select>" ones changes parsing behavior, leading to possibly unsanitizing code.

  Affected Versions - 0.9.0 to 1.7.9

  External References - CVE-2020-7676

- **AngularJS Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**

  There is a vulnerability in all angular versions before 1.5.0-beta.0, where after escaping the context of the web application, the web application delivers data to its users along with other trusted dynamic content, without validating it.

  Affected Versions - 1.0.0 to 1.4.14

  External References - CVE-2019-14863

- **AngularJS Denial of Service (DoS)**

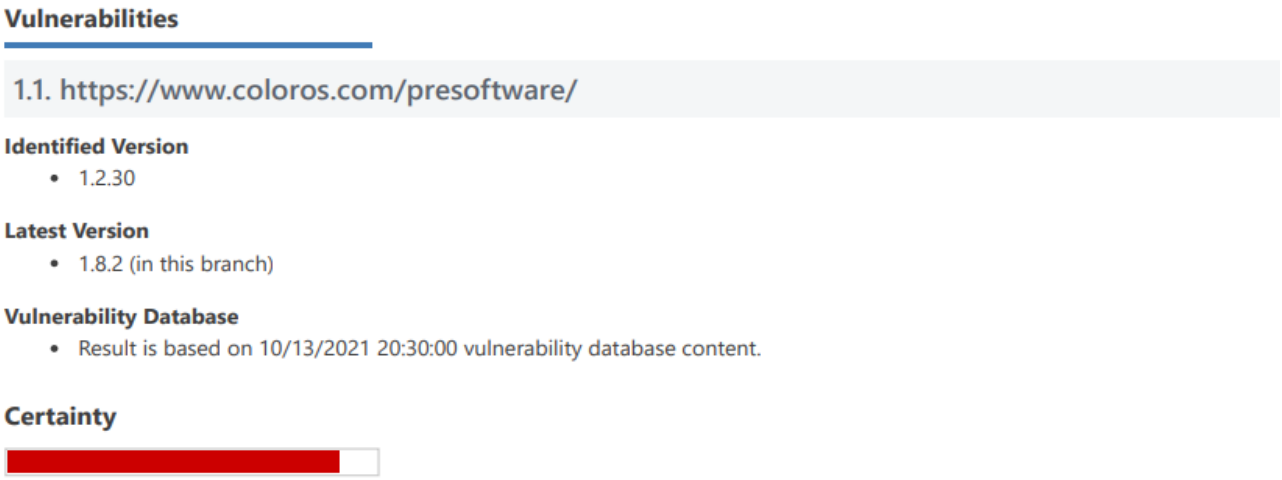
  AngularJS.Core is a AngularJS.* package for other Angular modules within .NET.Affected versions of this package are vulnerable to Denial of Service (DoS).https://snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-471886

Affected Versions - 0.9.0 to 1.6.2

- **AngularJS Cross-site Scripting (XSS) Vulnerability**

  AngularJS.Core is an AngularJS.* package for other Angular modules within .NET.Affected versions of this package are vulnerable to Cross-site Scripting (XSS)https://snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-471883

  Affected Versions - 0.9.0 to 1.6.4



- **CVE-2019-10768**

Description

AngularJS is a package that lets developers to write client-side web applications. It also lets HTML to use as template language and also let extend HTML's syntax to express particular application's components clearly and succinctly.

Impact

Affected versions of this package are vulnerable to Prototype Pollution. The function merge() could be tricked into adding or modifying properties of Object.prototype using a __proto__ payload.

Exploit / Payloads

```
angular.merge({}, JSON.parse('{"__proto__": {"xxx": "polluted"}}'));
console.log(({}).xxx);
```

Recommended Actions / Remedy

Since this occurs based on outdated version, administrators should need to update to current AngularJS version 1.8.2

Classification

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
SANS Top 25	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

B. Active Mixed Content over HTTPS

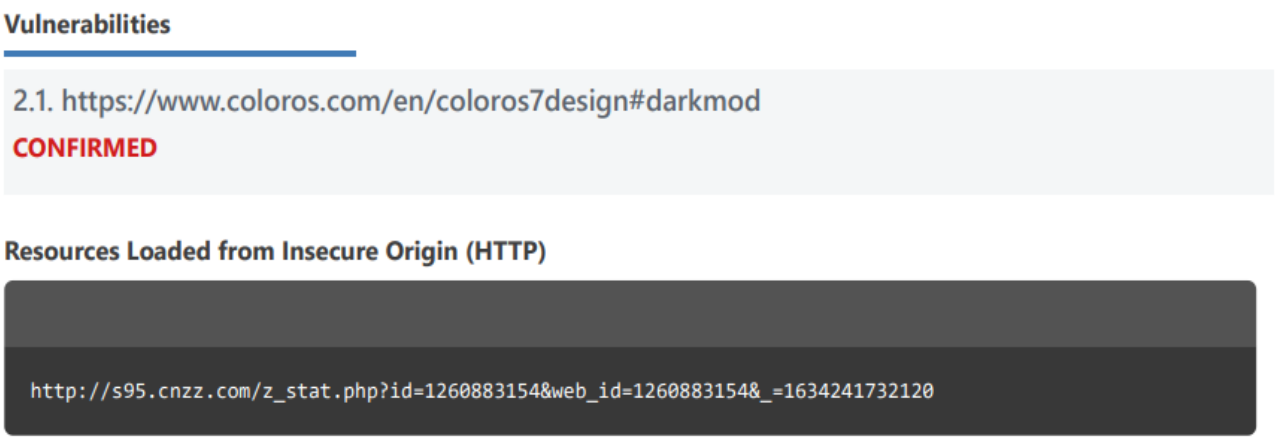
Severity : Medium [Confirmed]
Method : GET

Netsparker detected that an active content loaded over HTTP within an HTTPS page

Impact

Active Content is a resource that can run in the context of your page and change the entire page. If the HTTPS page contains active content, such as scripts or stylesheets, that was obtained via regular, cleartext HTTP, the connection is only partially encrypted. Sniffers can read the unencrypted content.

A man-in-the-middle attacker can intercept the HTTP content request and rewrite the response with malicious code. Malicious active content can steal the user's credentials, collect sensitive data about the user, or attempt to install malware on the user's system (for example, by exploiting vulnerabilities in the browser or its plugins), and thus the connection is no longer secure.

