Sri Lanka Institute of Information Technology

VULNERABILITY ASSESSMENT - WEB AUDIT

https://www.uber.com

Individual Assignment

IE2062 – Web Security

Submitted by:

Student Registration Number	Student Name
IT19003610	**K.G.S.SHIRANTHAKA**

Date of submission: 23/10/2020

Table of Contents

Acknowledgement

I would like to express my deep gratuity for his invaluable guidance and advice, Dr. Lakmal rupasinghe the lecture in charge of Web security module, which was vital to the initiation of this web audit.

I also want to thank Ms. Chethna Lyanapathirana, Ms. Lanisha Rugghahakotuwa and Ms. Chathu Udagedra for the help and guidance they have given us during this Web audit.

Assessment Objectives

The security assessment of the http://uber.com/ for the second year second semester Web Security Module. The purpose of this assessment is to discover the vulnerabilities in the target domain and to indicate the subsequent risk level for the vulnerabilities.

Application Credentials and URL

The audit was done on the following URLs.

- https://uber.com
- https://accessibility.uber.com
- https://brand.uber.com
- https://base.uber.com
- https://careersinfo.uber.com
- https://movement.uber.com
- https://www.ubereats.com/
- https://drive.uber.com
- https://guest.uber.com
- https://marketplace.uber.com

Assessment Methodology

OWASP Top 10 Security Risks and Vulnerabilities

Open Web Application Security Project (OWASP) is a not-for-profit worldwide charitable organization focused on improving the security of application software.

- Injection.
- Broken Authentication.
- Sensitive Data Exposure.
- XML External Entities (XXE)
- Broken Access Control.
- Security Misconfiguration.
- Cross-Site Scripting XSS
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring.

Risk	Information
Injection	The injection is referred to as a broad class of attack vectors. Here, the attacker supplies untrusted, malicious input for the program. Types of injection: ▪ Code injection ▪ CSRF injection ▪ Cross-site Scripting ▪ Email header injection ▪ SQL injection
Broken Authentication	This is usually related to authentication and session management. This will allow an attacker to compromise passwords, API-keys, session tokens, etc. ▪ Credential stuffing ▪ Un-hashed passwords ▪ Misconfigured session timeouts ▪ Exploiting the Cookies can be caused to Broken Authentication
Sensitive Data Exposure	Many web applications and API do not ensure sensitive data properly. The attackers may steal, delete, or modify such data, and this causes to identity theft or other crimes.

XML External Entities (XXE)	An XML External Entity attack is a type of attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. This may lead to: ▪ The discourse of the sensitive data ▪ Denial of attack ▪ Identity theft
Broken Access Control	Broken authentication vulnerabilities occur when users can act perform to their intended permissions. This may lead to information disclosure, unauthorized access, modifications, or destruction of data. Common access control vulnerabilities include: ▪ Modifying the URL, application state, or HTML page or by using customize API attack vector ▪ Horizontal Privilege Escalation – user can perform an action or gaining the access rights of another user with the same level of permissions. ▪ Vertical Privilege Escalation - user can perform an action or gaining the access rights of another user that requires a level of access beyond their role.

Security Misconfiguration	This is the most commonly seen issue. This is caused because of insecure default configurations, misconfigured HTTP headers, and verbose error messages containing sensitive information. Example of security misconfiguration: ▪ If directory listing is not disabled on the server then the attacker can discover the same list to find any file and execute it. An attacker can use tools like OWASP Dirbuster, go buster. Configuring the app server makes it possible to return stack tracks to users with potential underlying defects.
Cross-Site Scripting XSS	This is another common web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. Cross-site scripting attack types: ▪ Reflected XSS ▪ Stored XSS ▪ DOM-based XSS

Insecure Deserialization	This leads to remote code execution. Not only that it allows to attacker to perform attacks like replay attacks, injection attacks, and privilege escalation attacks.
Using Components with Known Vulnerabilities	While some known vulnerabilities lead to only minor impacts, some of the largest breaches to date have relied on exploiting known vulnerabilities in components. Depending on the assets you are protecting, perhaps this risk should be at the top of the list.
Insufficient Logging & Monitoring.	Ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot more systems, and destroy data. Not implement the intrusion detection systems (IDS) and intrusion prevention

Risk Level Information and Necessary Actions

High	The high-risk level shows the highest risk associated with a specific vulnerability. An attacker can successfully exploit the target application and can compromise the application data partially or completely. An Attacker may lead to modifying data delete the data of the web application.
Medium	The medium risk level indicates considerable risk combine with a specific vulnerability. Exploiting medium vulnerability, an attacker can gain low-level information about the application. After mitigating the High-risk vulnerabilities, medium risk vulnerabilities should be mitigated.
Low	The low-risk level indicates the lowest risk associated with a specific vulnerability. This may lead to gain some information about the web application which is not intended to be known otherwise.

Assessment Scope

- Authentication
- Authorization
- Session Management
- Input Validation
- Encryption and cryptography
- Error Handling

Out of Scope

- DOS
- Details available in https://hackerone.com/uber under out of the scope content.

Out of Scope Domains

- support-uber.com
- lioncityrentals.com.sg
- xchangeleasing.com
- *.uber.com.cn domains or any other properties relating to Uber in China, since they belong to Didi Chuxing
- uber.onelogin.com (OneLogin runs their own bug bounty program and any vulnerabilities for OneLogin should be reported to them)
- bizblog.uber.com
- newsroom.uber.com
- love.uber.com
- drive.uber.com
- eng.uber.com
- people.uber.com
- *.et.uber.com

Reconnaissance Phrase (Information Gathering)

The most important part when doing bug hunting or web pen-testing is recon. The main goal of this is to gather and collect as much as possible a form about the company we are targeting.

Subdomain Enumeration

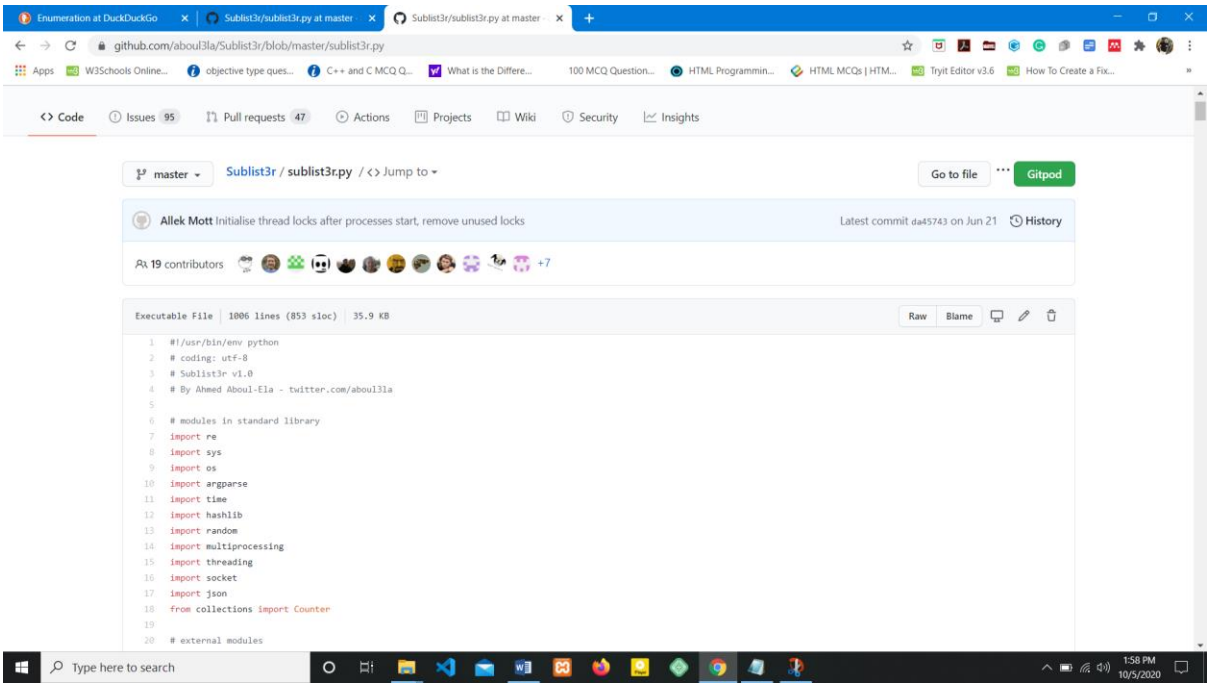
1. Sublist3r

Installation:

```
$ git colne https://github.com/aboul3la/Sublist3r
```

For the installation go to the following GitHub page and clone to the machine.

Github Link: https://github.com/aboul3la/Sublist3r



Then install the pip for our machine for installing sublist3r. To install pip enter the following command.

```
root@kali:~/Downloads/Sublist3r-master#
root@kali:~/Downloads/Sublist3r-master#
root@kali:~/Downloads/Sublist3r-master# pip install -r requirements.txt
```

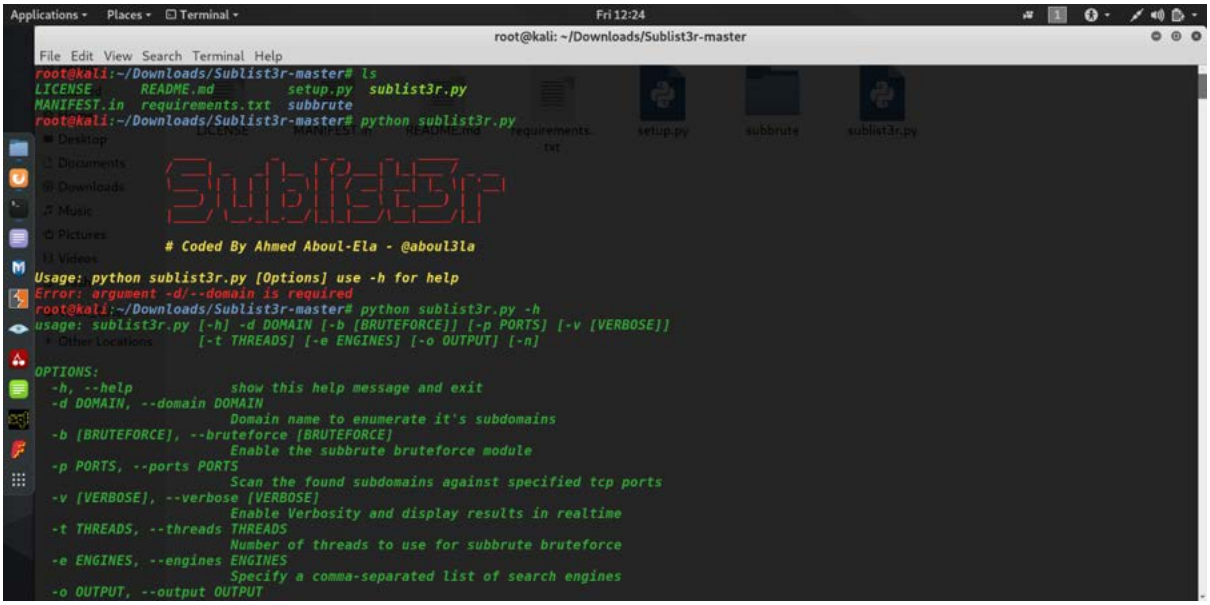
After installing pip then execute the following command to install python to the machine.

```
root@kali:~/Downloads/Sublist3r-master#
root@kali:~/Downloads/Sublist3r-master#
root@kali:~/Downloads/Sublist3r-master# apt-get install -y python3-pip
```

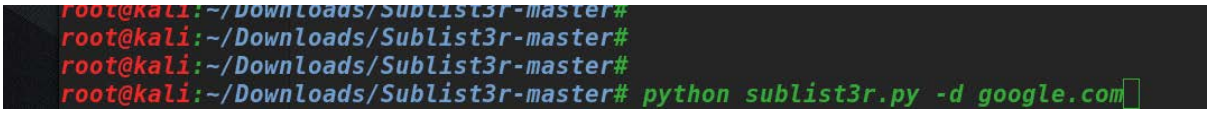
```
root@kali:~/Downloads/Sublist3r-master# python3.8 -V
Python 3.8.5
root@kali:~/Downloads/Sublist3r-master#
```

To get the help option we can enter the following command.

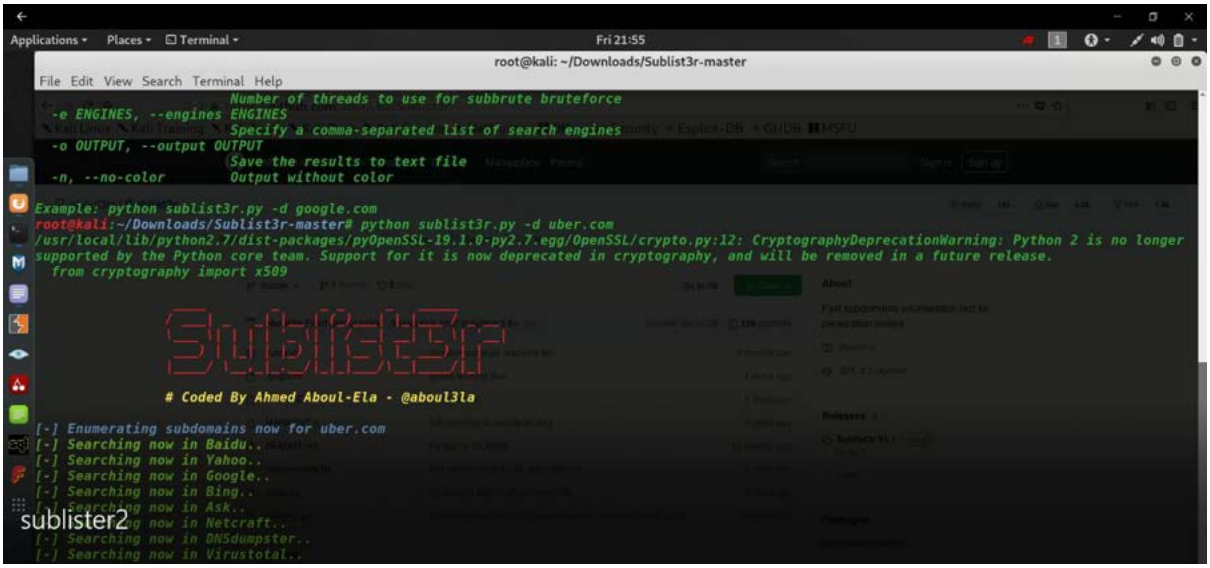
```
root@kali:~/Downloads/Sublist3r-master#
root@kali:~/Downloads/Sublist3r-master#
root@kali:~/Downloads/Sublist3r-master# python sublist3r.py -h
```

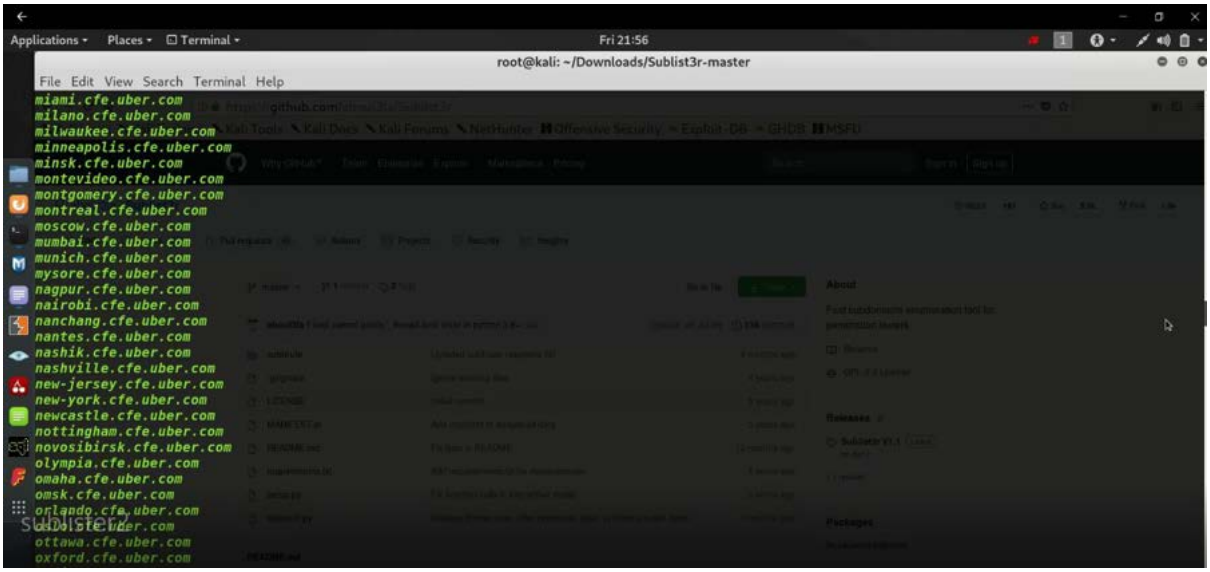


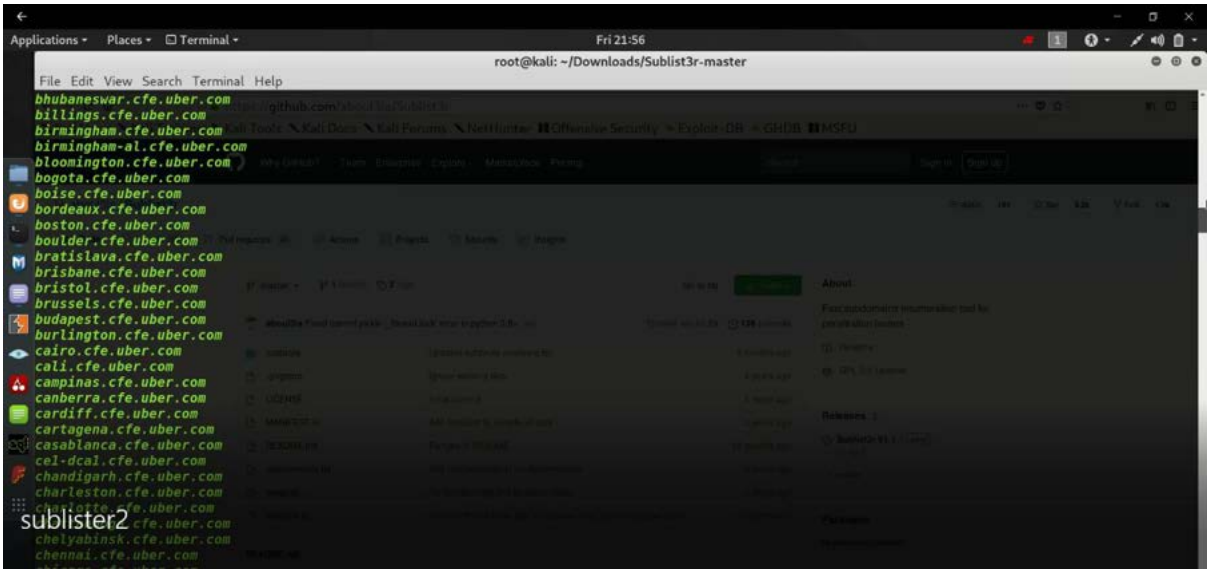
To get the subdomains of the targeted domain I enter the following command.