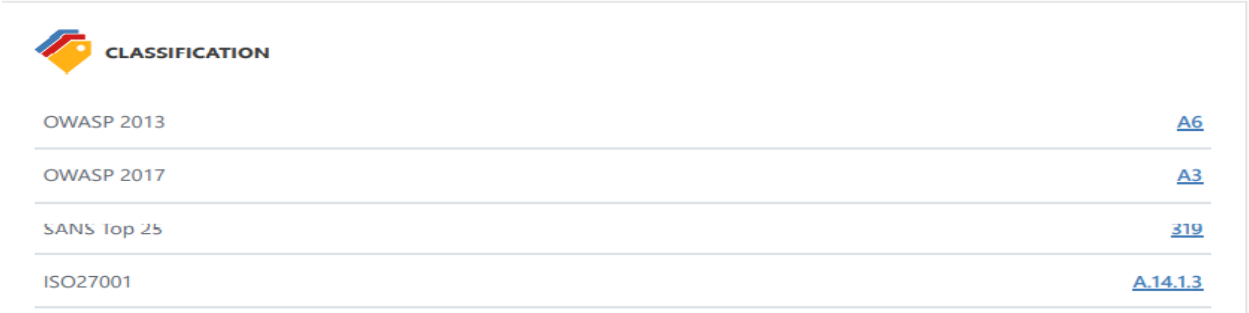


Recommended Actions / Remedy

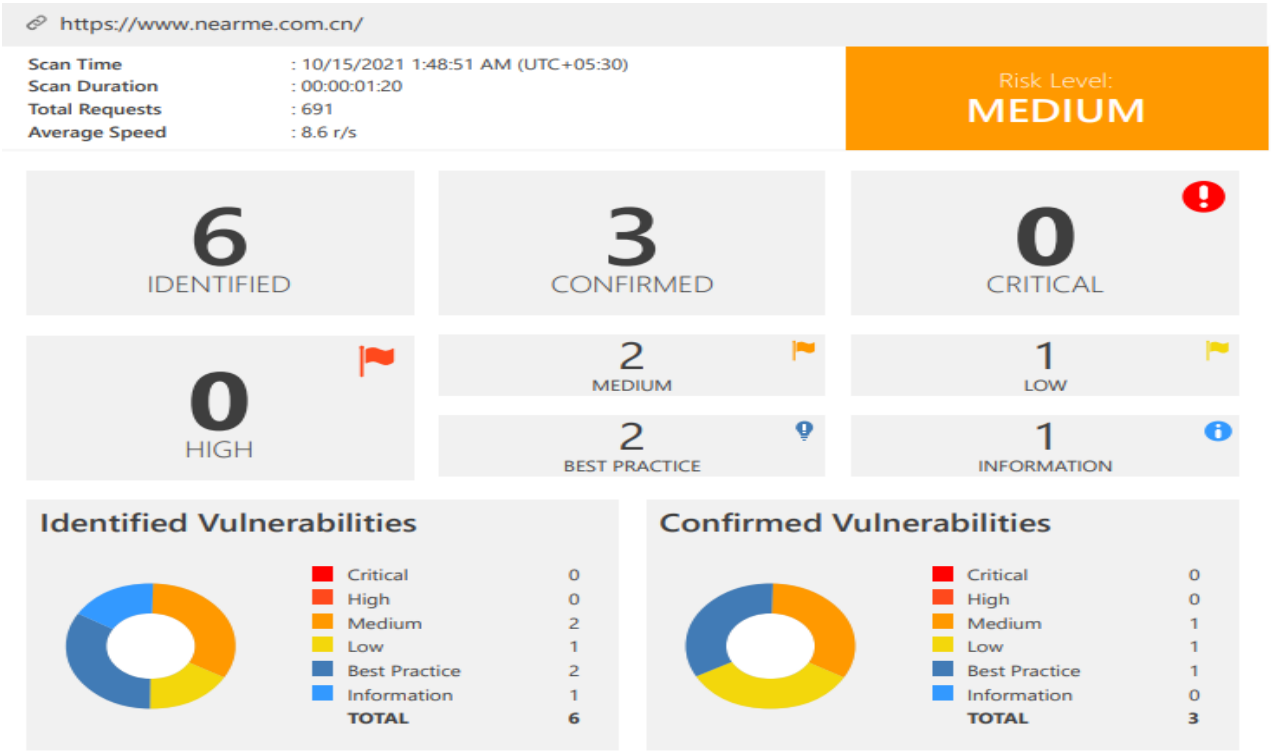
There are two technologies to defense against the mixed content issues.

- HTTP Strict Transport Security (HSTS) is a mechanism that enforces secure resource retrieval, even in the face of user mistakes (attempting to access your web site on port 80) and implementation errors (your developers place an insecure link into a secure page)
- Content Security Policy (CSP) can be used to block insecure resource retrieval from third-party web sites.
- Can use "protocol relative URLs" to have the user's browser automatically choose HTTP or HTTPS as appropriate, depending on which protocol the user is connected with.

Classification



5. Target Domain: https://www.nearme.com.cn/



A. HTTP Strict Transport Security (HSTS) Policy Not Enabled

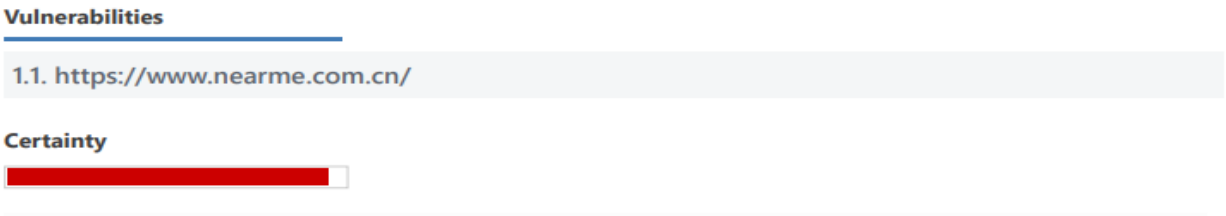
Severity : Medium
Method : GET

Impact

The target website is being served from not only HTTPS but also HTTP and it lacks HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion. When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

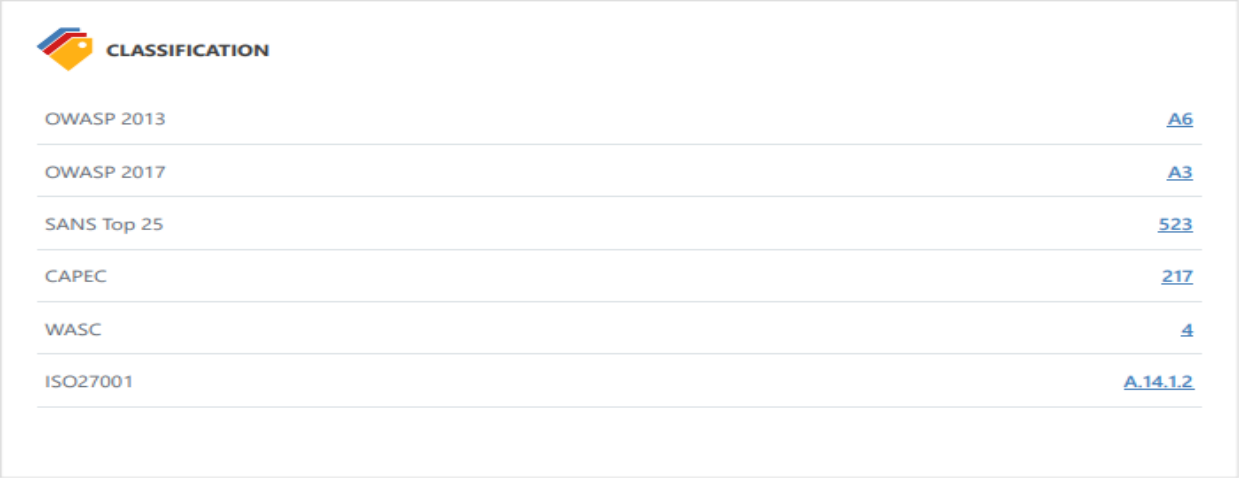
- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links.
- If the security of the connection cannot be ensured, user agents show an error message and do not allow the user to access the web application.



Recommended Actions / Remedy

- Implement the HSTS header with proper configuration of directives.
- Implement the suitable redirect mechanisms.

Classification



CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

B. Weak Ciphers Enable

Severity : Medium
Method : GET

Netsparker detected that weak ciphers are enabled during secure communication (SSL). Should allow only strong ciphers on web server to protect secure communication with Clients.

Impact

Attackers might decrypt SSL traffic between server and visitors.

Vulnerabilities

2.1. https://www.nearme.com.cn/

CONFIRMED

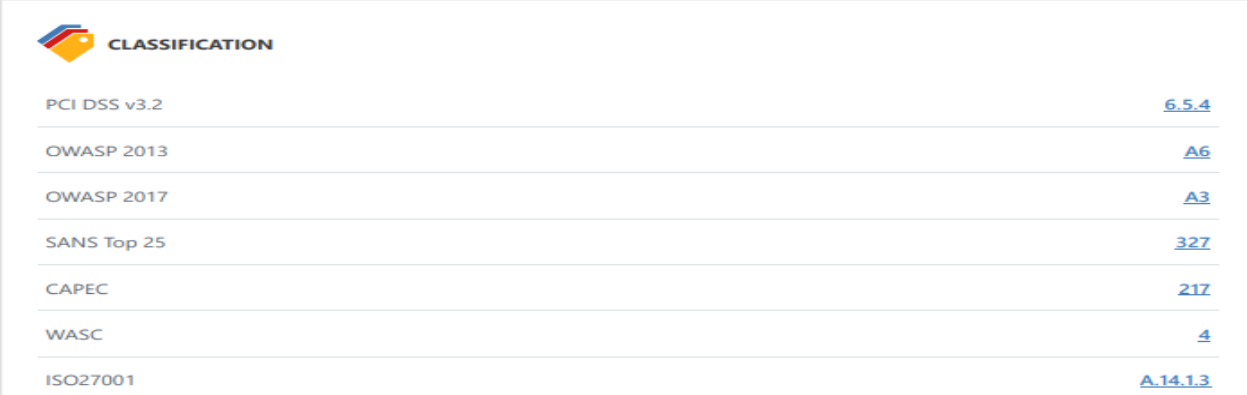
List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)

Recommended Actions / Remedy

Configure your web server to disallow using weak ciphers.