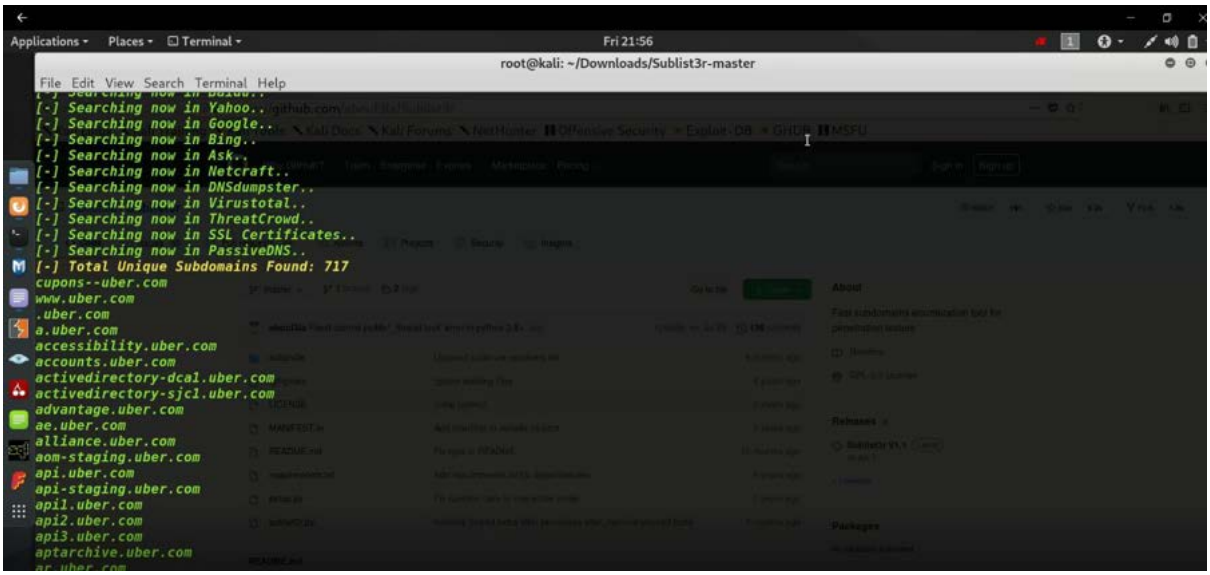


Proof of concept:




Applications Places Terminal
Fri 21:56
root@kali: ~/Downloads/Sublist3r-master
File Edit View Search Terminal Help
miami.cfe.uber.com
milano.cfe.uber.com
milwaukee.cfe.uber.com
minneapolis.cfe.uber.com
minsk.cfe.uber.com
montevideo.cfe.uber.com
montgomery.cfe.uber.com
montreal.cfe.uber.com
moscow.cfe.uber.com
mumbai.cfe.uber.com
munich.cfe.uber.com
mysore.cfe.uber.com
nagpur.cfe.uber.com
nairobi.cfe.uber.com
nanchang.cfe.uber.com
nantes.cfe.uber.com
nashik.cfe.uber.com
nashville.cfe.uber.com
new-jersey.cfe.uber.com
new-york.cfe.uber.com
newcastle.cfe.uber.com
nottingham.cfe.uber.com
novosibirsk.cfe.uber.com
olympia.cfe.uber.com
omaha.cfe.uber.com
omsk.cfe.uber.com
orlando.cfe.uber.com
ottawa.cfe.uber.com
oxford.cfe.uber.com


Applications Places Terminal
Fri 21:56
root@kali: ~/Downloads/Sublist3r-master
File Edit View Search Terminal Help
bhubaneswar.cfe.uber.com
billings.cfe.uber.com
birmingham.cfe.uber.com
birmingham-al.cfe.uber.com
bloomington.cfe.uber.com
bogota.cfe.uber.com
boise.cfe.uber.com
bordeaux.cfe.uber.com
boston.cfe.uber.com
boulder.cfe.uber.com
bratislava.cfe.uber.com
brisbane.cfe.uber.com
bristol.cfe.uber.com
brussels.cfe.uber.com
budapest.cfe.uber.com
burlington.cfe.uber.com
cairo.cfe.uber.com
cali.cfe.uber.com
campinas.cfe.uber.com
canberra.cfe.uber.com
cardiff.cfe.uber.com
cartagena.cfe.uber.com
casablanca.cfe.uber.com
cel-dcal.cfe.uber.com
chandigarh.cfe.uber.com
charleston.cfe.uber.com
chelyabinsk.cfe.uber.com
chennai.cfe.uber.com
sublister2

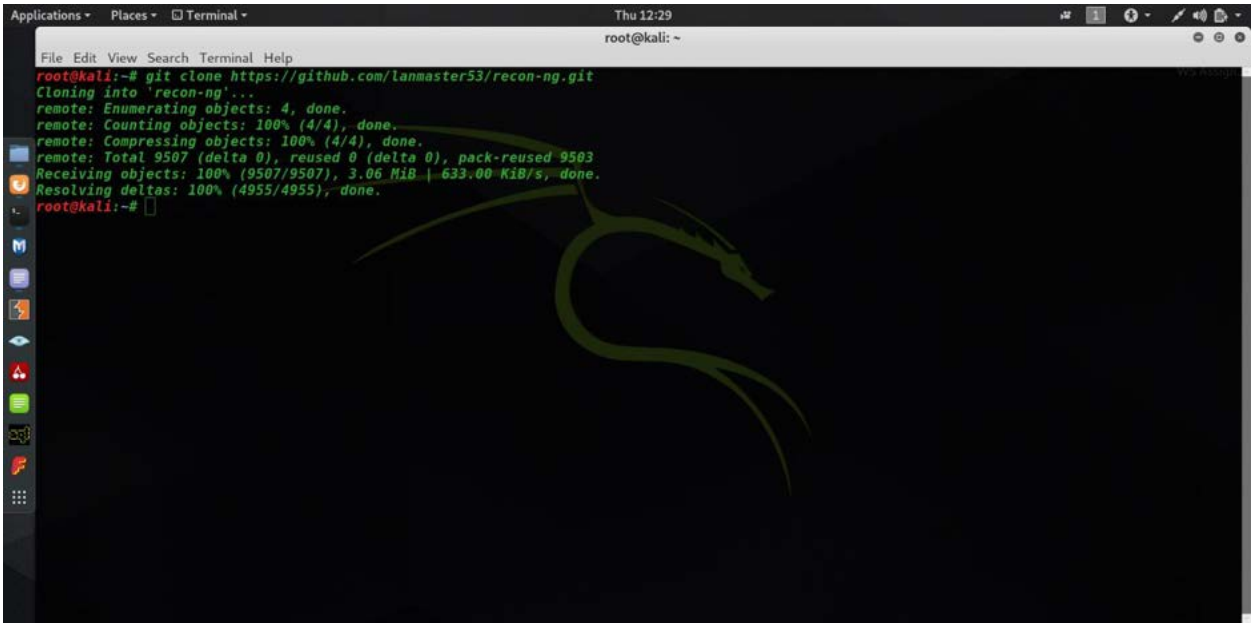


2. Recon –ng Tools

Installation:

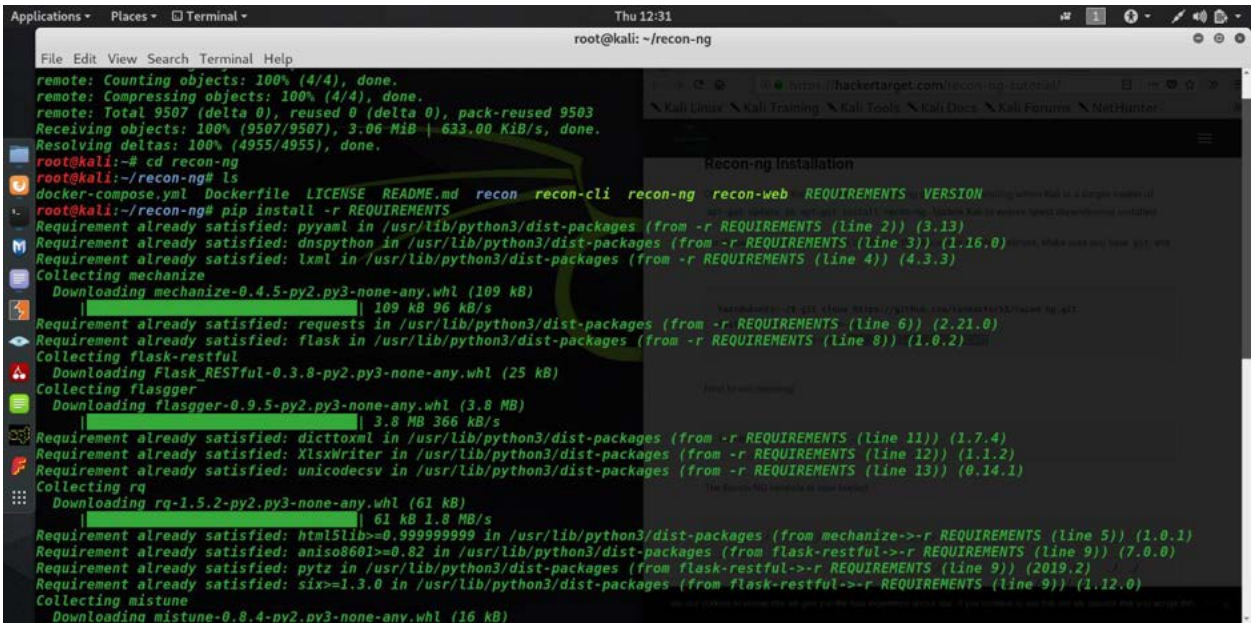
Go to the following link and clone it to the machine.

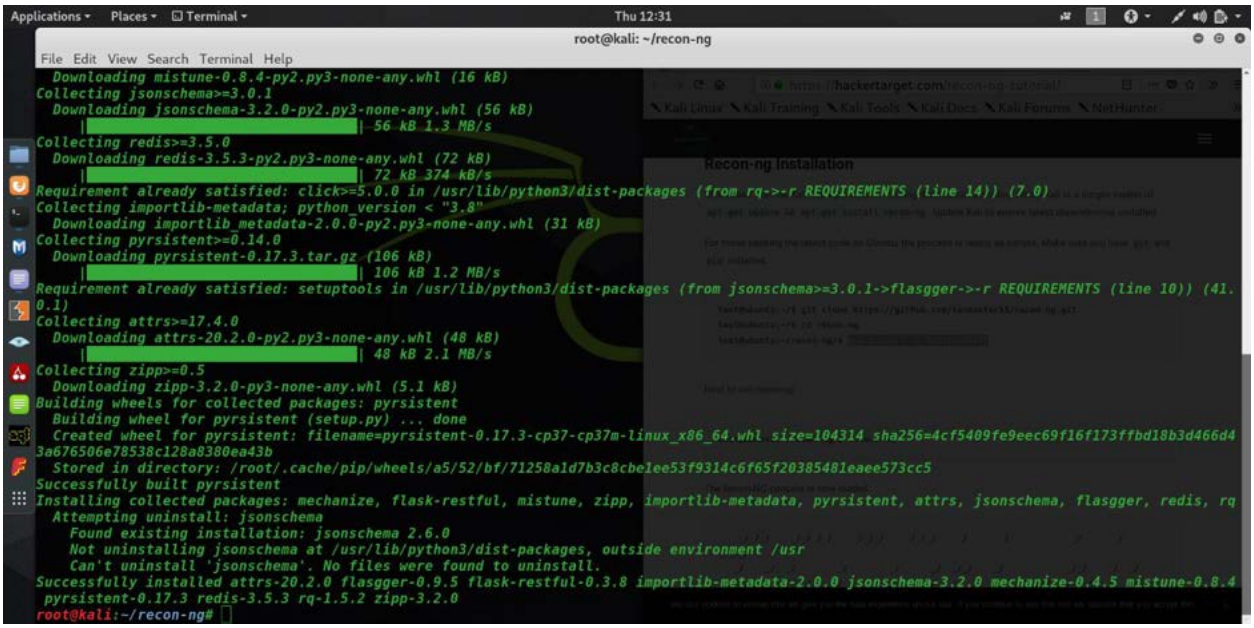
Github link: https://github.com/lanmaster53/recon-ng



Open the recon-ng directory and installing recon – ng by giving the following command.

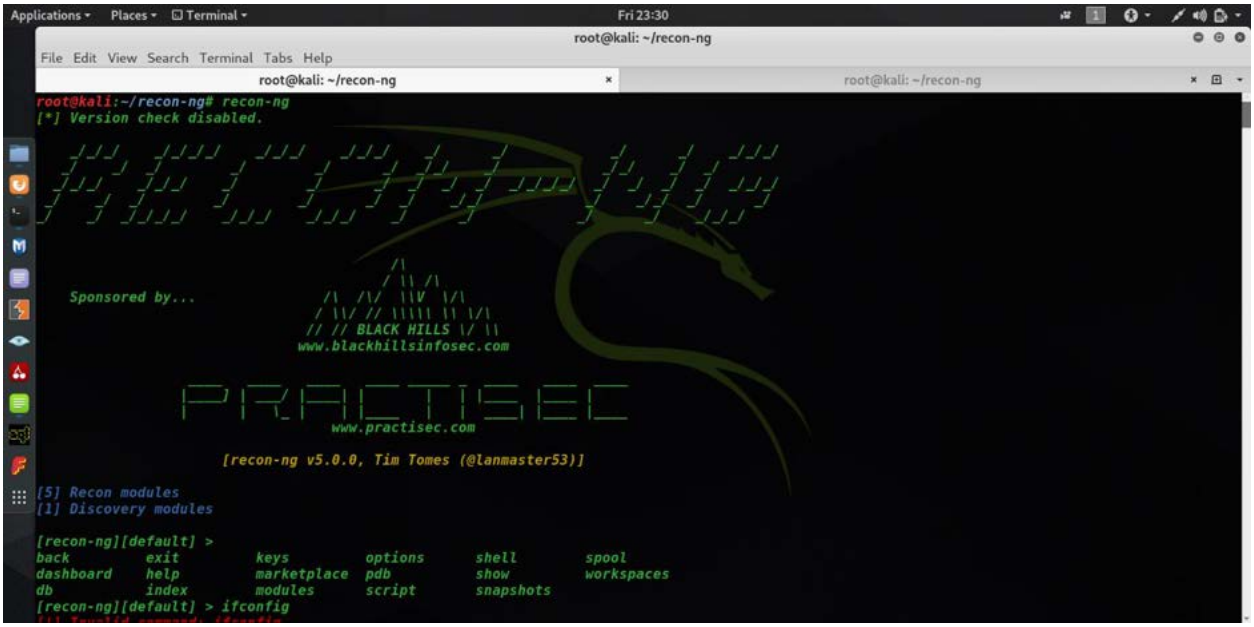
```
$ pip install -r REQUIREMENTS
```

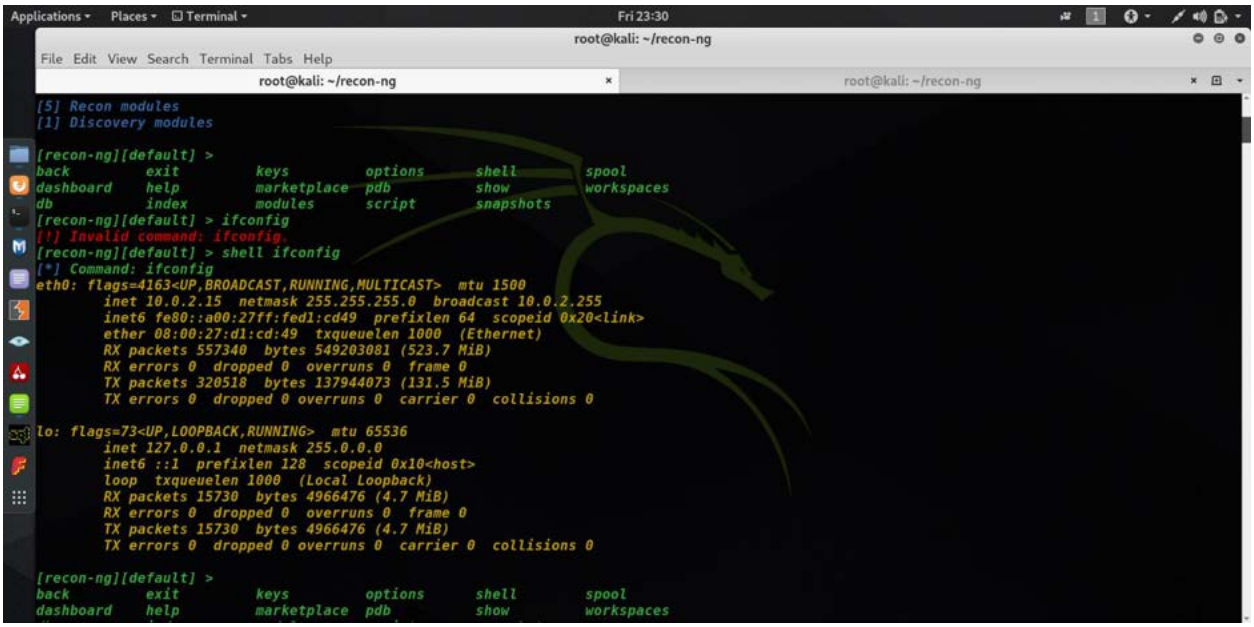


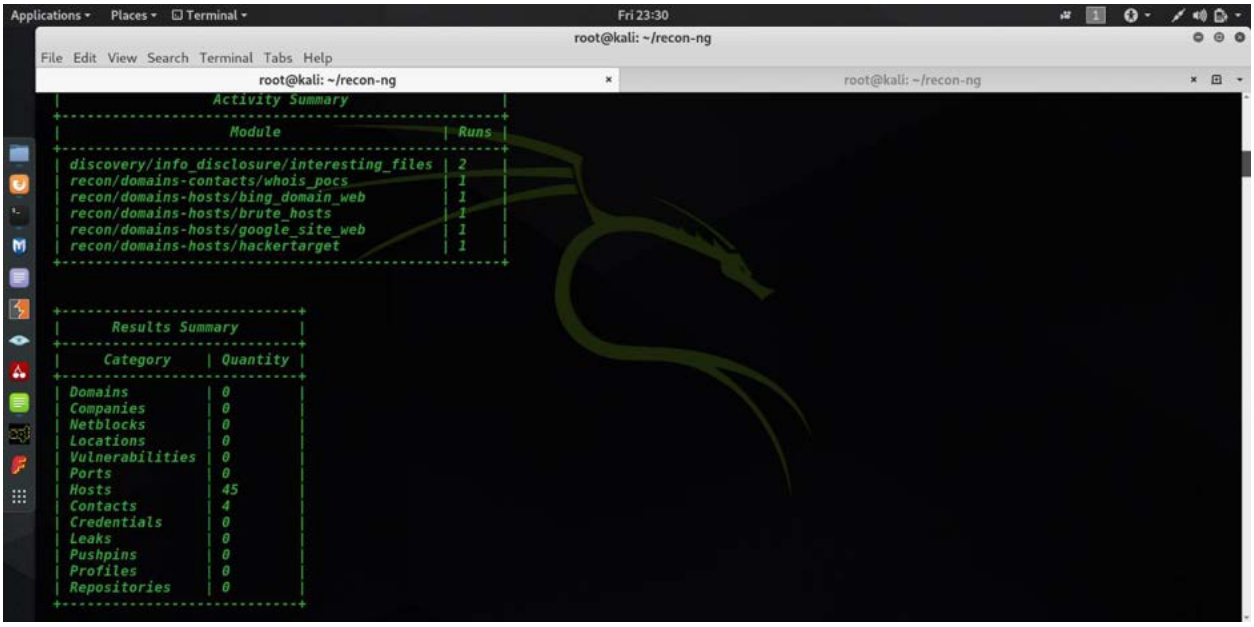


Proof of Concept:

To run the recon – ng, type recon and we can get the options by pressing the Tab button.