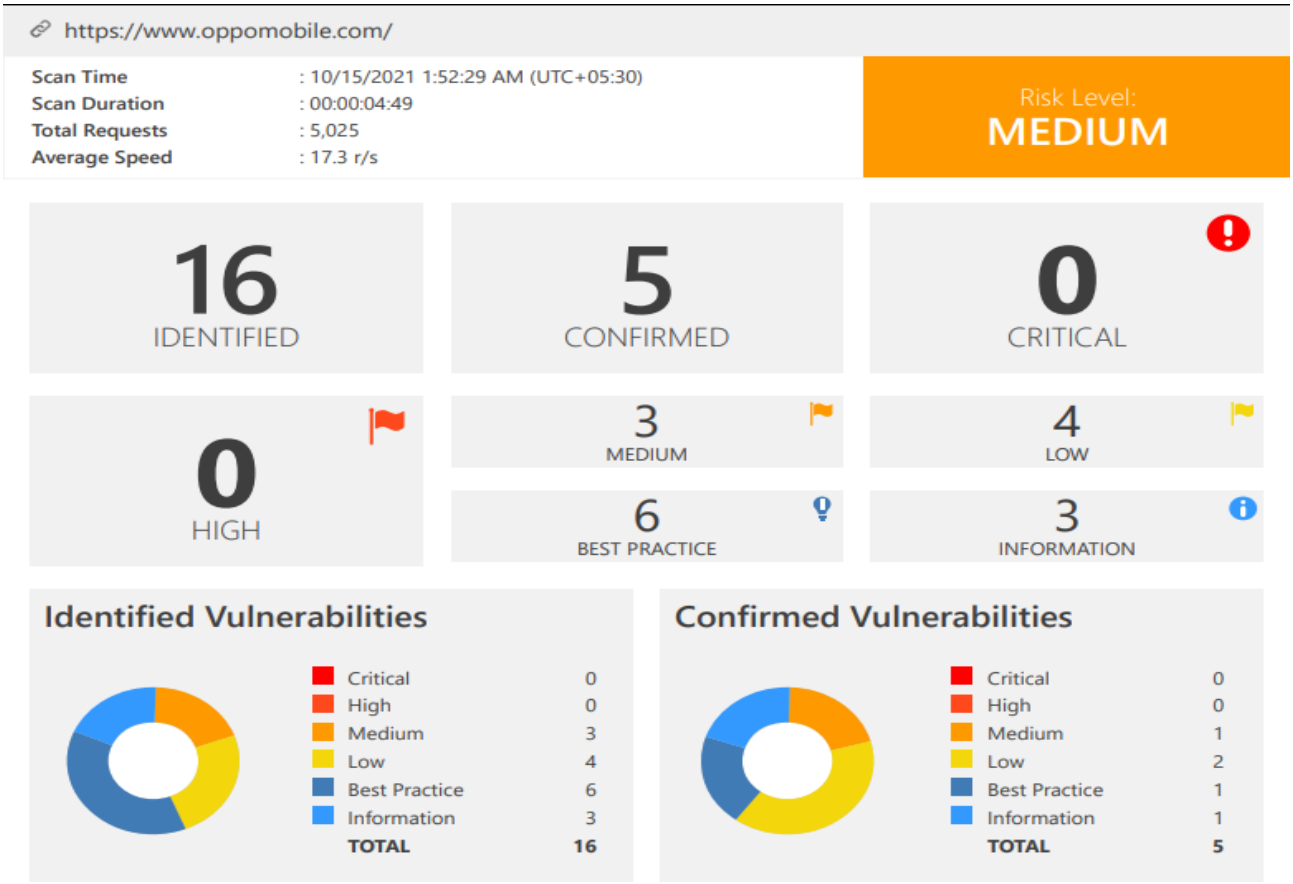
Classification



CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

6. Target Domain: **https://www.oppomobile.com/**



A. Out-of-date Version (JQuery)

Severity : Medium
Method : GET
OWASP : No 06 Type

Netsparker identified the target web site is using jQuery and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

- jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

  jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

  Affected Versions 1.8.0 to 2.2.4

  External References CVE-2015-9251

- jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

  jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

  Affected Versions 1.8.0 to 1.8.3

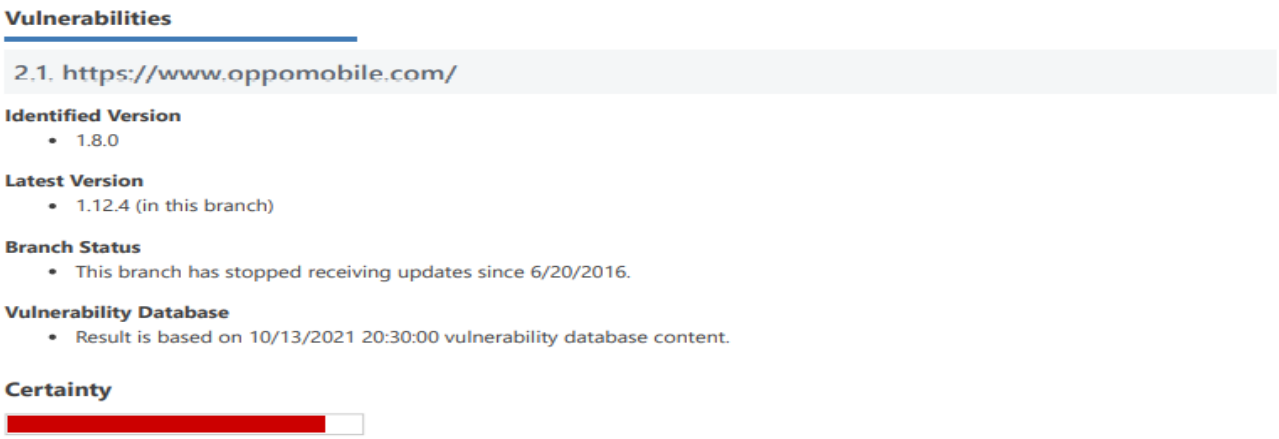
  External References CVE-2012-6708

- JQuery Prototype Pollution Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Affected Versions 1.0 to 3.3.1

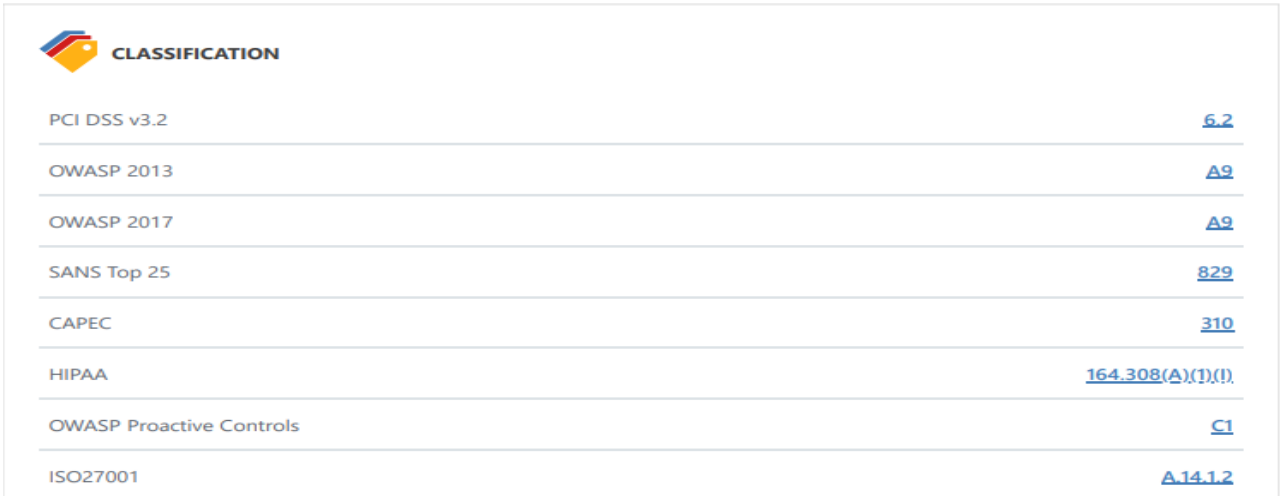
External References CVE-2019-11358



Recommended Actions / Remedy

Since this occurs based on outdated version, administrators should need to update to current jQuery version 1.12.4

Classification



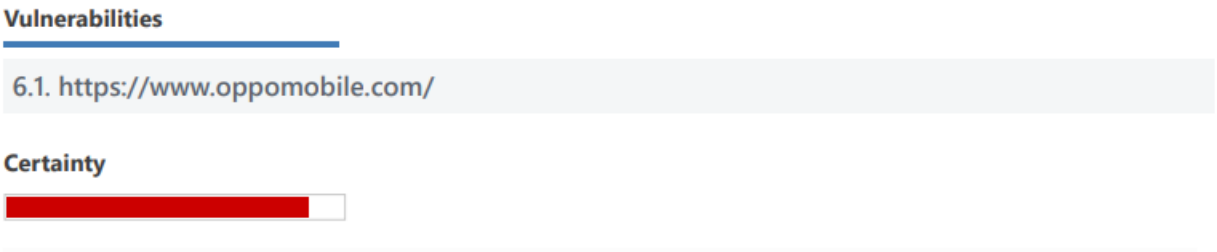
B. Missing X-Frame-Option Header

Severity : Low
Method : GET
OWASP : No 05 Type

The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

- Clickjacking
- Keystroke hijacking

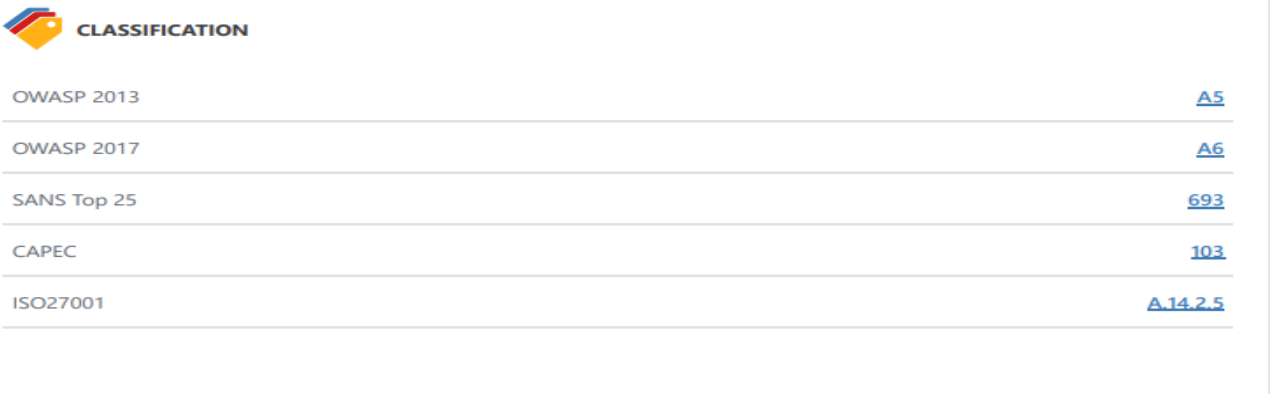


Recommended Actions / Remedy

Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

- X-Frame-Options: DENY, completely denies to be loaded in frame/iframe.
- X-Frame-Options: SAMEORIGIN, allows only if the site which wants to load has a same origin.
- X-Frame-Options: ALLOW-FROM URL, grants a specific URL to load itself in an iframe (not all browsers support)
- Employing defensive code in the UI to ensure that the current frame is the most top-level window

Classification



CLASSIFICATION	
OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	693
CAPEC	103
ISO27001	A.14.2.5

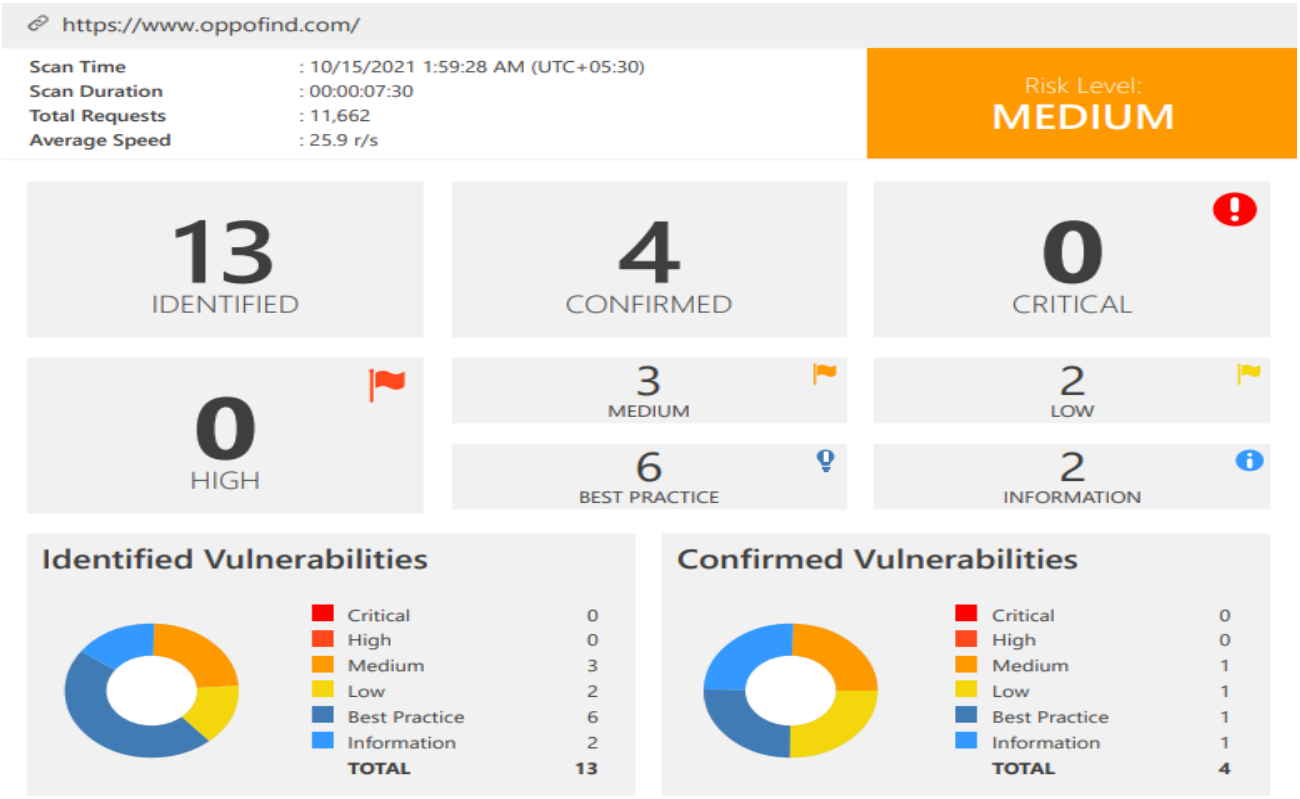
Clickjacking and Keystroke Hijacking

Whenever an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they intended to click on the top-level page, this is known as clickjacking. As a result, the attacker "hijacks" clicks intended for their page and redirects them to another page, most likely owned by another application, domain, or both. Users may unknowingly download malware, visit malicious web pages, provide credentials or sensitive information, purchase products online because of this. There are two variations of this attack type,

- Likejacking
- Courserjacking

Keystrokes can also be hijacked using a similar approach. A carefully crafted combination of stylesheets, iframes, and text boxes can fool a user into thinking they are typing in their email or bank account password, when in fact they are typing into an invisible frame controlled by the attacker.

7. Target Domain: **https://www.oppofind.com/**



A. [Possible] Phishing by Navigating Browser Tabs

Severity : Low
Method : GET

Open windows with normal hrefs with the tag target="_blank" can modify window.opener.location and replace the parent webpage with something else, even on a different origin.

Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack rel="noopener noreferrer" attribute, a third party site can change the URL of the source tab using window.opener.location.assign and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

reverse tabnabbing attacks and blankshield techniques are famous.

Vulnerabilities

4.1. https://www.oppofind.com/

External Links

- https://www.oppo.com/cn/
- https://www.opposhop.cn/products/487.html
- https://www.oppo.com/cn/product/findx/index.html
- http://beian.miit.gov.cn

Certainty

Recommended Actions / Remedy

There is no such a method for prevent from phishing attacks but user awareness is the grate way to mitigate the attack vectors.

Classification

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

4. OWASP ZAP

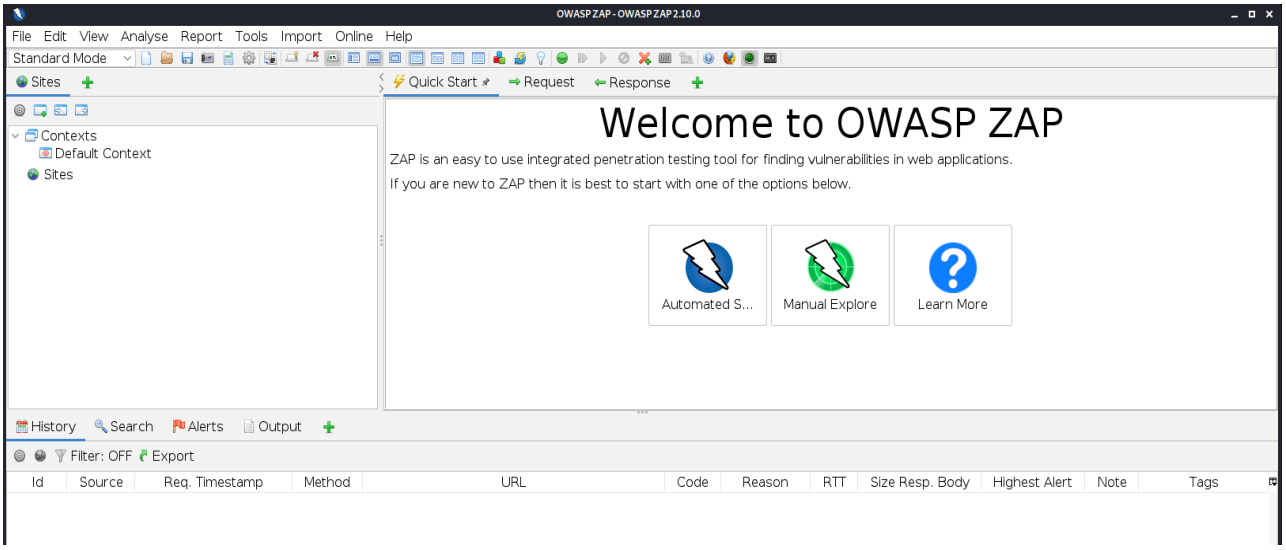
OWASP ZAP [Zed Attack Proxy] is an open-source web penetration tool which is developed and maintained by Umbrella of the Open Web Application Security Project (OWASP). ZAP is also known as a "man-in-the-middle proxy." It sits between the tester's browser and the web application, intercepting and inspecting messages sent between the two, modifying the contents as needed, and then forwarding those packets on to the destination. It can run as a standalone application or as a daemon process. ZAP is also a corporate tool which means ZAP can be connect to the other existing network proxy as well.

Since ZAP is an open-source program, functionality of this tool can be used in beginner to expert range of testers and also different versions of ZAP available for major operating systems. Some operating systems like KALI, PARROT OS provide the built in ZAP versions. ZAP extensions also can be plug in to the web browsers.

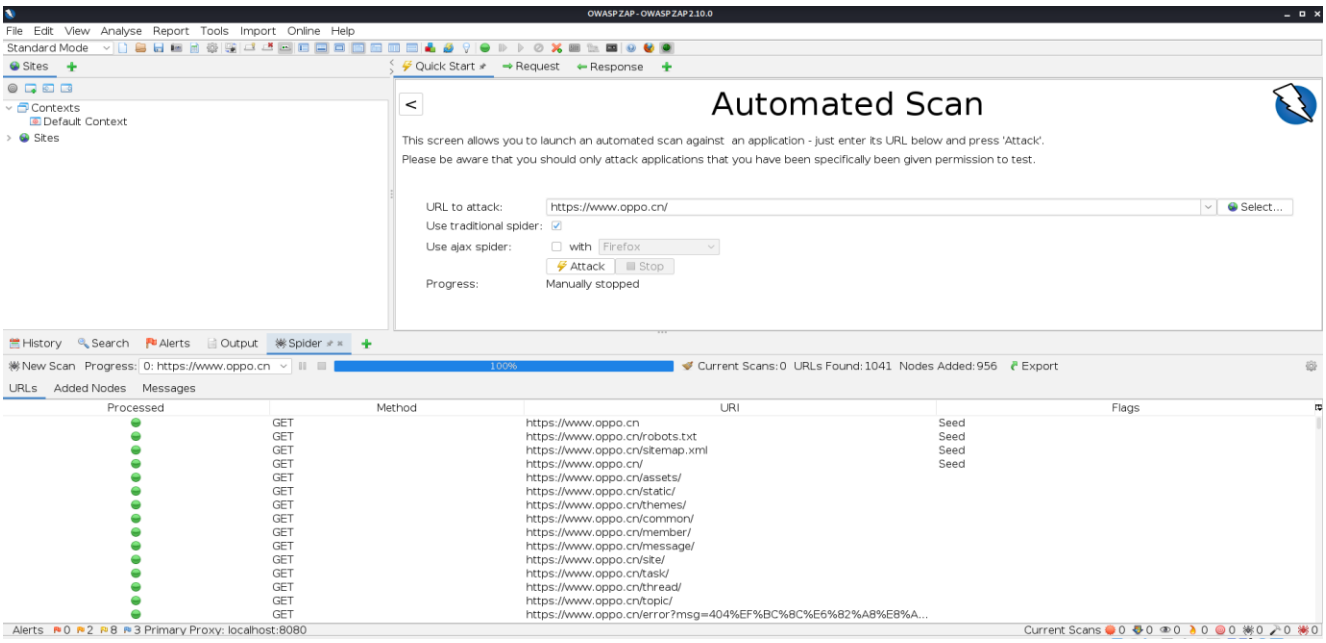
Installation

Download URL -: https://www.zaproxy.org/

- JAVA JDK version 8 or above required before installing ZAP.
- After the installation process, in the initial launching, ZAP will be asked if user want to persist the ZAP session or default mode will be applied. When using the default mode, all the data will remove when exit from ZAP.