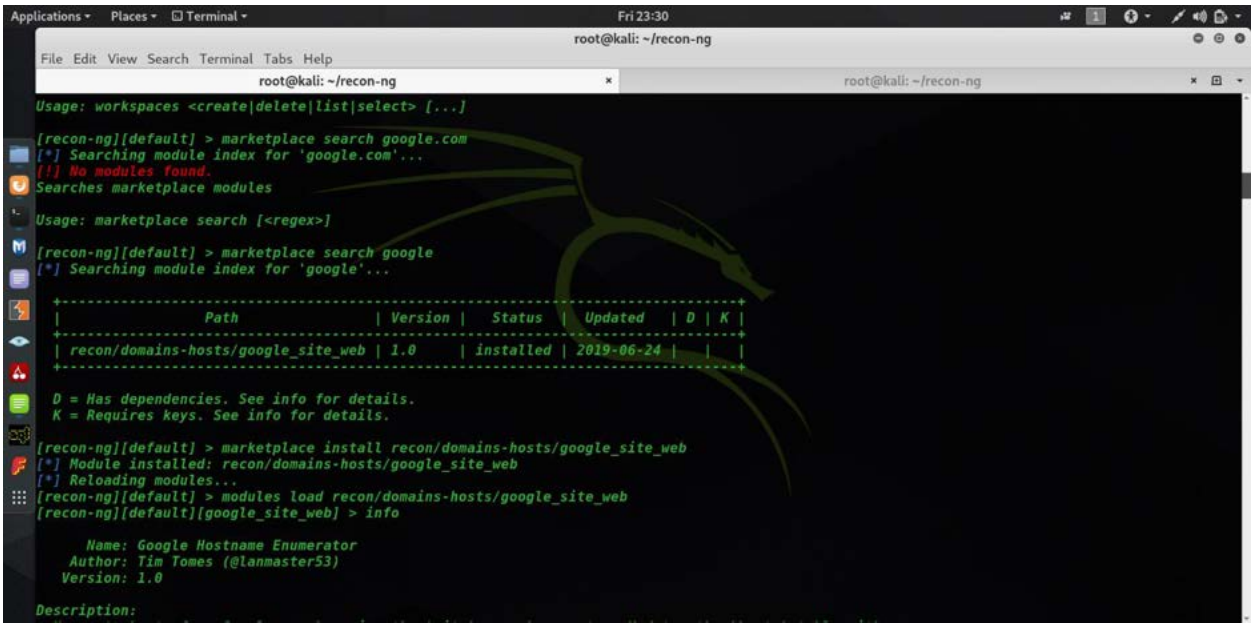


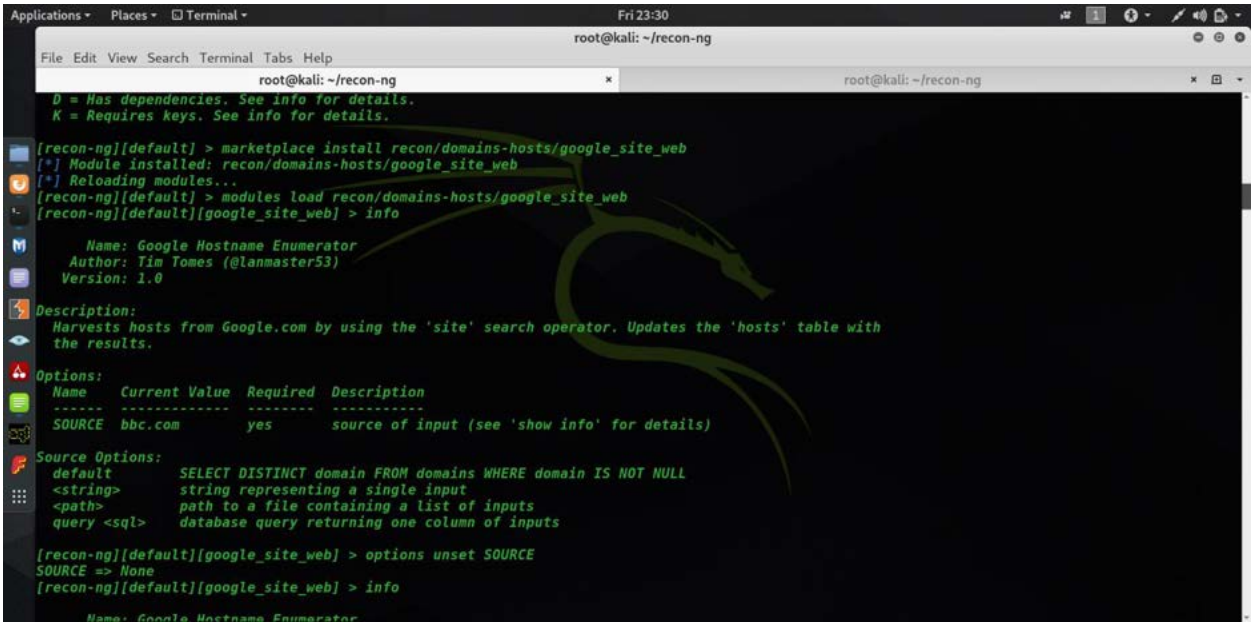




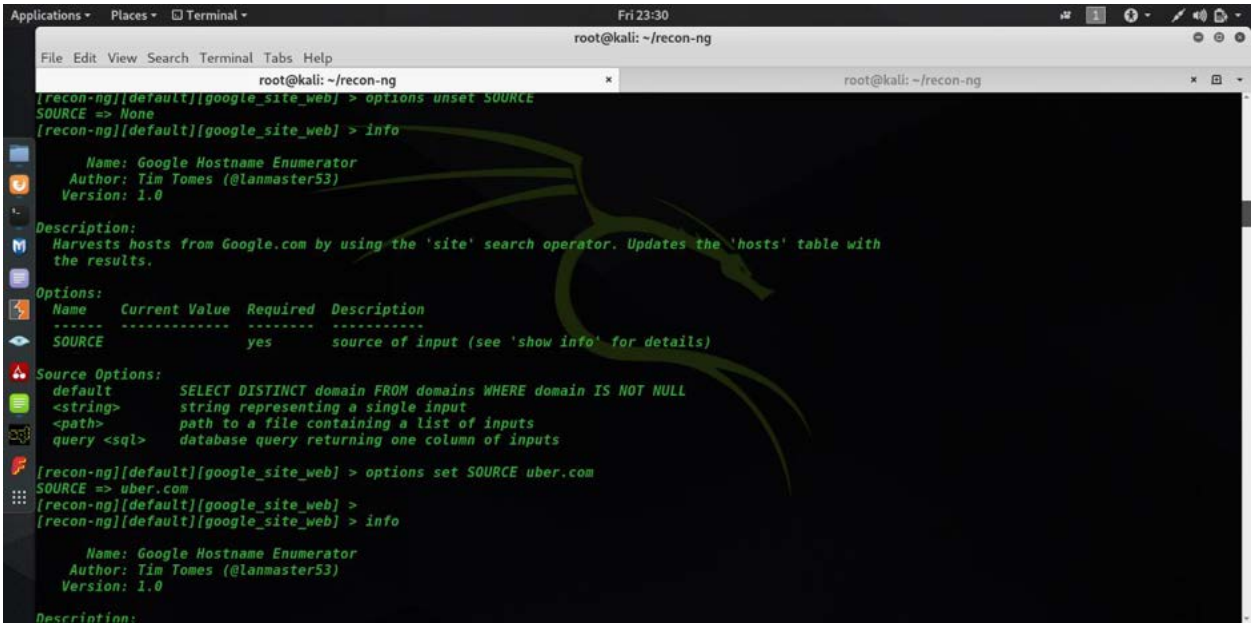
To get the google site web, I used the marketplace search command.

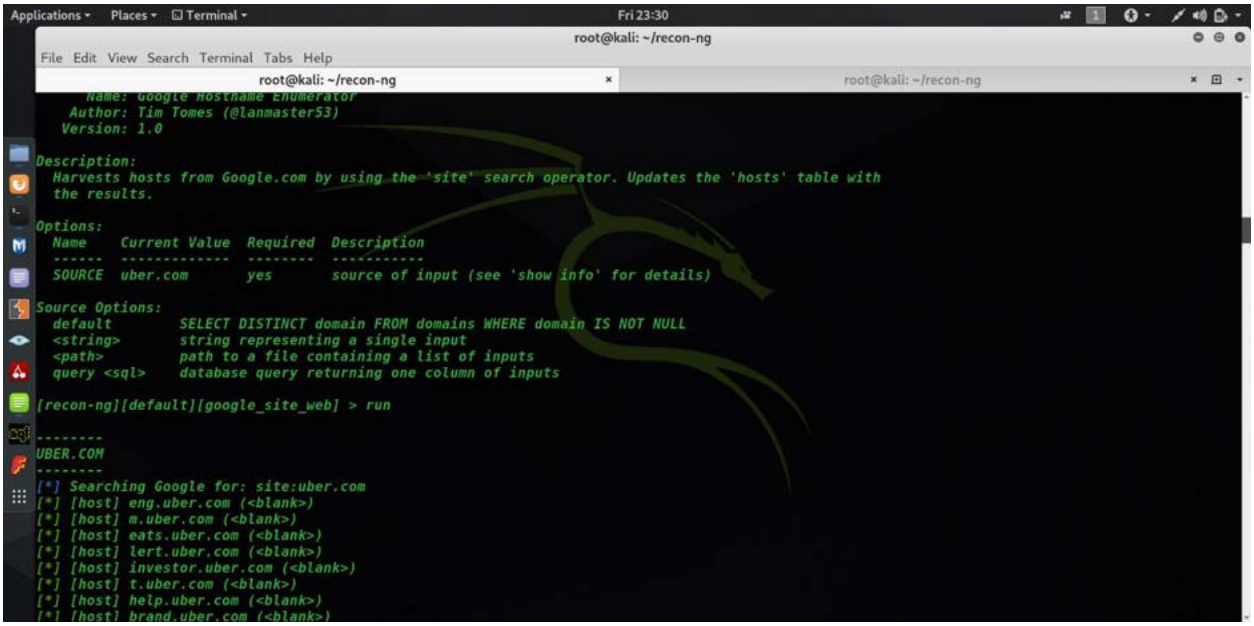
Then install it and load that marketplace.





Afterload the marketplace I set the current value into my target domain.


Applications Places Terminal Fri 23:30
root@kali: ~/recon-ng
File Edit View Search Terminal Tabs Help
root@kali: ~/recon-ng
root@kali: ~/recon-ng
[recon-ng][default][google_site_web] > options unset SOURCE
SOURCE => None
[recon-ng][default][google_site_web] > info
Name: Google Hostname Enumerator
Author: Tim Tomes (@lanmaster53)
Version: 1.0
Description:
Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results.
Options:
Name Current Value Required Description
SOURCE yes source of input (see 'show info' for details)
Source Options:
default SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string> string representing a single input
<path> path to a file containing a list of inputs
query <sql> database query returning one column of inputs
[recon-ng][default][google_site_web] > options set SOURCE uber.com
SOURCE => uber.com
[recon-ng][default][google_site_web] >
[recon-ng][default][google_site_web] > info
Name: Google Hostname Enumerator
Author: Tim Tomes (@lanmaster53)
Version: 1.0
Description:


Applications Places Terminal Fri 23:30
root@kali: ~/recon-ng
File Edit View Search Terminal Tabs Help
root@kali: ~/recon-ng
root@kali: ~/recon-ng
Name: Google Hostname Enumerator
Author: Tim Tomes (@lanmaster53)
Version: 1.0
Description:
Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results.
Options:
Name Current Value Required Description
SOURCE uber.com yes source of input (see 'show info' for details)
Source Options:
default SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string> string representing a single input
<path> path to a file containing a list of inputs
query <sql> database query returning one column of inputs
[recon-ng][default][google_site_web] > run
UBER.COM
[*] Searching Google for: site:uber.com
[*] [host] eng.uber.com (<blank>)
[*] [host] m.uber.com (<blank>)
[*] [host] eats.uber.com (<blank>)
[*] [host] lert.uber.com (<blank>)
[*] [host] investor.uber.com (<blank>)
[*] [host] t.uber.com (<blank>)
[*] [host] help.uber.com (<blank>)
[*] [host] brand.uber.com (<blank>)

3. Bug Bounty hunting Tool (BBHT) by Nahamsec

Bug Bounty Hunting Tools is a script to install the most popular tools used while looking for vulnerabilities for a bug bounty program.

Github link: https://github.com/nahamsec/bbht

Available tools:

- dirsearch
- JSParser
- knockpy
- lazys3
- recon_profile
- sqlmap-dev
- Sublist3r
- teh_s3_bucketeers
- virtual-host-discovery
- wpscan
- webscreenshot

- Massdns
- Asnlookup
- Unfurl
- Waybackurls
- Httprobe
- Seclists collection

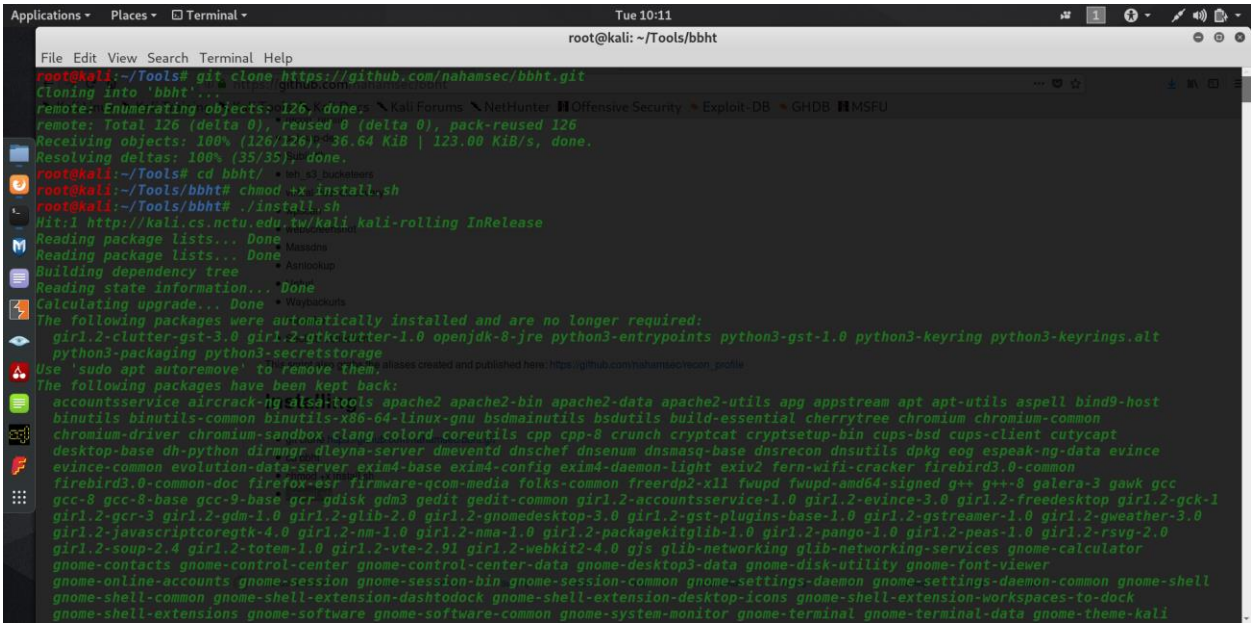
Installation:

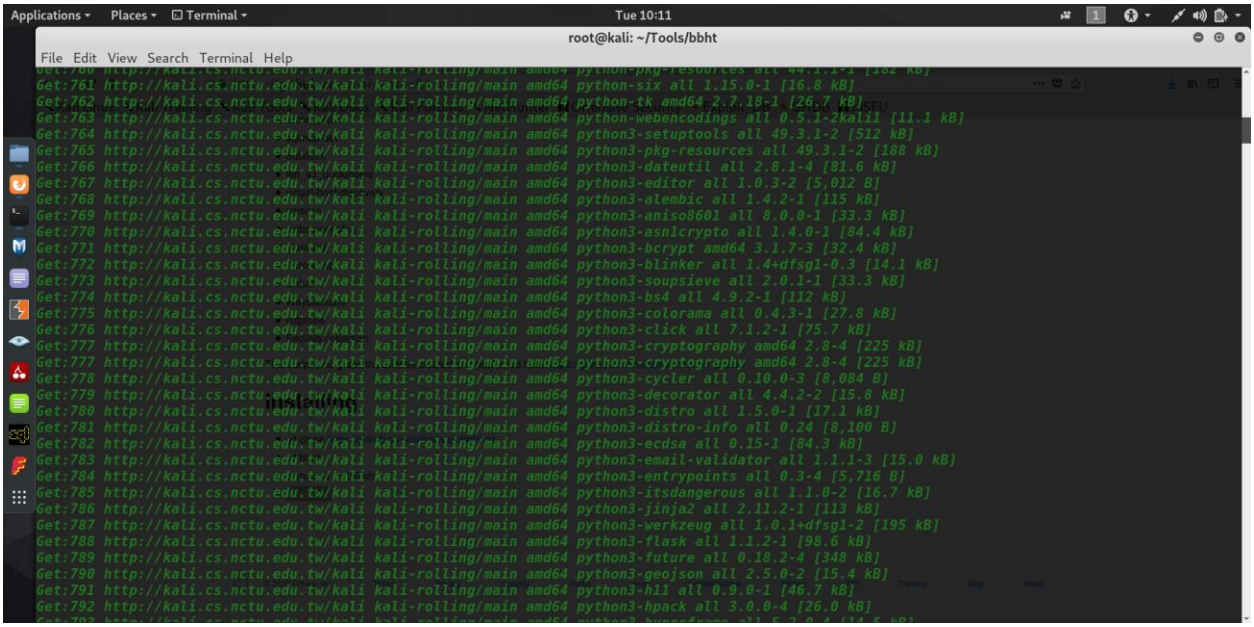
```
git clone https://github.com/nahamsec/bbht.git
cd bbht
chmod +x install.sh
./install.sh
```

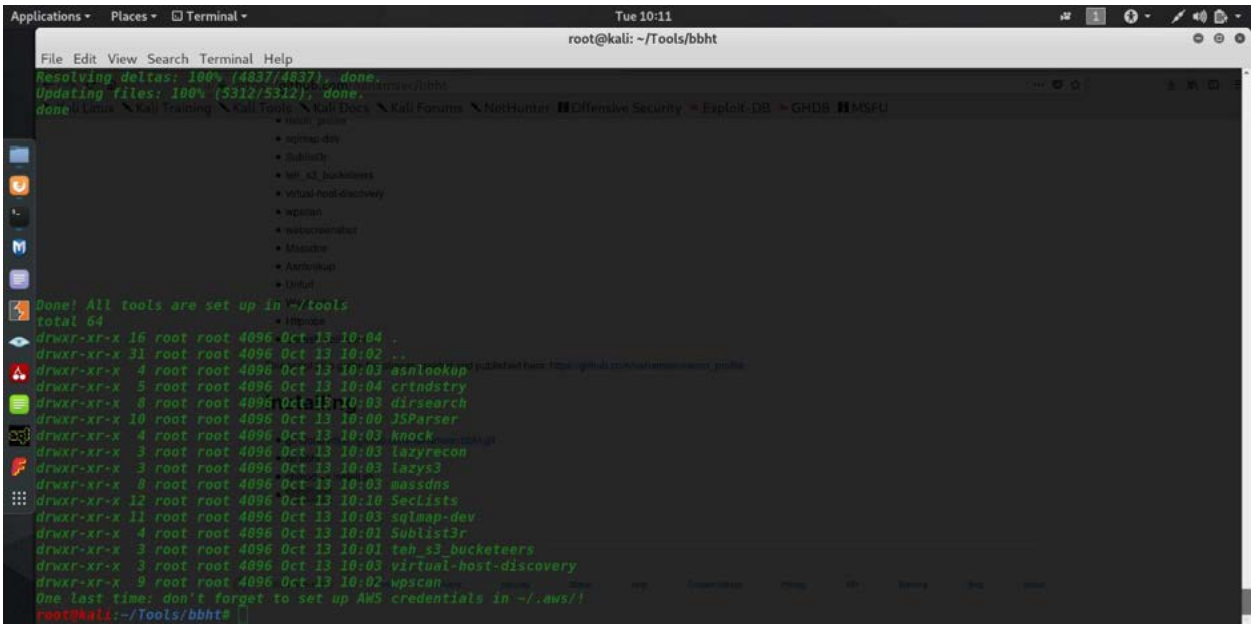
After installing bbht tool we should copy the nahamsec recon_profile to our ./bash_profile

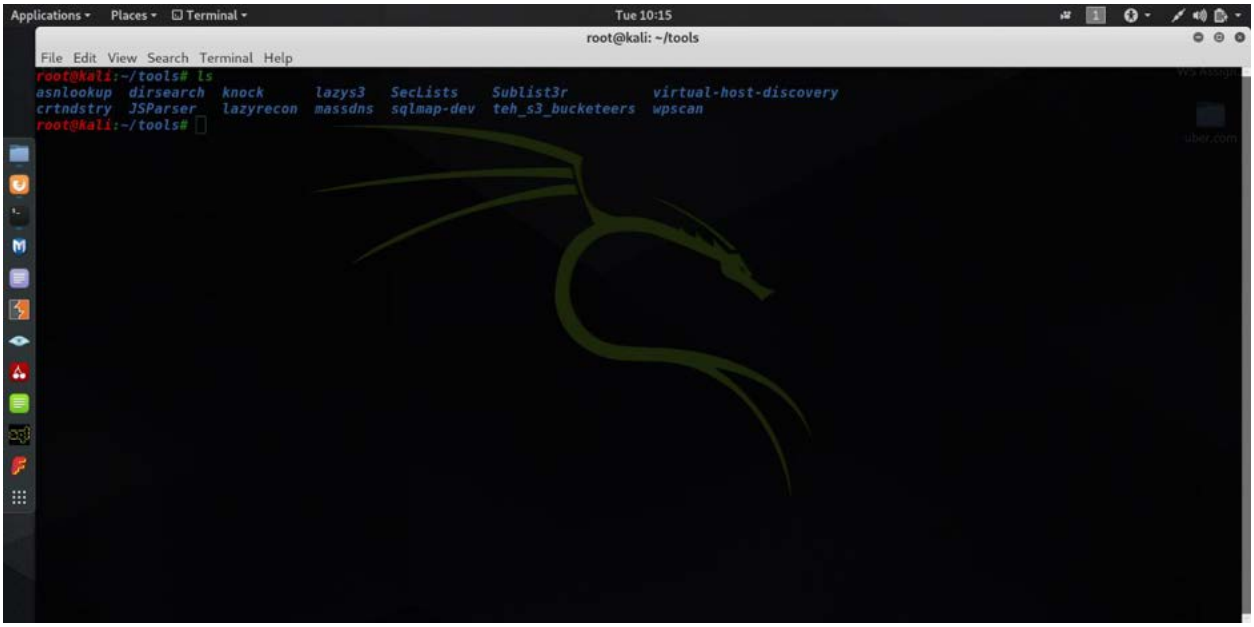
Github link: https://github.com/nahamsec/recon_profile

Proof of concept




Applications Places Terminal Tue 10:11
root@kali: ~/Tools/bbht
File Edit View Search Terminal Help
Get:761 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python-six all 1.15.0-1 [16.8 kB]
Get:762 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python-tk amd64 2.7.18-1 [26.7 kB]
Get:763 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python-webencodings all 0.5.1-2kali1 [11.1 kB]
Get:764 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-setuptools all 49.3.1-2 [512 kB]
Get:765 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-pkg-resources all 49.3.1-2 [188 kB]
Get:766 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-dateutil all 2.8.1-4 [81.6 kB]
Get:767 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-editor all 1.0.3-2 [5,012 B]
Get:768 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-alembic all 1.4.2-1 [115 kB]
Get:769 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-aniso8601 all 8.0.0-1 [33.3 kB]
Get:770 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-asn1crypto all 1.4.0-1 [84.4 kB]
Get:771 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-bcrypt amd64 3.1.7-3 [32.4 kB]
Get:772 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-blinker all 1.4+dfsg1-0.3 [14.1 kB]
Get:773 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-soupsieve all 2.0.1-1 [33.3 kB]
Get:774 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-bs4 all 4.9.2-1 [112 kB]
Get:775 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-colorama all 0.4.3-1 [27.8 kB]
Get:776 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-click all 7.1.2-1 [75.7 kB]
Get:777 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-cryptography amd64 2.8-4 [225 kB]
Get:777 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-cryptography amd64 2.8-4 [225 kB]
Get:778 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-cycler all 0.10.0-3 [8,084 B]
Get:779 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-decorator all 4.4.2-2 [15.8 kB]
Get:780 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-distro all 1.5.0-1 [17.1 kB]
Get:781 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-distro-info all 0.24 [8,100 B]
Get:782 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-ecdsa all 0.15-1 [84.3 kB]
Get:783 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-email-validator all 1.1.1-3 [15.0 kB]
Get:784 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-entrypoints all 0.3-4 [5,716 B]
Get:785 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-itsdangerous all 1.1.0-2 [16.7 kB]
Get:786 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-jinja2 all 2.11.2-1 [113 kB]
Get:787 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-werkzeug all 1.0.1+dfsg1-2 [195 kB]
Get:788 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-flask all 1.1.2-1 [98.6 kB]
Get:789 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-future all 0.18.2-4 [348 kB]
Get:790 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-geojson all 2.5.0-2 [15.4 kB]
Get:791 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-h11 all 0.9.0-1 [46.7 kB]
Get:792 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 python3-hpack all 3.0.0-4 [26.0 kB]

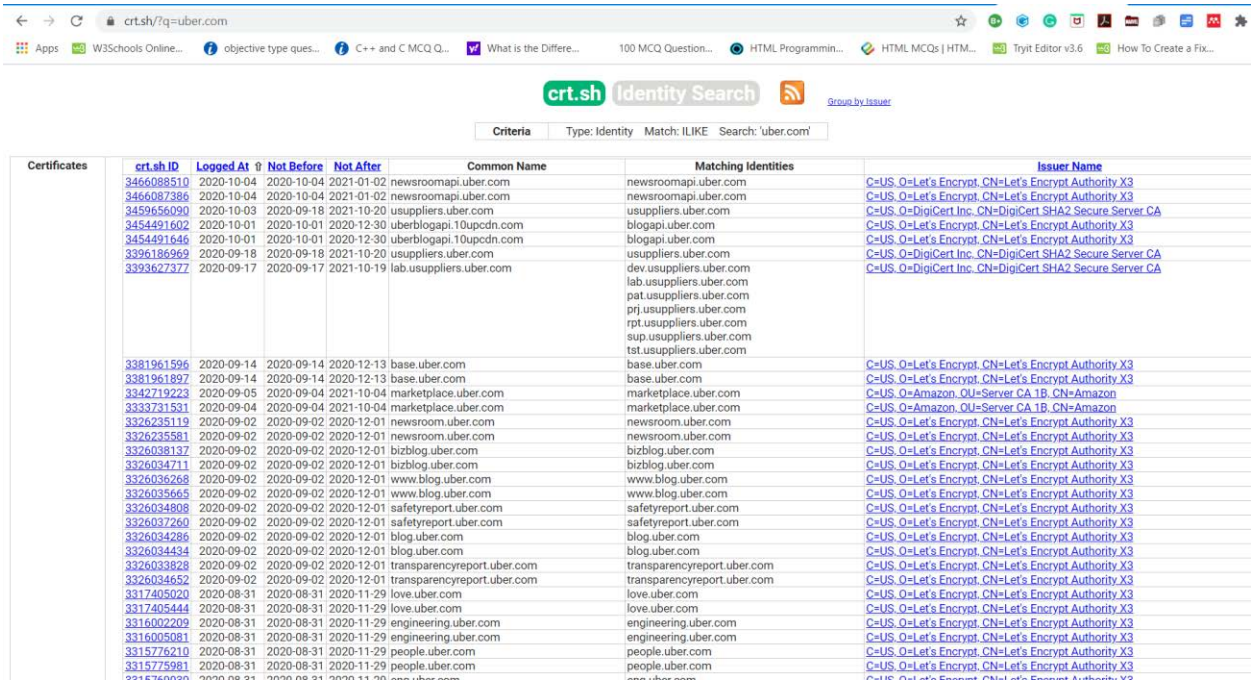

Applications Places Terminal Tue 10:11
root@kali: ~/Tools/bbht
File Edit View Search Terminal Help
Resolving deltas: 100% (4837/4837), done.
Updating files: 100% (5312/5312), done.
done
Done! All tools are set up in ~/tools
total 64
drwxr-xr-x 16 root root 4096 Oct 13 10:04 .
drwxr-xr-x 31 root root 4096 Oct 13 10:02 ..
drwxr-xr-x 4 root root 4096 Oct 13 10:03 asnlookup
drwxr-xr-x 5 root root 4096 Oct 13 10:04 crtndstry
drwxr-xr-x 8 root root 4096 Oct 13 10:03 dirsearch
drwxr-xr-x 10 root root 4096 Oct 13 10:00 JSParser
drwxr-xr-x 4 root root 4096 Oct 13 10:03 knock
drwxr-xr-x 3 root root 4096 Oct 13 10:03 lazyrecon
drwxr-xr-x 3 root root 4096 Oct 13 10:03 lazys3
drwxr-xr-x 8 root root 4096 Oct 13 10:03 massdns
drwxr-xr-x 12 root root 4096 Oct 13 10:10 SecLists
drwxr-xr-x 11 root root 4096 Oct 13 10:03 sqlmap-dev
drwxr-xr-x 4 root root 4096 Oct 13 10:01 Sublist3r
drwxr-xr-x 3 root root 4096 Oct 13 10:01 teh_s3_bucketeers
drwxr-xr-x 3 root root 4096 Oct 13 10:03 virtual-host-discovery
drwxr-xr-x 9 root root 4096 Oct 13 10:02 wpscan
One last time: don't forget to set up AWS credentials in ~/.aws/!
root@kali:~/Tools/bbht#



4. Crt.sh

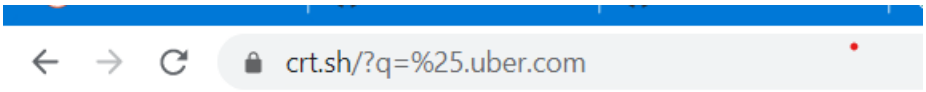
Website link: https://crt.sh/

I also used crt.sh for finding subdomains. Then I created one file called all.txt which contains all the sub domains I have found.



crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
3466088510	2020-10-04	2020-10-04	2021-01-02	newsroomapi.uber.com	newsroomapi.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3466087386	2020-10-04	2020-10-04	2021-01-02	newsroomapi.uber.com	newsroomapi.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3459656090	2020-10-03	2020-09-18	2021-10-20	usuppliers.uber.com	usuppliers.uber.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
3454491602	2020-10-01	2020-10-01	2020-12-30	uberblogapi.10upcdn.com	blogapi.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3454491646	2020-10-01	2020-10-01	2020-12-30	uberblogapi.10upcdn.com	blogapi.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3396186969	2020-09-18	2020-09-18	2021-10-20	usuppliers.uber.com	usuppliers.uber.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
3393627377	2020-09-17	2020-09-17	2021-10-19	lab.usuppliers.uber.com	dev.usuppliers.uber.com lab.usuppliers.uber.com pat.usuppliers.uber.com prj.usuppliers.uber.com rpt.usuppliers.uber.com sup.usuppliers.uber.com tst.usuppliers.uber.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
3381961596	2020-09-14	2020-09-14	2020-12-13	base.uber.com	base.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3381961897	2020-09-14	2020-09-14	2020-12-13	base.uber.com	base.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3342719223	2020-09-05	2020-09-04	2021-10-04	marketplace.uber.com	marketplace.uber.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3333731531	2020-09-04	2020-09-04	2021-10-04	marketplace.uber.com	marketplace.uber.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3326235119	2020-09-02	2020-09-02	2020-12-01	newsroom.uber.com	newsroom.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3326235581	2020-09-02	2020-09-02	2020-12-01	newsroom.uber.com	newsroom.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3326038137	2020-09-02	2020-09-02	2020-12-01	bizblog.uber.com	bizblog.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3326034711	2020-09-02	2020-09-02	2020-12-01	bizblog.uber.com	bizblog.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3326036268	2020-09-02	2020-09-02	2020-12-01	www.blog.uber.com	www.blog.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3326035665	2020-09-02	2020-09-02	2020-12-01	www.blog.uber.com	www.blog.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3326034808	2020-09-02	2020-09-02	2020-12-01	safetyreport.uber.com	safetyreport.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3326037260	2020-09-02	2020-09-02	2020-12-01	safetyreport.uber.com	safetyreport.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3326034286	2020-09-02	2020-09-02	2020-12-01	blog.uber.com	blog.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3326034434	2020-09-02	2020-09-02	2020-12-01	blog.uber.com	blog.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3326033828	2020-09-02	2020-09-02	2020-12-01	transparencyreport.uber.com	transparencyreport.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3326034652	2020-09-02	2020-09-02	2020-12-01	transparencyreport.uber.com	transparencyreport.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3317405020	2020-08-31	2020-08-31	2020-11-29	love.uber.com	love.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3317405444	2020-08-31	2020-08-31	2020-11-29	love.uber.com	love.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3316002209	2020-08-31	2020-08-31	2020-11-29	engineering.uber.com	engineering.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3316005081	2020-08-31	2020-08-31	2020-11-29	engineering.uber.com	engineering.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3315776210	2020-08-31	2020-08-31	2020-11-29	people.uber.com	people.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3315775981	2020-08-31	2020-08-31	2020-11-29	people.uber.com	people.uber.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

I used wild cards for crawling more subdomains.

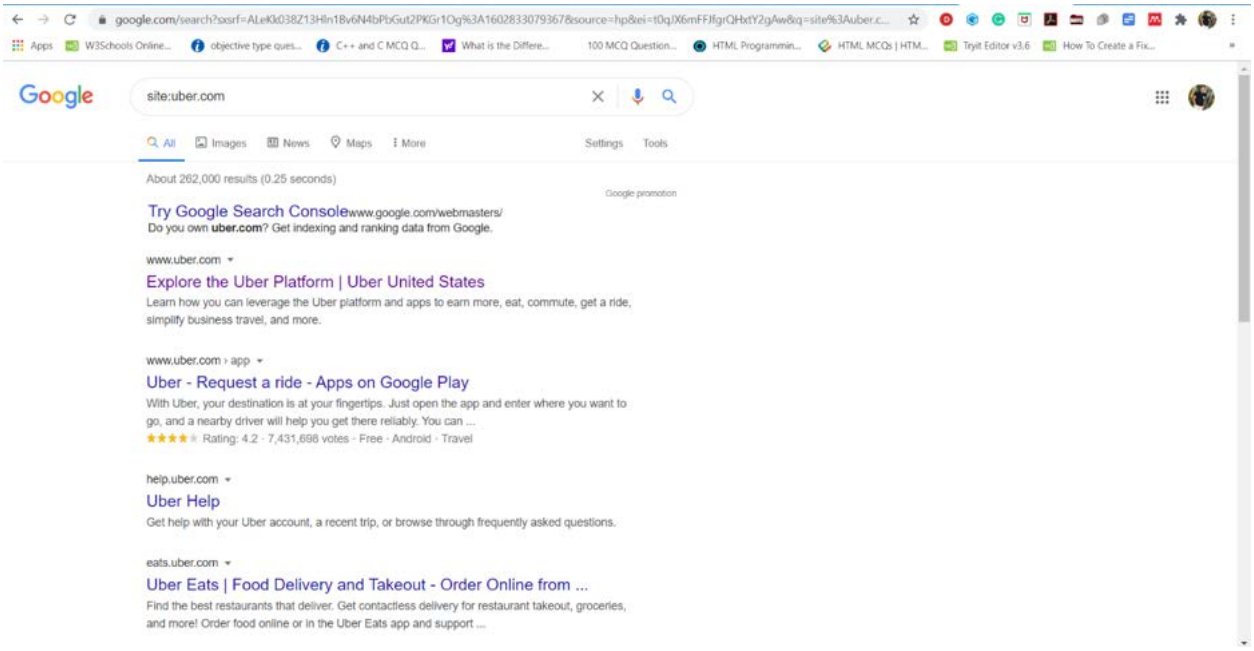


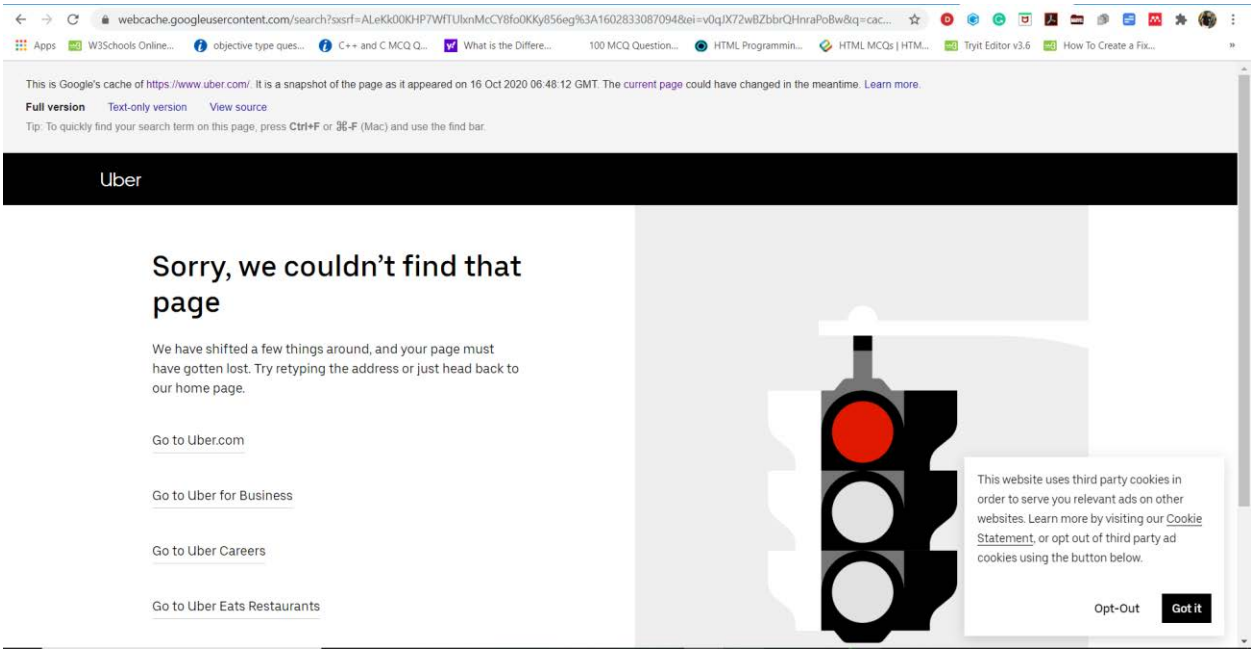
Here I consider more about the following sub-domains because those are the most important for any organization.