Initially I perform automated scan for ***oppo.com** for validate the previous funded vulnerabilities.



Then the available vulnerability list available in report.

ZAP Scanning Report

Summary of Alerts

Generated on Sat, 16 Oct 2021 02:39:55

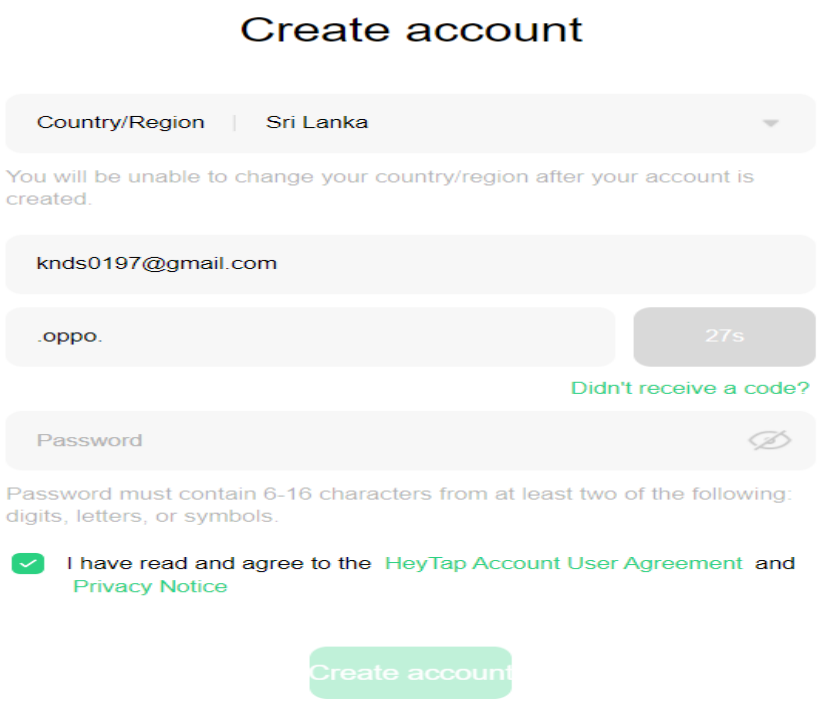
Risk Level	Number of Alerts
High	0
Medium	4
Low	11
Informational	9

Alerts

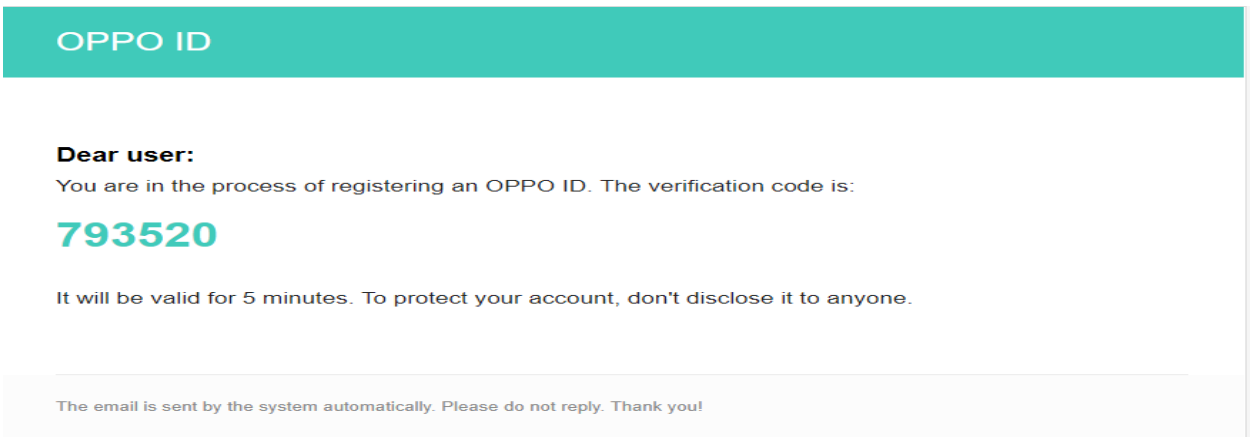
Name	Risk Level	Number of Instances
Cross-Domain Misconfiguration	Medium	4764
Vulnerable JS Library	Medium	1
X-Frame-Options Header Not Set	Medium	683
Absence of Anti-CSRF Tokens	Low	74
Application Error Disclosure	Low	2
Cookie No HttpOnly Flag	Low	2
Cookie without SameSite Attribute	Low	626
Cookie Without Secure Flag	Low	626
Cross-Domain JavaScript Source File Inclusion	Low	19535
Incomplete or No Cache-control Header Set	Low	3636
Information Disclosure - Debug Error Messages	Low	10
Secure Pages Include Mixed Content	Low	1
X-Content-Type-Options Header Missing	Low	126
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	3
Content-Type Header Missing	Informational	7
Information Disclosure - Suspicious Comments	Informational	5102
Loosely Scoped Cookie	Informational	624

Manual Testing

For manually checking the selected domains, I initially created the user account on https://www.oppo.cn,