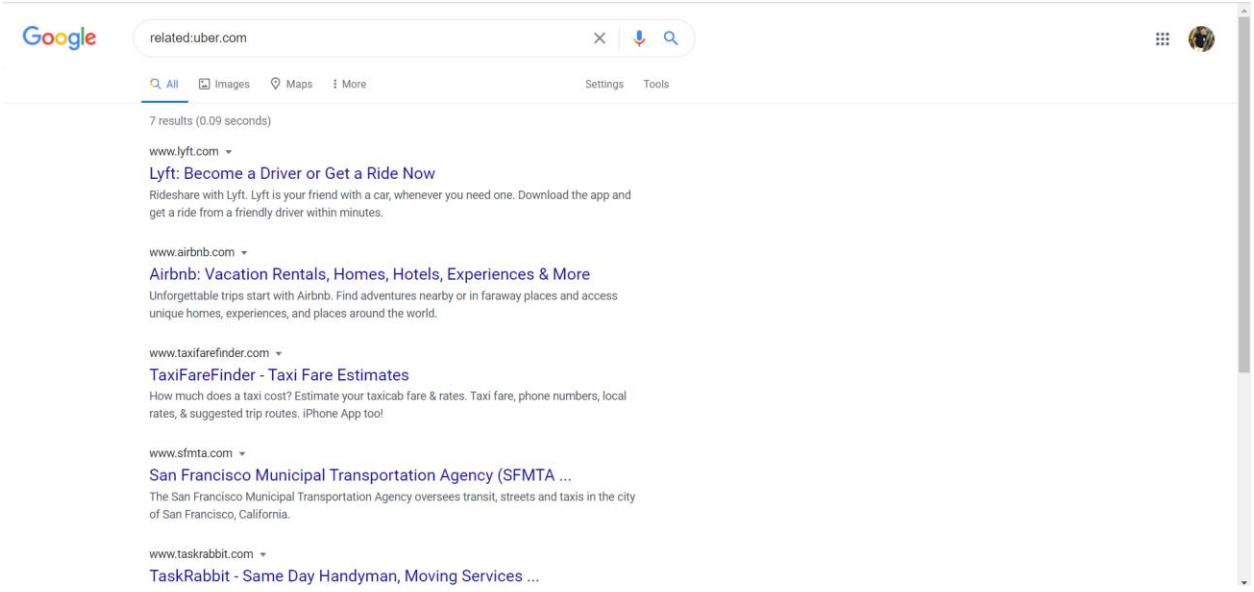
```
%api%
%corp%
%internal%
```

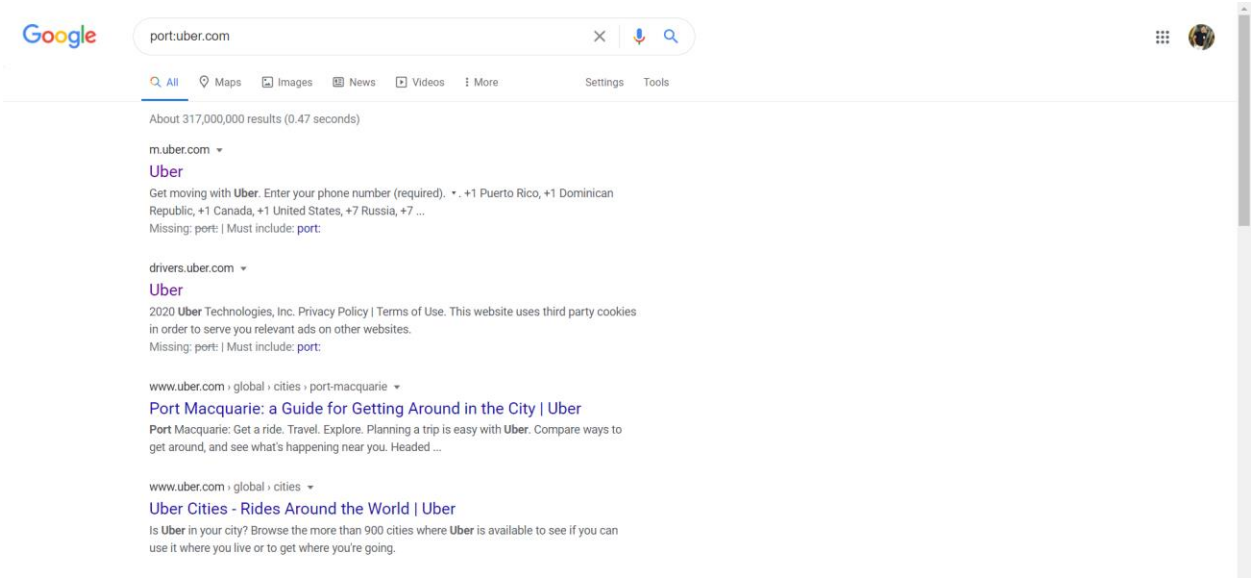
Then I have found more interesting sub dominos and I include all these to all.txt

5. Google dork




webcache.googleusercontent.com/search?sxsrf=ALeKk00KHP7WfTUlxnMcCY8fo0KKy856eg%3A1602833087094&ei=v0qJX72wBZbbrQHnraPoBw&q=cac...
Apps
W3Schools Online...
objective type ques...
C++ and C MCQ Q...
What is the Differe...
100 MCQ Question...
HTML Programmin...
HTML MCQs | HTM...
Tryit Editor v3.6
How To Create a Fix...
This is Google's cache of https://www.uber.com/. It is a snapshot of the page as it appeared on 16 Oct 2020 06:48:12 GMT. The current page could have changed in the meantime. Learn more.
Full version
Text-only version
View source
Tip: To quickly find your search term on this page, press Ctrl+F or ⌘-F (Mac) and use the find bar.
Uber
Sorry, we couldn't find that page
We have shifted a few things around, and your page must have gotten lost. Try retyping the address or just head back to our home page.
Go to Uber.com
Go to Uber for Business
Go to Uber Careers
Go to Uber Eats Restaurants
This website uses third party cookies in order to serve you relevant ads on other websites. Learn more by visiting our Cookie Statement, or opt out of third party ad cookies using the button below.
Opt-Out
Got it

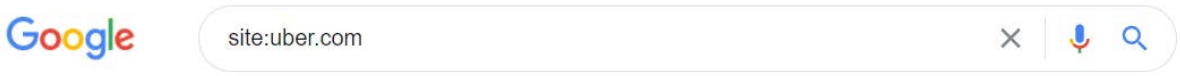

Google
related:uber.com
All
Images
Maps
More
Settings
Tools
7 results (0.09 seconds)
www.lyft.com
Lyft: Become a Driver or Get a Ride Now
Rideshare with Lyft. Lyft is your friend with a car, whenever you need one. Download the app and get a ride from a friendly driver within minutes.
www.airbnb.com
Airbnb: Vacation Rentals, Homes, Hotels, Experiences & More
Unforgettable trips start with Airbnb. Find adventures nearby or in faraway places and access unique homes, experiences, and places around the world.
www.taxifarefinder.com
TaxiFareFinder - Taxi Fare Estimates
How much does a taxi cost? Estimate your taxicab fare & rates. Taxi fare, phone numbers, local rates, & suggested trip routes. iPhone App too!
www.sfmta.com
San Francisco Municipal Transportation Agency (SFMTA ...
The San Francisco Municipal Transportation Agency oversees transit, streets and taxis in the city of San Francisco, California.
www.taskrabbit.com
TaskRabbit - Same Day Handyman, Moving Services ...



Google dorks is another tool to use to find subdomains. This is a technique to find security holes in a website through Google search.

We can use **Site** operator for this.

```
site:www.uber.com
```



Then after getting the results we can try the negative of the previous result for subdomain enumeration.

Google web crawling can help to find usernames, passwords, and other sensitive information.

Example:

```
cache:www.uber.com
related:www.uber.com
```

Getting Alive Sub Domains

1. Httprobe

Github link: github.com/tomnomnom/httprobe

Httprobe is a tool that gives all live subdomains in our wordlist.

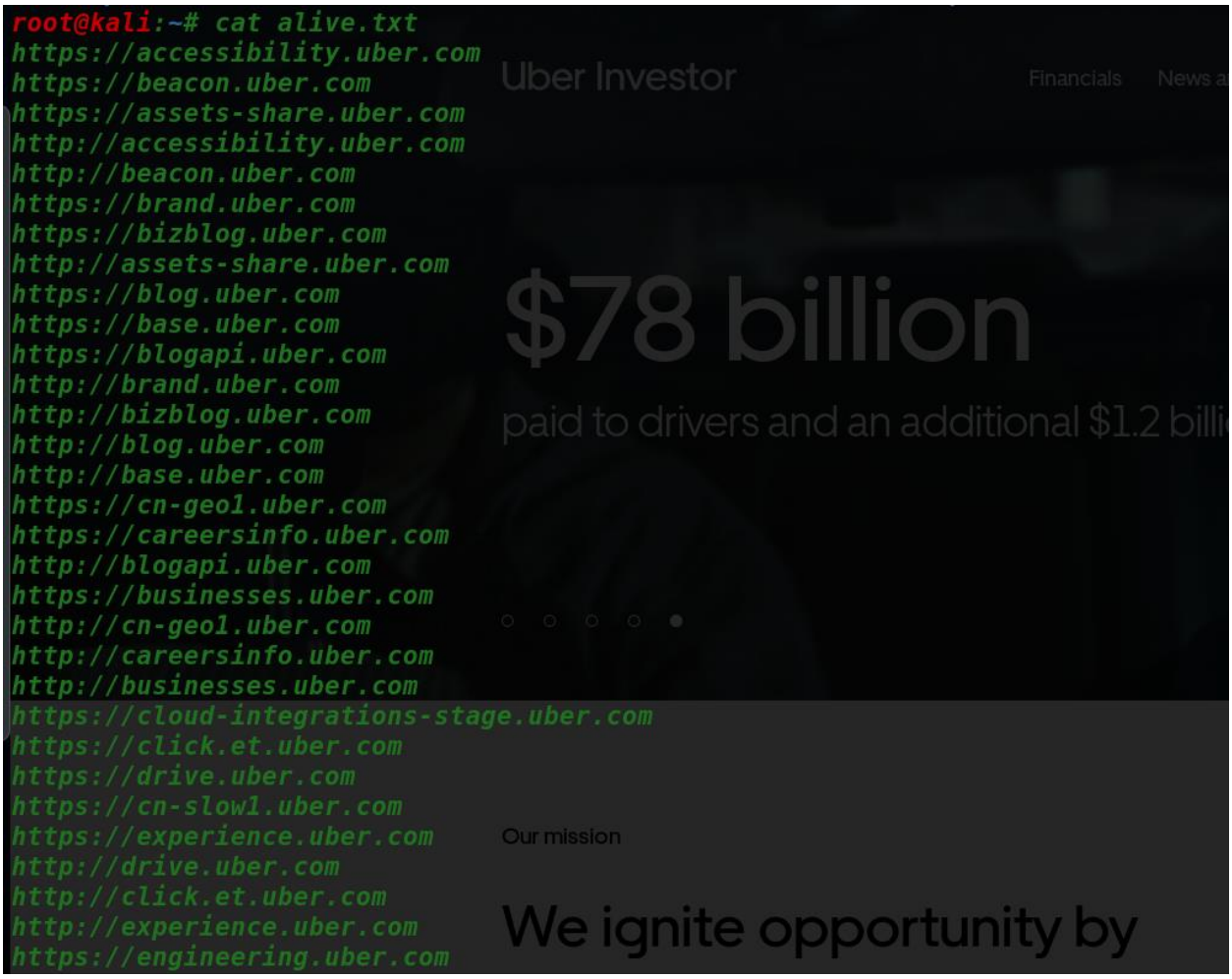
Installation:

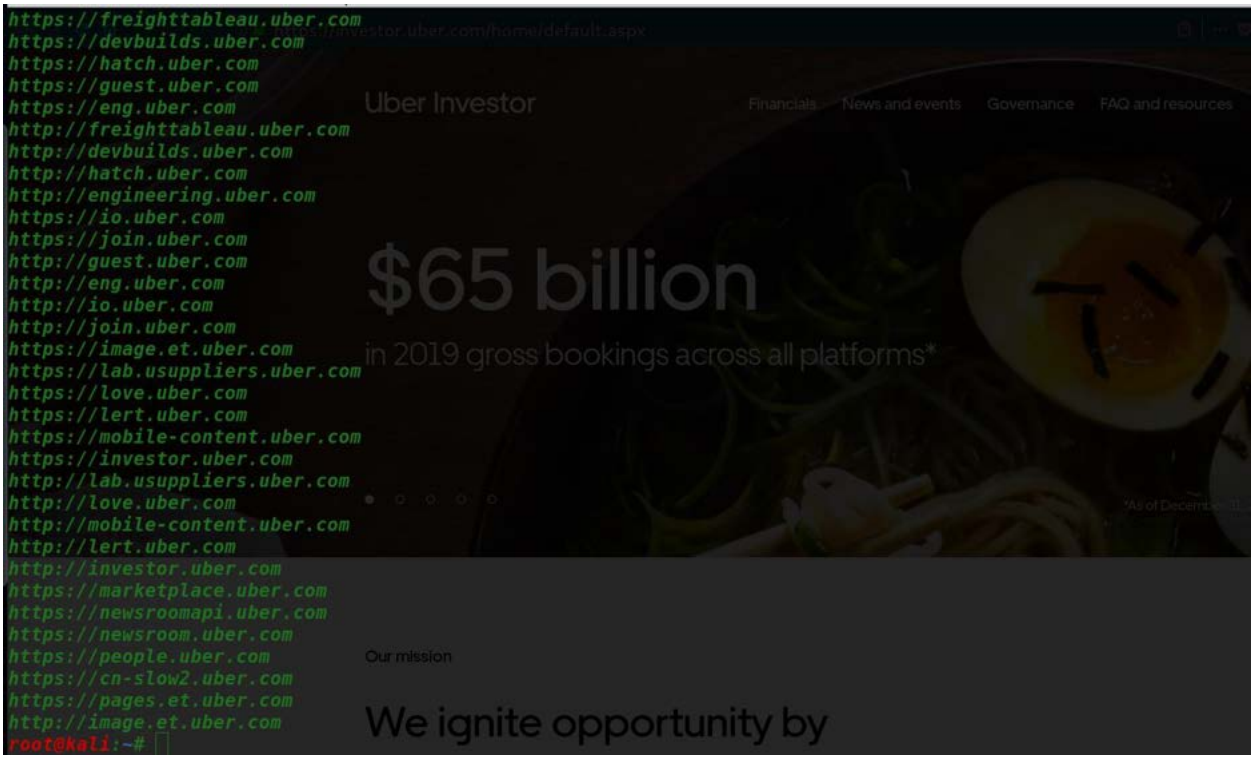
```
go get -u github.com/tomnomnom/httprobe
```

I saved all the alive sub-domains to the alive.txt file.

```
cat all.txt | httprobe >> alive.txt
```

Proof of concept:



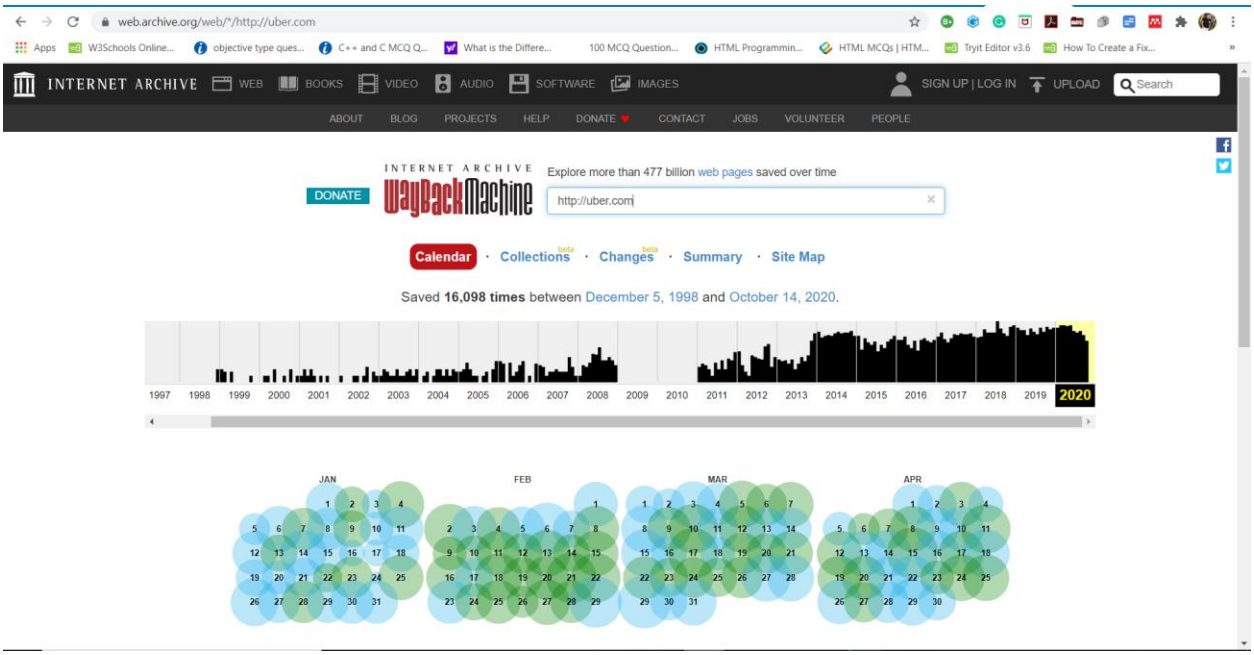


Finding Achieved information

1. Way Back Machine

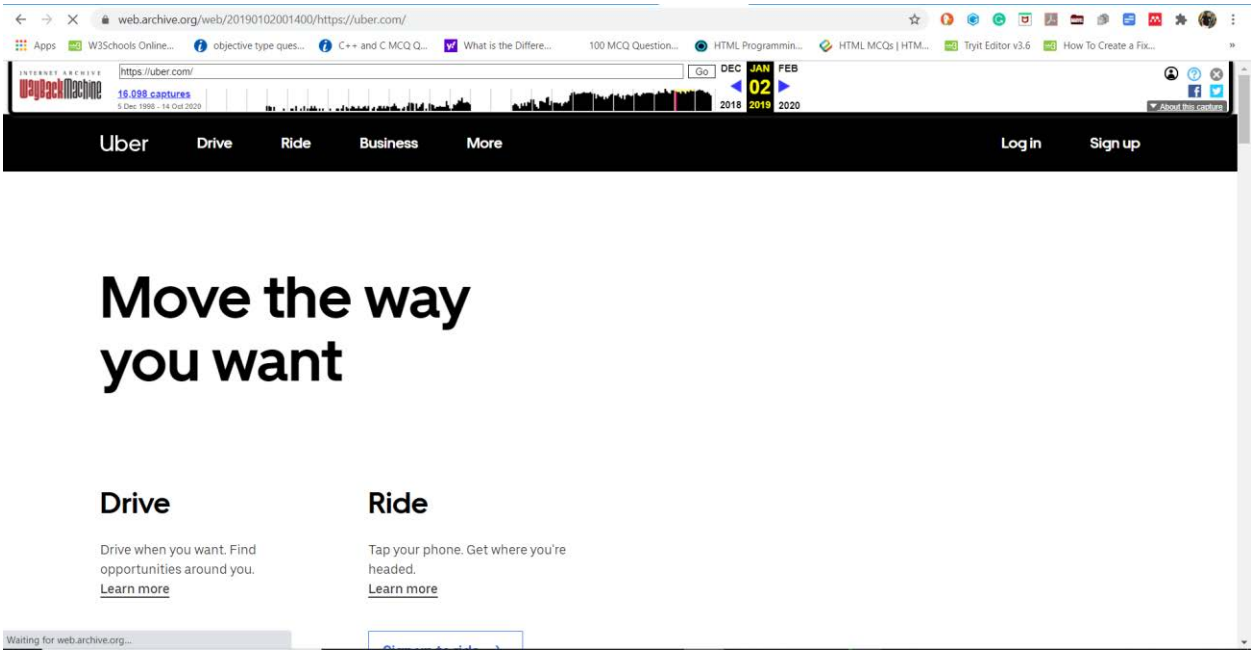
Website link: http://archive.org/web/

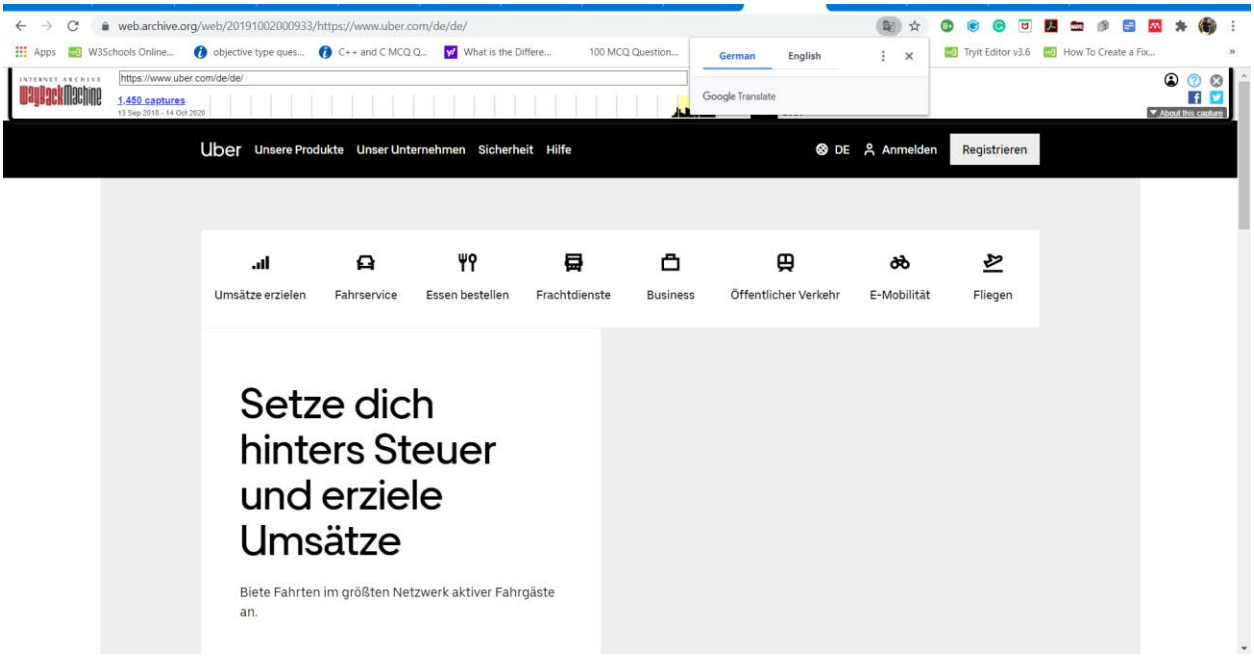
The Wayback Machine is an Internet archive, located at http://archive.org/web/. It's a collection of more than 349 billion snapshots of web pages saved over time. Wayback Machine contains copies of web pages, books, videos, audios, images, etc.

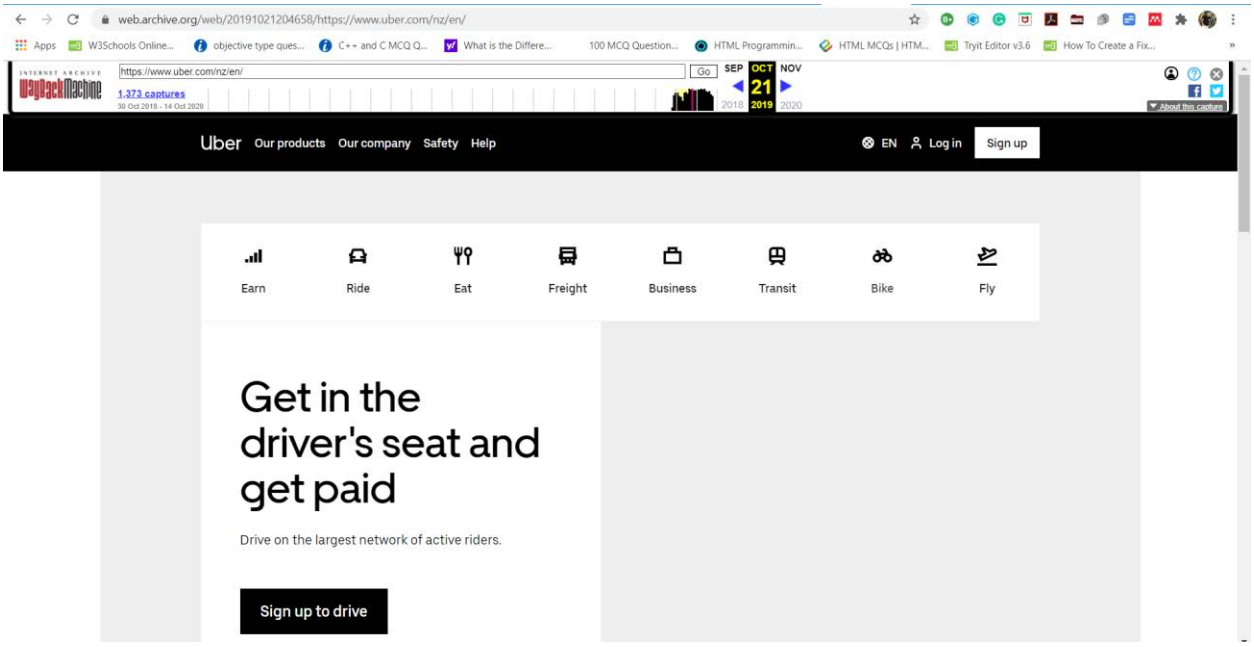


This is very helpful for information gathering because we can find some interesting data with this process. Such as,

- Old forgotten endpoints
- Interesting JS files
- Sensitive information




web.archive.org/web/20191002000933/https://www.uber.com/de/de/
https://www.uber.com/de/de/
1,450 captures
13 Sep 2018 - 14 Oct 2020
German
English
Google Translate
Uber
Unsere Produkte
Unser Unternehmen
Sicherheit
Hilfe
DE
Anmelden
Registrieren
Umsätze erzielen
Fahrservice
Essen bestellen
Frachtdienste
Business
Öffentlicher Verkehr
E-Mobilität
Fliegen
Setze dich hinters Steuer und erziele Umsätze
Biete Fahrten im größten Netzwerk aktiver Fahrgäste an.


web.archive.org/web/20191021204658/https://www.uber.com/nz/en/
https://www.uber.com/nz/en/
1,373 captures
30 Oct 2018 - 14 Oct 2020
Go
SEP
OCT
NOV
21
2018
2019
2020
Uber
Our products
Our company
Safety
Help
EN
Log in
Sign up
Earn
Ride
Eat
Freight
Business
Transit
Bike
Fly
Get in the driver's seat and get paid
Drive on the largest network of active riders.
Sign up to drive

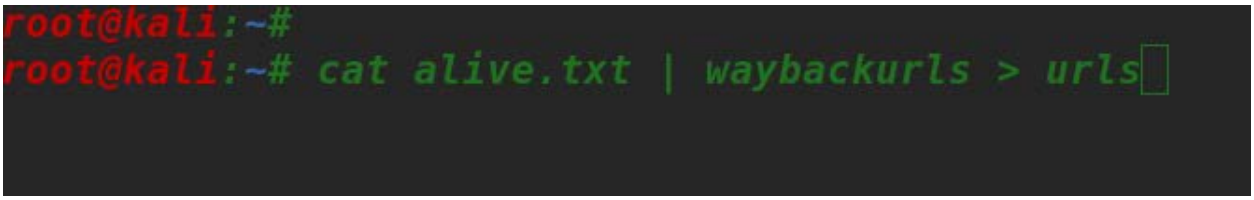
2. Wayback URLs

Waybackurls returns a list of all the URLs that the Wayback Machine knows about for a domain.

Github link: https://github.com/tomnomnom/waybackurls

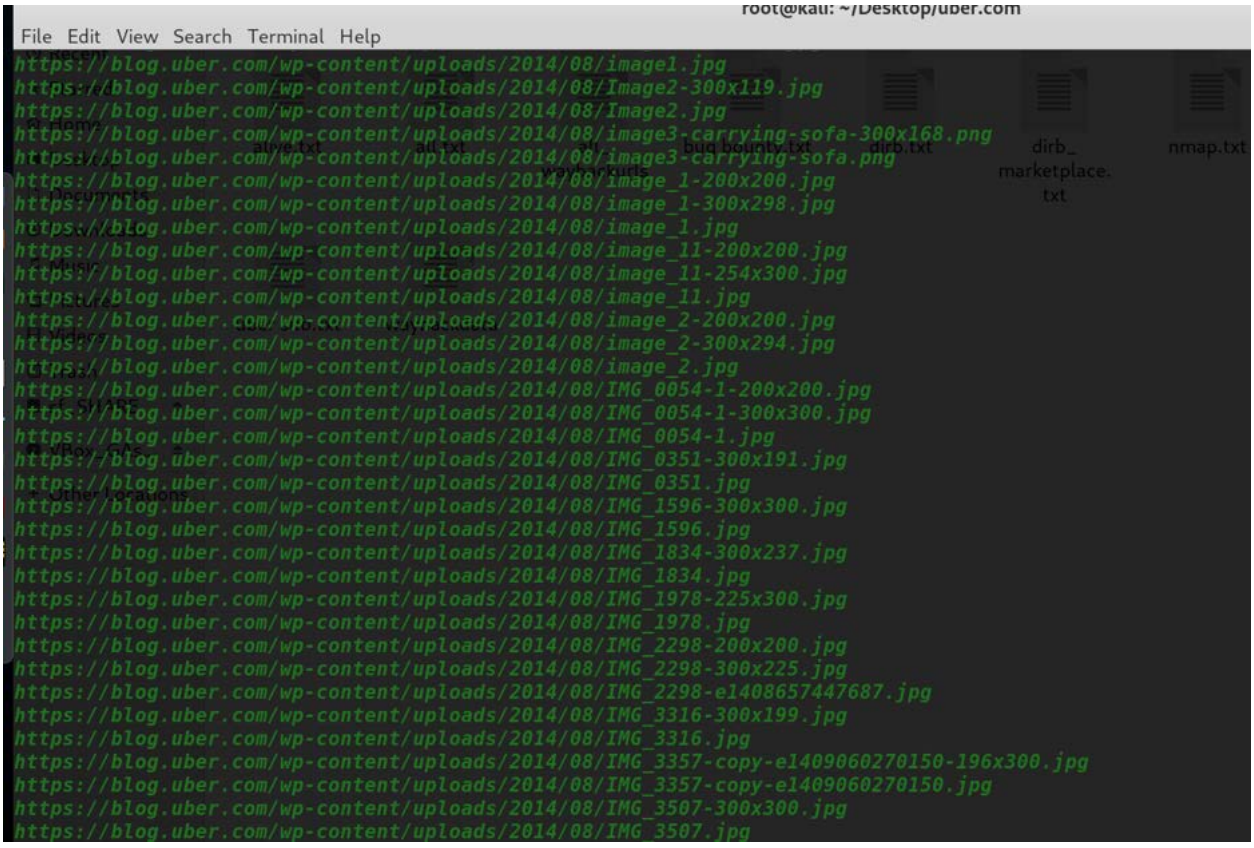
Installation:

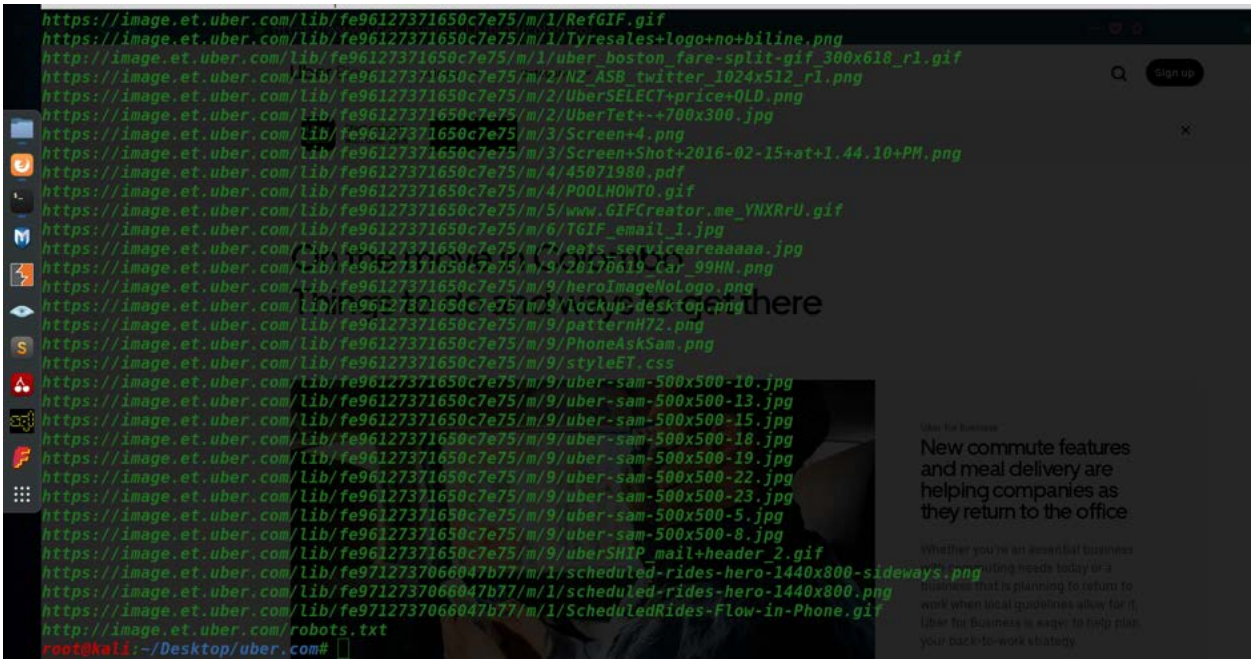
Usage:



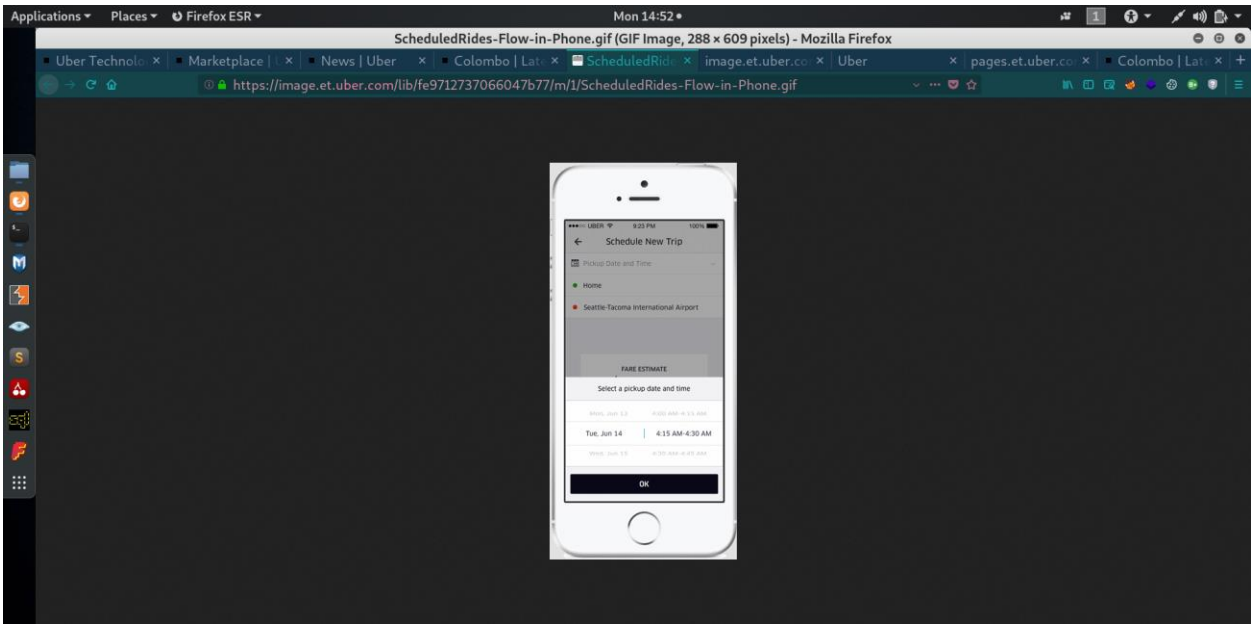
I get all the archived images and URLs of the Uber domain by sending the alive domains through the waybackurls and save as waybackdata.txt

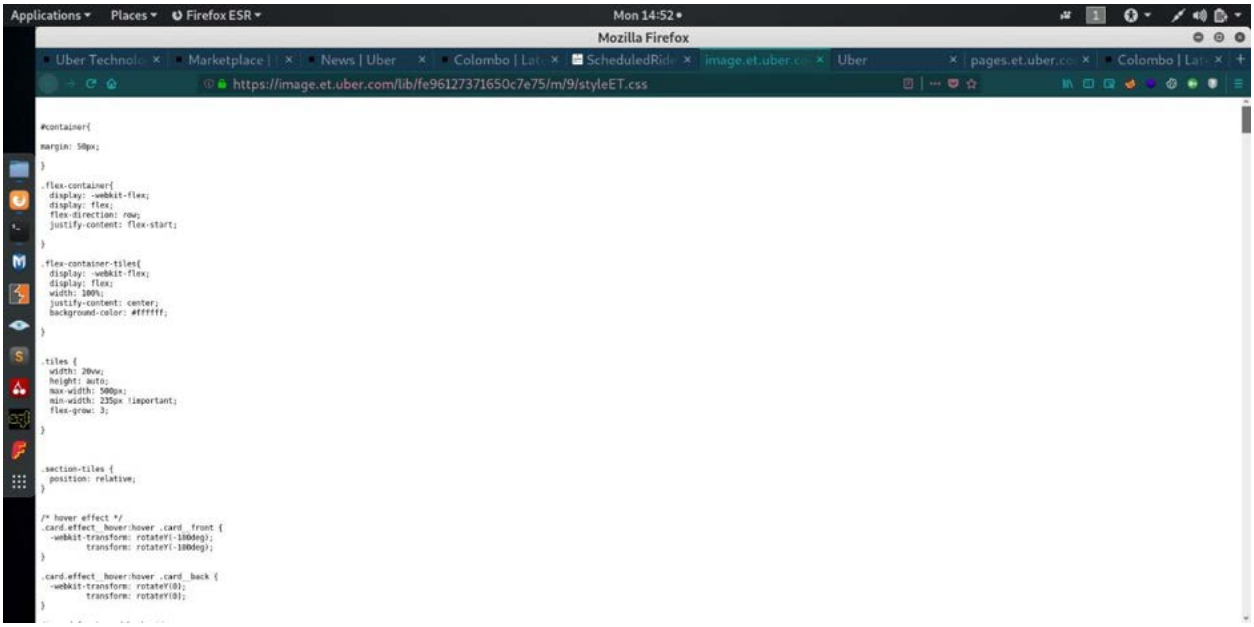

root@kali: ~/Desktop/uber.com
File Edit View Search Terminal Help
root@kali:~/Desktop/uber.com# cat waybackdata


root@kali: ~/Desktop/uber.com
File Edit View Search Terminal Help



Some interesting archived data which I got.