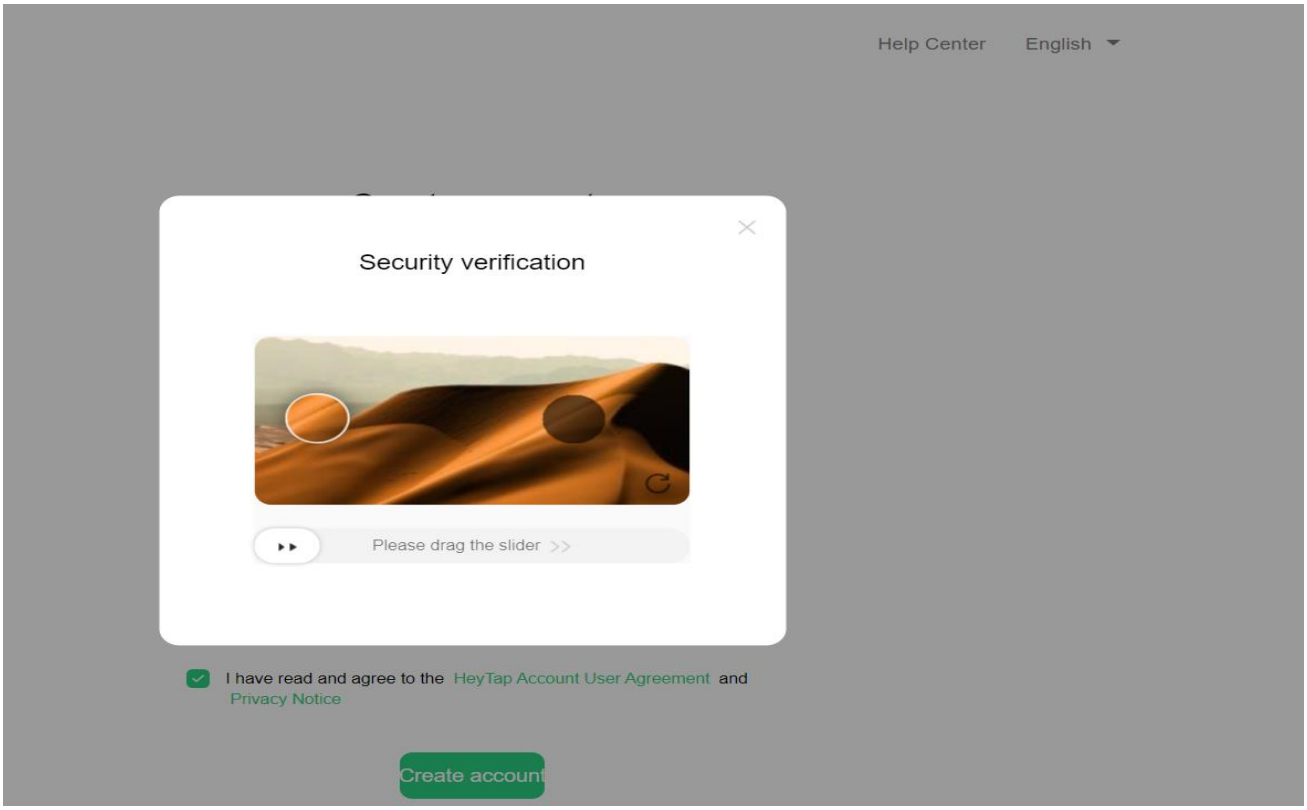
Initially server will identify our region and after I insert my email address, server will send the One Time Passcode [OTP] for verify the user. When I insert a wrong OTP, server did not allow me to create an account. Also, we had to submit the OTP withing 50 seconds.



Even if a user fails to provide the valid OTP within the 50s, users can re-request the OTP, but system will provide the same OTP until the OTP terminate in 5 minutes. Due to the time restrictions, we cannot perform brute- force attack against the web system

For password, system ask 6 -16 characters length password which contain minimum of digits, letters or symbols.

When I press the create account button, system check whether user is human by using some basic captcha. System will give three chances to fulfill the captchas. If a user fails to complete the tasks, then system won't create the user account.



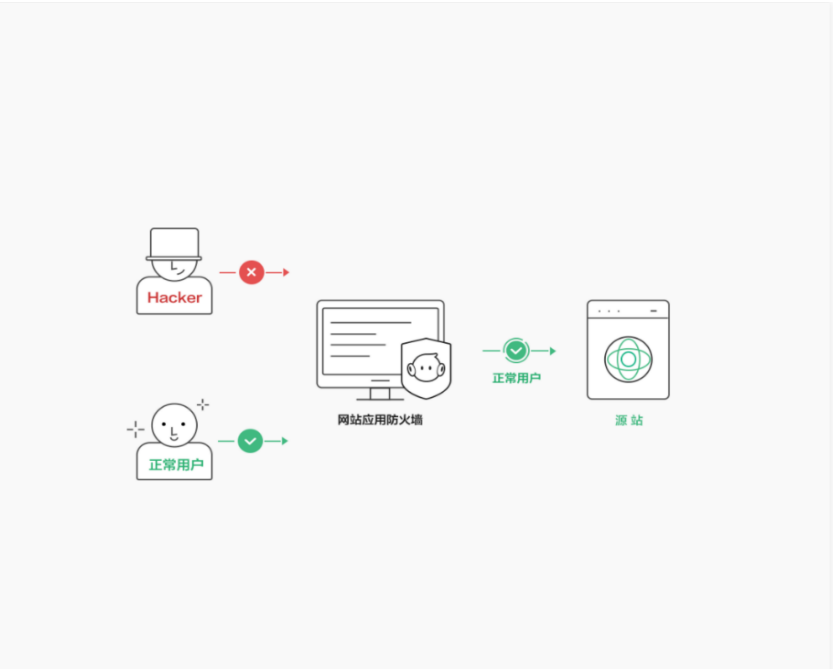
Cross-site Scripting (XSS)

Cross-site scripting is a client-side mascaraed type of attack. Attackers input malicious payloads/ scripts to webpages through input fields such as forms, comment sections and etc. when a legitimate user rendering the particular webpage, then the malicious script will execute. After the successful script execution, the legitimate user's cookies, session IDs and other sensitive information will send to the attacker.

There are three different types of XSS attacks. Each of them is different based on the final impact.

- Reflective Cross-site Scripting
- Dom based Cross-site Scripting
- Stored Cross-site Scripting

I tried to insert the basic script into the website, but website didn't reflect any actions. When I'm repeating the same action, system identified me as an intruder



Conclusion

web audit is necessary for in order to assess the web applications security. Several flaws were discovered during this investigation, which must be addressed as soon as possible. The severity of the discovered issues must be used to prioritize corrective measures.

After the all the information gathering, scanning and testing, the selected domains contain all the severity level vulnerabilities,

- Critical Vulnerabilities – 2
- High Vulnerabilities - 3
- Several Medium and Low vulnerabilities

Since, Oppo is a one of world technology company, it's essentials to address all the flaws in their system. Otherwise, attackers might try to exploit above vulnerabilities for takedown the company's assets.

Reference

1. https://hackerone.com/oppo?type=team

2. https://owasp.org/www-community/attacks/xss/

3. https://www.netsparker.com/support/what-is-netsparker/

4. https://kalilinuxtutorials.com/whatweb/

5. https://github.com/TomNomNom

6. https://owasp.org/www-community/attacks/Clickjacking

7. https://nvd.nist.gov/

8. https://www.zaproxy.org/docs/

9. https://tzusec.com/httprobe/

10. https://kalilinuxtutorials.com/legion-penetration-testing/

11. https://medium.com/geekculture/bug-bounty-methodology-v4-0-demonstrated-8e9cb6ed1b12

12. https://thehackerish.com/my-bug-bounty-methodology-and-how-i-approach-a-target/

13. http://index-of.es/Miscellanous/LIVRES/web-hacking-101.pdf