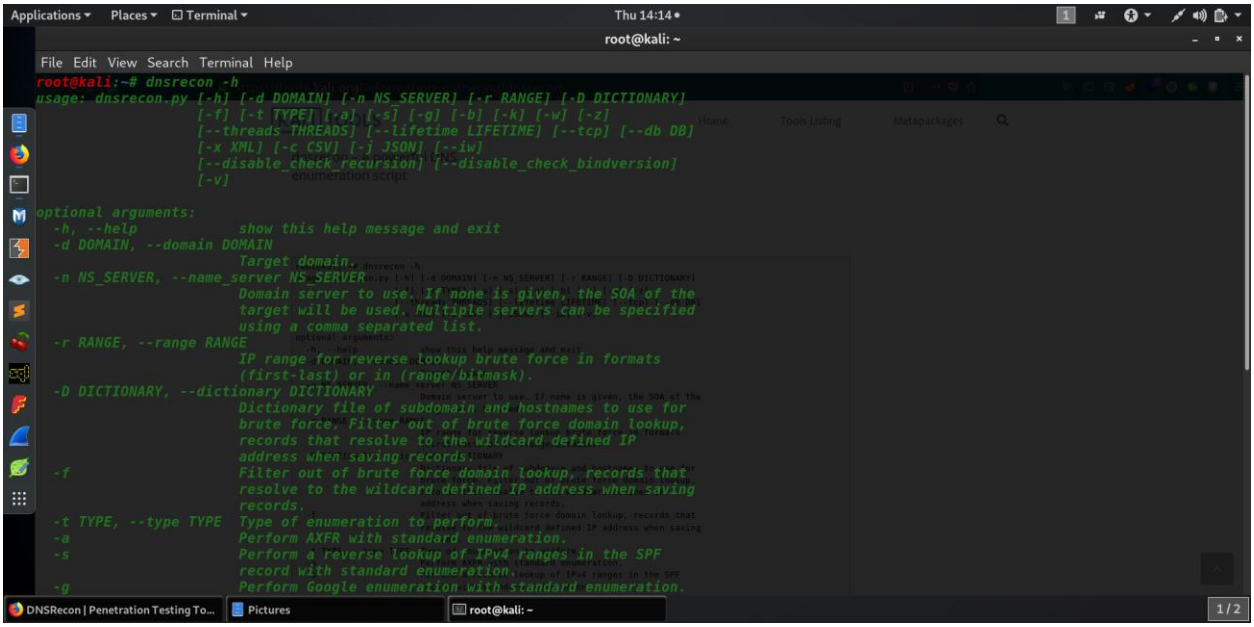
DNS enumeration

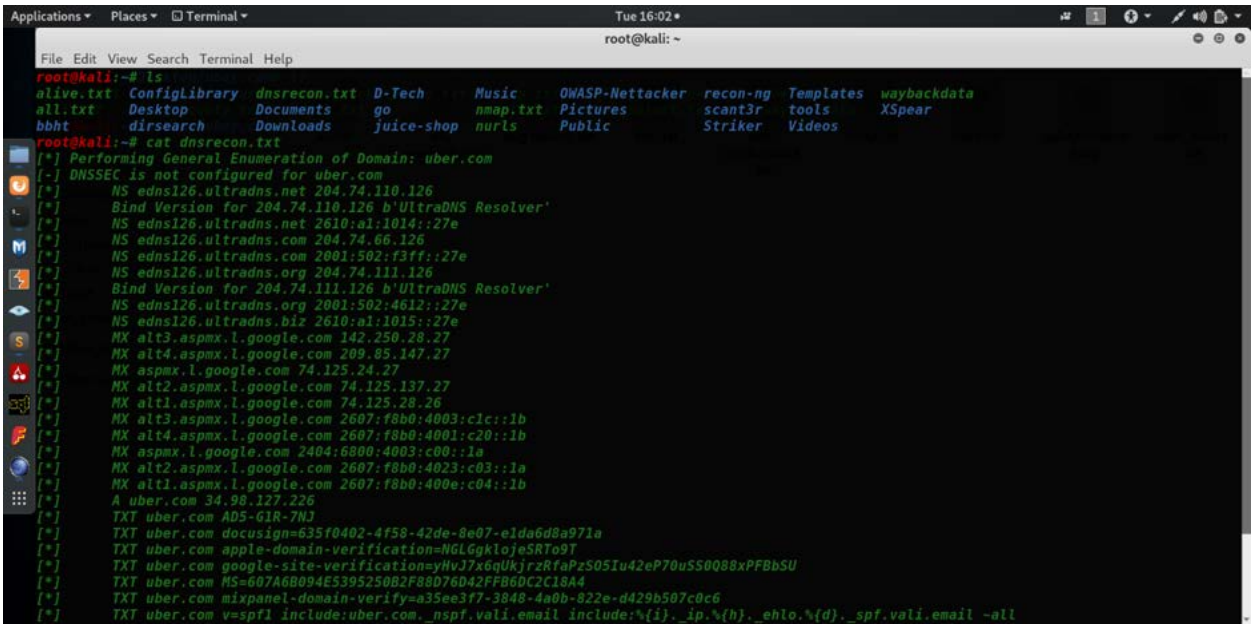
1. Dnsrecon

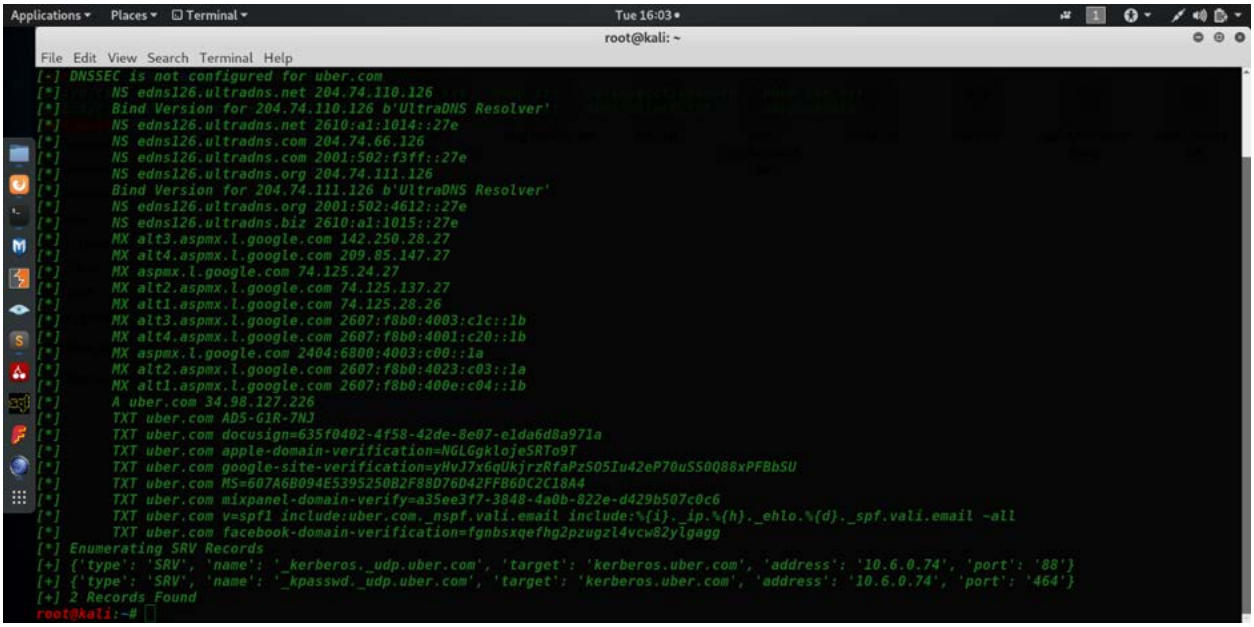
Dnsrecon is a powerful Domain Name System Enumeration tool in Kali Linux. We can use this tool for reverse lookup against an IP range, Domain brute force enumeration, cache snooping against name servers, standard records enumeration, etc.

Usage:

```
dnsrecon -d uber.com -D /usr/share/wordlists/dnsmap.txt -t std --xml dnsrecon.xml
```


Applications Places Terminal
Thu 14:14
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dnsrecon -h
usage: dnsrecon.py [-h] [-d DOMAIN] [-n NS_SERVER] [-r RANGE] [-D DICTIONARY]
[-f] [-t TYPE] [-a] [-s] [-g] [-b] [-k] [-w] [-z]
[--threads THREADS] [--lifetime LIFETIME] [--tcp] [--db DB]
[-x XML] [-c CSV] [-j JSON] [--iw]
[--disable_check_recursion] [--disable_check_bindversion]
[-v]
optional arguments:
-h, --help show this help message and exit
-d DOMAIN, --domain DOMAIN
Target domain.
-n NS_SERVER, --name_server NS_SERVER
Domain server to use. If none is given, the SOA of the
target will be used. Multiple servers can be specified
using a comma separated list.
-r RANGE, --range RANGE
IP range for reverse lookup brute force in formats
(first-last) or in (range/bitmask).
-D DICTIONARY, --dictionary DICTIONARY
Dictionary file of subdomain and hostnames to use for
brute force. Filter out of brute force domain lookup,
records that resolve to the wildcard defined IP
address when saving records
-f Filter out of brute force domain lookup, records that
resolve to the wildcard defined IP address when saving
records.
-t TYPE, --type TYPE Type of enumeration to perform.
-a Perform AXFR with standard enumeration.
-s Perform a reverse lookup of IPv4 ranges in the SPF
record with standard enumeration.
-g Perform Google enumeration with standard enumeration.
DNSRecon | Penetration Testing To...
Pictures
root@kali: ~
1 / 2


Applications Places Terminal
Tue 16:02
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ls
alive.txt ConfigLibrary dnsrecon.txt D-Tech Music OWASP-Nettacker recon-ng Templates waybackdata
all.txt Desktop Documents go nmap.txt Pictures scant3r tools XSpear
bbht dirsearch Downloads juice-shop nurls Public Striker Videos
root@kali:~# cat dnsrecon.txt
[*] Performing General Enumeration of Domain: uber.com
[-] DNSSEC is not configured for uber.com
[*] NS edns126.ultradns.net 204.74.110.126
[*] Bind Version for 204.74.110.126 b'UltraDNS Resolver'
[*] NS edns126.ultradns.net 2610:a1:1014::27e
[*] NS edns126.ultradns.com 204.74.66.126
[*] NS edns126.ultradns.com 2001:502:f3ff::27e
[*] NS edns126.ultradns.org 204.74.111.126
[*] Bind Version for 204.74.111.126 b'UltraDNS Resolver'
[*] NS edns126.ultradns.org 2001:502:4612::27e
[*] NS edns126.ultradns.biz 2610:a1:1015::27e
[*] MX alt3.aspmx.l.google.com 142.250.28.27
[*] MX alt4.aspmx.l.google.com 209.85.147.27
[*] MX aspmx.l.google.com 74.125.24.27
[*] MX alt2.aspmx.l.google.com 74.125.137.27
[*] MX alt1.aspmx.l.google.com 74.125.28.26
[*] MX alt3.aspmx.l.google.com 2607:f8b0:4003:c1c::1b
[*] MX alt4.aspmx.l.google.com 2607:f8b0:4001:c20::1b
[*] MX aspmx.l.google.com 2404:6800:4003:c00::1a
[*] MX alt2.aspmx.l.google.com 2607:f8b0:4023:c03::1a
[*] MX alt1.aspmx.l.google.com 2607:f8b0:400e:c04::1b
[*] A uber.com 34.98.127.226
[*] TXT uber.com AD5-GIR-7NJ
[*] TXT uber.com docusign=635f0402-4f58-42de-8e07-e1da6d8a971a
[*] TXT uber.com apple-domain-verification=NGLGgklojeSRTo9T
[*] TXT uber.com google-site-verification=yHvJ7x6qUkjrzRfaPzSO5Iu42eP70uSS0Q88xPFBbSU
[*] TXT uber.com MS=607A6B094E5395250B2F88D76D42FFB6DC2C18A4
[*] TXT uber.com mixpanel-domain-verify=a35ee3f7-3848-4a0b-822e-d429b507c0c6
[*] TXT uber.com v=spf1 include:uber.com._nspf.vali.email include:%{i}._ip.%{h}._ehlo.%{d}._spf.vali.email ~all

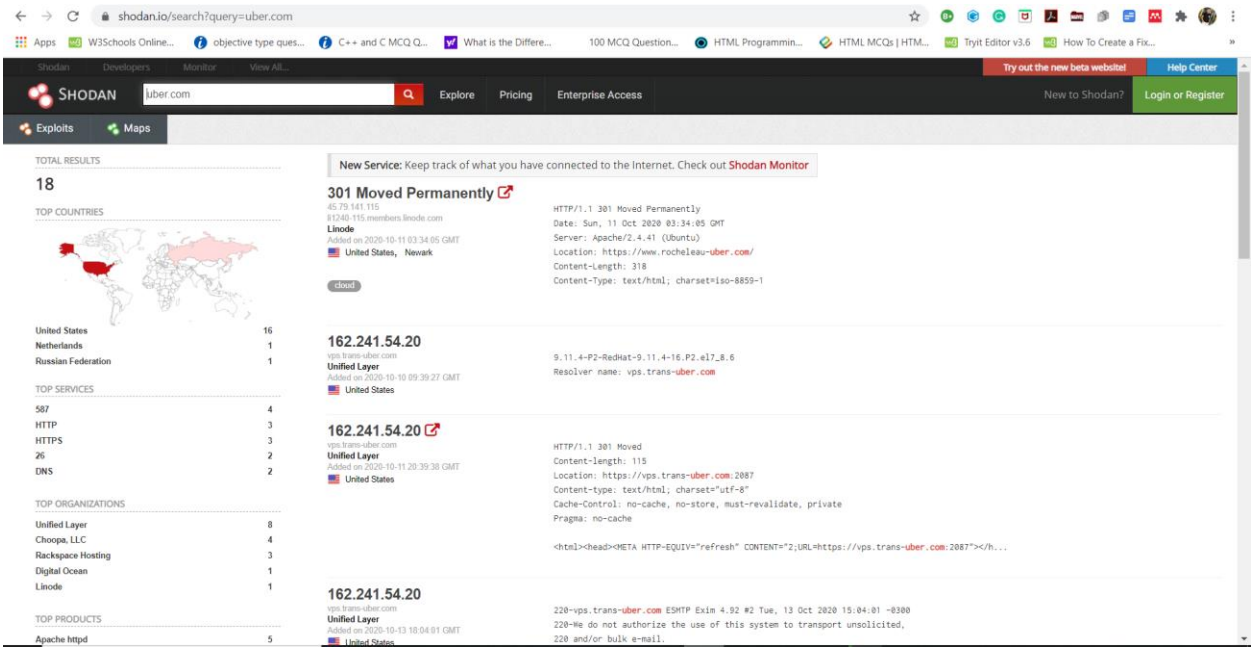


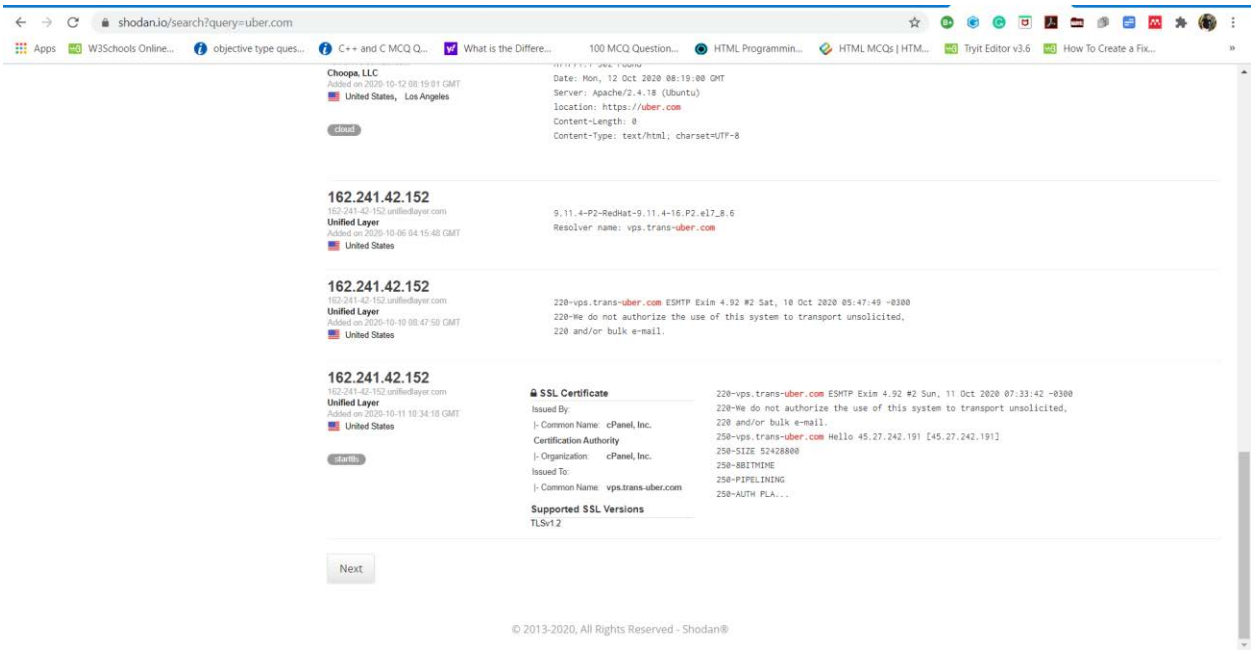
Public Device Enumeration

1. Shodan

Web site link: https://www.shodan.io/

This gives details about all the internet-connected devices for the targeted domain. If there any public IP address exposing a service on a certain port then it is available in the Shodan. Not only the IP but also we can get web server details, banners, ISP, SSH, FTP, etc.

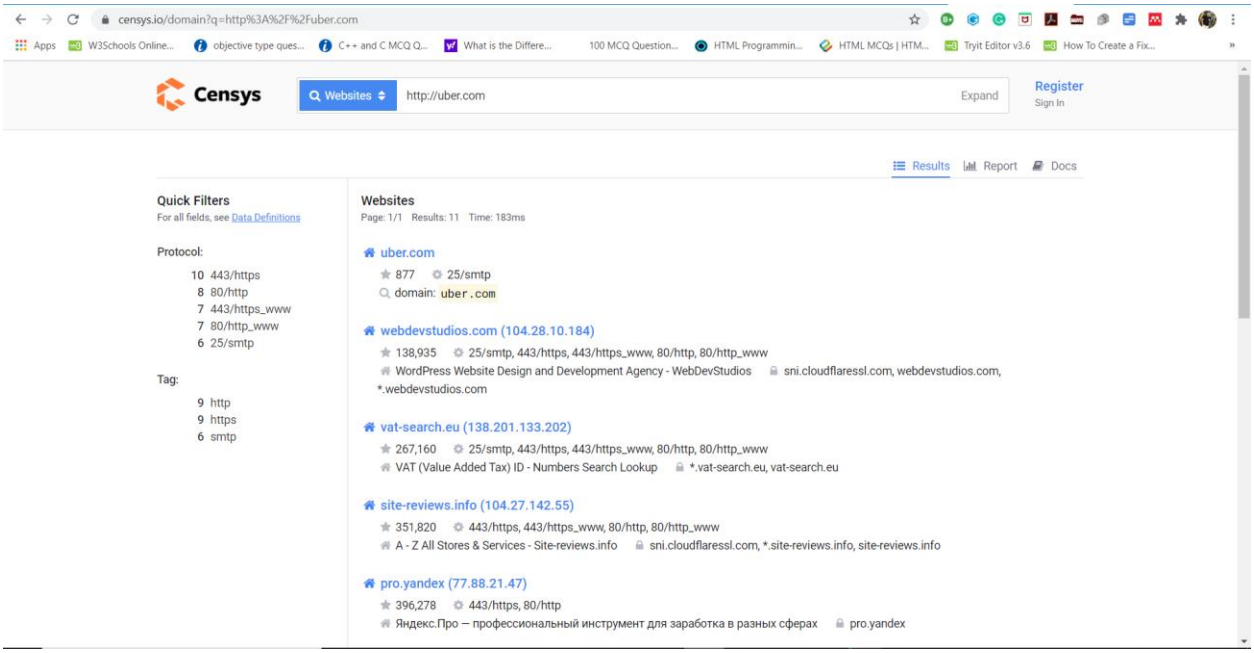

shodan.io/search?query=uber.com
SHODAN
uber.com
Explore
Pricing
Enterprise Access
New to Shodan?
Login or Register
Exploits
Maps
TOTAL RESULTS
18
TOP COUNTRIES
United States 16
Netherlands 1
Russian Federation 1
TOP SERVICES
587 4
HTTP 3
HTTPS 3
26 2
DNS 2
TOP ORGANIZATIONS
Unified Layer 8
Choopa, LLC 4
Rackspace Hosting 3
Digital Ocean 1
Linode 1
TOP PRODUCTS
Apache httpd 5
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
301 Moved Permanently
45.79.141.115
Linode
United States, Newark
HTTP/1.1 301 Moved Permanently
Date: Sun, 11 Oct 2020 03:34:05 GMT
Server: Apache/2.4.41 (Ubuntu)
Location: https://www.rocheleau-uber.com/
Content-Length: 318
Content-Type: text/html; charset=iso-8859-1
162.241.54.20
Unified Layer
United States
9.11.4-P2-RedHat-9.11.4-16.P2.el7_8.6
Resolver name: vps.trans-uber.com
162.241.54.20
Unified Layer
United States
HTTP/1.1 301 Moved
Content-length: 115
Location: https://vps.trans-uber.com:2087
Content-type: text/html; charset="utf-8"
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
<html><head><META HTTP-EQUIV="refresh" CONTENT="2;URL=https://vps.trans-uber.com:2087"></h...
162.241.54.20
Unified Layer
220-vps.trans-uber.com ESMTP Exim 4.92 #2 Tue, 13 Oct 2020 15:04:01 -0300
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.

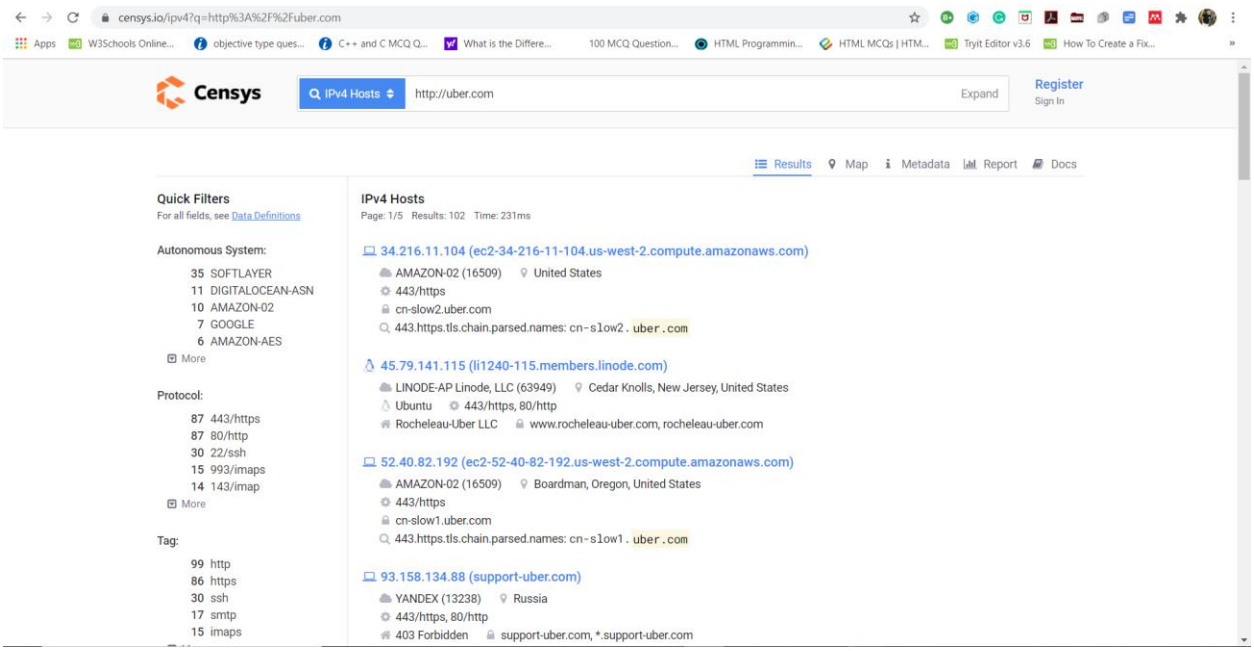

shodan.io/search?query=uber.com
Choopa, LLC
United States, Los Angeles
Date: Mon, 12 Oct 2020 08:19:00 GMT
Server: Apache/2.4.18 (Ubuntu)
location: https://uber.com
Content-Length: 0
Content-Type: text/html; charset=UTF-8
162.241.42.152
Unified Layer
United States
9.11.4-P2-RedHat-9.11.4-16.P2.el7_8.6
Resolver name: vps.trans-uber.com
162.241.42.152
Unified Layer
United States
220-vps.trans-uber.com ESMTP Exim 4.92 #2 Sat, 10 Oct 2020 05:47:49 -0300
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
162.241.42.152
Unified Layer
United States
SSL Certificate
Issued By:
|- Common Name: cPanel, Inc.
Certification Authority
|- Organization: cPanel, Inc.
Issued To:
|- Common Name: vps.trans-uber.com
Supported SSL Versions
TLSv1.2
220-vps.trans-uber.com ESMTP Exim 4.92 #2 Sun, 11 Oct 2020 07:33:42 -0300
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
250-vps.trans-uber.com Hello 45.27.242.191 [45.27.242.191]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-AUTH PLA...
Next
© 2013-2020, All Rights Reserved - Shodan®

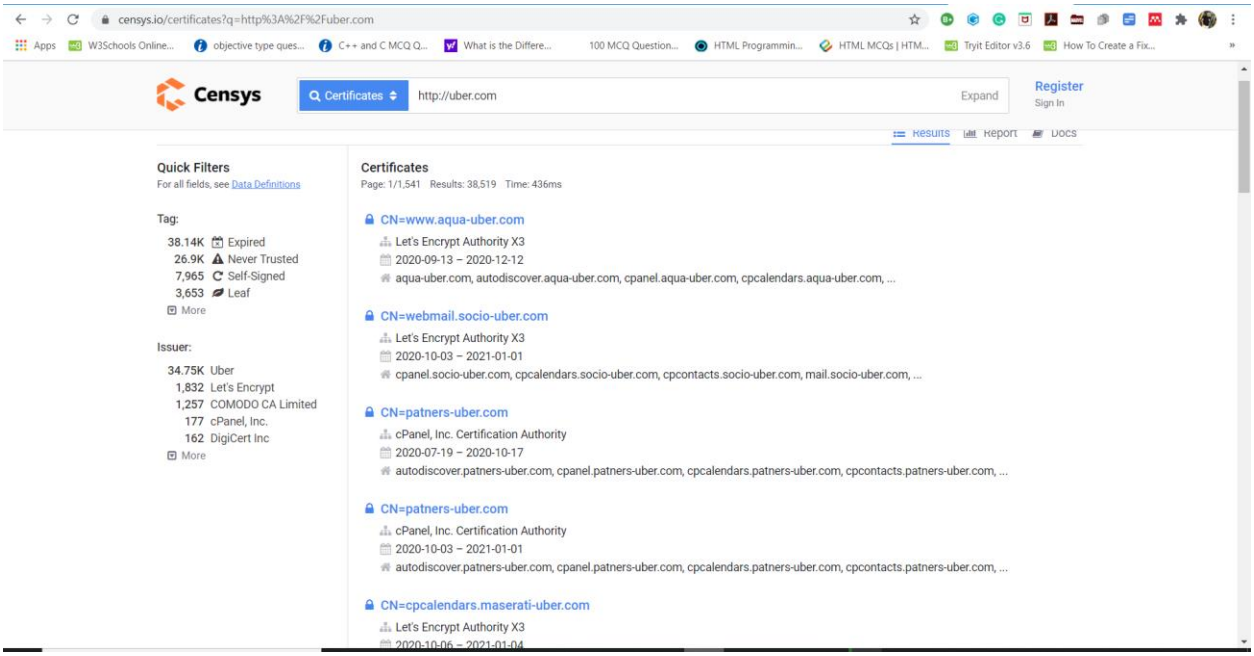
2. Censys

Web site link: https://censys.io/

This is a very similar tool for Shodan which we can use for public device enumeration. Censys can use to scan devices, hosts, and gives the proper report about how the system is configured. (websites, certifications, etc.)




censys.io/ipv4?q=http%3A%2F%2Fuber.com
Censys
IPv4 Hosts
http://uber.com
Expand
Register
Sign In
Results
Map
Metadata
Report
Docs
Quick Filters
For all fields, see Data Definitions
Autonomous System:
35 SOFTLAYER
11 DIGITALOCEAN-ASN
10 AMAZON-02
7 GOOGLE
6 AMAZON-AES
More
Protocol:
87 443/https
87 80/http
30 22/ssh
15 993/imaps
14 143/imap
More
Tag:
99 http
86 https
30 ssh
17 smtp
15 imaps
IPv4 Hosts
Page: 1/5 Results: 102 Time: 231ms
34.216.11.104 (ec2-34-216-11-104.us-west-2.compute.amazonaws.com)
AMAZON-02 (16509) United States
443/https
cn-slow2.uber.com
443.https.tls.chain.parsed.names: cn-slow2.uber.com
45.79.141.115 (li1240-115.members.linode.com)
LINODE-AP Linode, LLC (63949) Cedar Knolls, New Jersey, United States
Ubuntu 443/https, 80/http
Rocheleau-Uber LLC www.rocheleau-uber.com, rocheleau-uber.com
52.40.82.192 (ec2-52-40-82-192.us-west-2.compute.amazonaws.com)
AMAZON-02 (16509) Boardman, Oregon, United States
443/https
cn-slow1.uber.com
443.https.tls.chain.parsed.names: cn-slow1.uber.com
93.158.134.88 (support-uber.com)
YANDEX (13238) Russia
443/https, 80/http
403 Forbidden support-uber.com, *.support-uber.com


censys.io/certificates?q=http%3A%2F%2Fuber.com
Censys
Certificates
http://uber.com
Expand
Register
Sign In
Results
Report
Docs
Quick Filters
For all fields, see Data Definitions
Tag:
38.14K Expired
26.9K Never Trusted
7,965 Self-Signed
3,653 Leaf
More
Issuer:
34.75K Uber
1,832 Let's Encrypt
1,257 COMODO CA Limited
177 cPanel, Inc.
162 DigiCert Inc
More
Certificates
Page: 1/1,541 Results: 38,519 Time: 436ms
CN=www.aqua-uber.com
Let's Encrypt Authority X3
2020-09-13 – 2020-12-12
aqua-uber.com, autodiscover.aqua-uber.com, cpanel.aqua-uber.com, cpcalendars.aqua-uber.com, ...
CN=webmail.socio-uber.com
Let's Encrypt Authority X3
2020-10-03 – 2021-01-01
cpanel.socio-uber.com, cpcalendars.socio-uber.com, cpcontacts.socio-uber.com, mail.socio-uber.com, ...
CN=patners-uber.com
cPanel, Inc. Certification Authority
2020-07-19 – 2020-10-17
autodiscover.patners-uber.com, cpanel.patners-uber.com, cpcalendars.patners-uber.com, cpcontacts.patners-uber.com, ...
CN=patners-uber.com
cPanel, Inc. Certification Authority
2020-10-03 – 2021-01-01
autodiscover.patners-uber.com, cpanel.patners-uber.com, cpcalendars.patners-uber.com, cpcontacts.patners-uber.com, ...
CN=cpcalendars.maserati-uber.com
Let's Encrypt Authority X3

Find Structure of File System

1. Dirsearch

This is a very famous free and open-source tool for brute force directories and files on websites. We can use a custom wordlist to brute force files and directories.

Installation: https://github.com/maurosoria/dirsearch

Usage:

```
python dirsearch.py -u https://uber.com -e html,php,jsp,asp,json
```

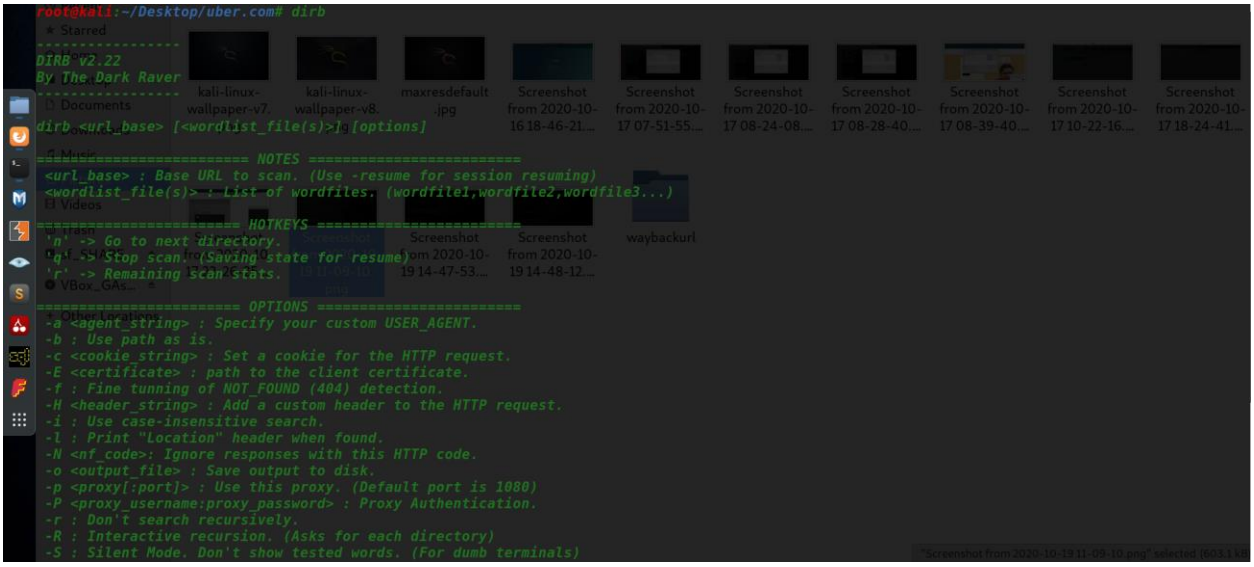
2. Dirb Tool

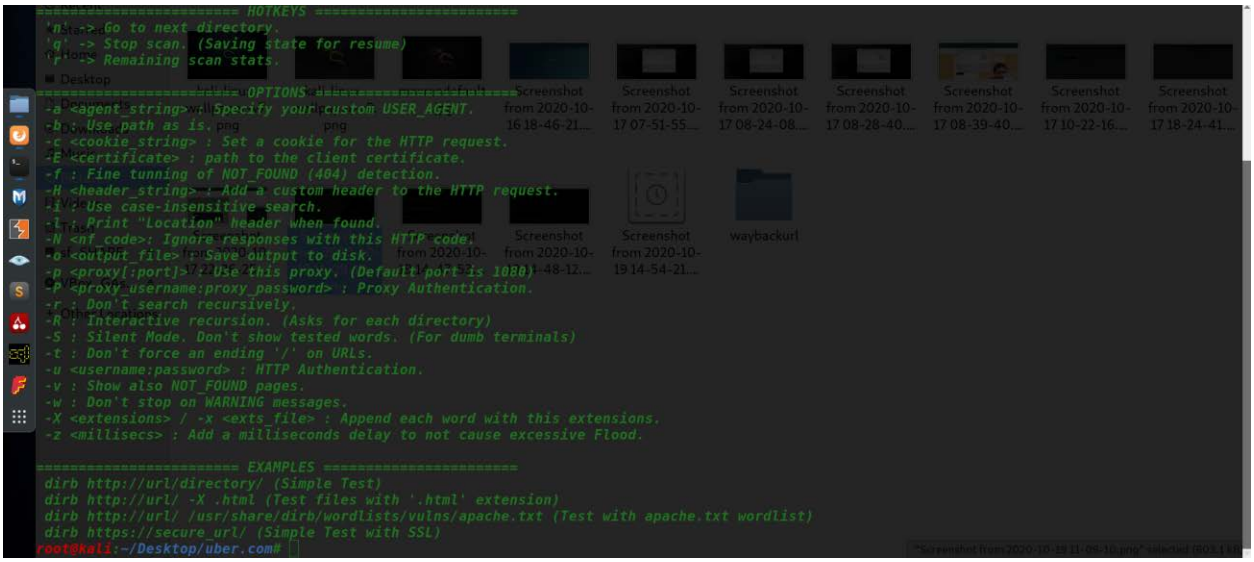
Dirb is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically, works by launching a dictionary-based attack against a web server and analyzing the response. By using DIRB we can scan all the content available in the target domain.

Download: https://sourceforge.net/projects/dirb/

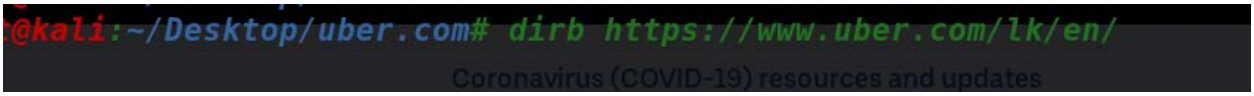
Usage:

```
dirb https://www.uber.com/lk/en /usr/share/wordlists/dirb/common.txt
```





I tried to brute force the following URLs and by giving below two commands.



```
root@kali:~# dirb https://www.uber.com/lk/en/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Oct 19 10:20:18 2020
URL_BASE: https://www.uber.com/lk/en/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://www.uber.com/lk/en/ ----
+ https://www.uber.com/lk/en/robots.txt (CODE:200|SIZE:58514)
+ https://www.uber.com/lk/en/sitemap.xml (CODE:200|SIZE:34064)

-----------------
END_TIME: Mon Oct 19 10:54:53 2020
DOWNLOADED: 4612 - FOUND: 2
root@kali:~#
```

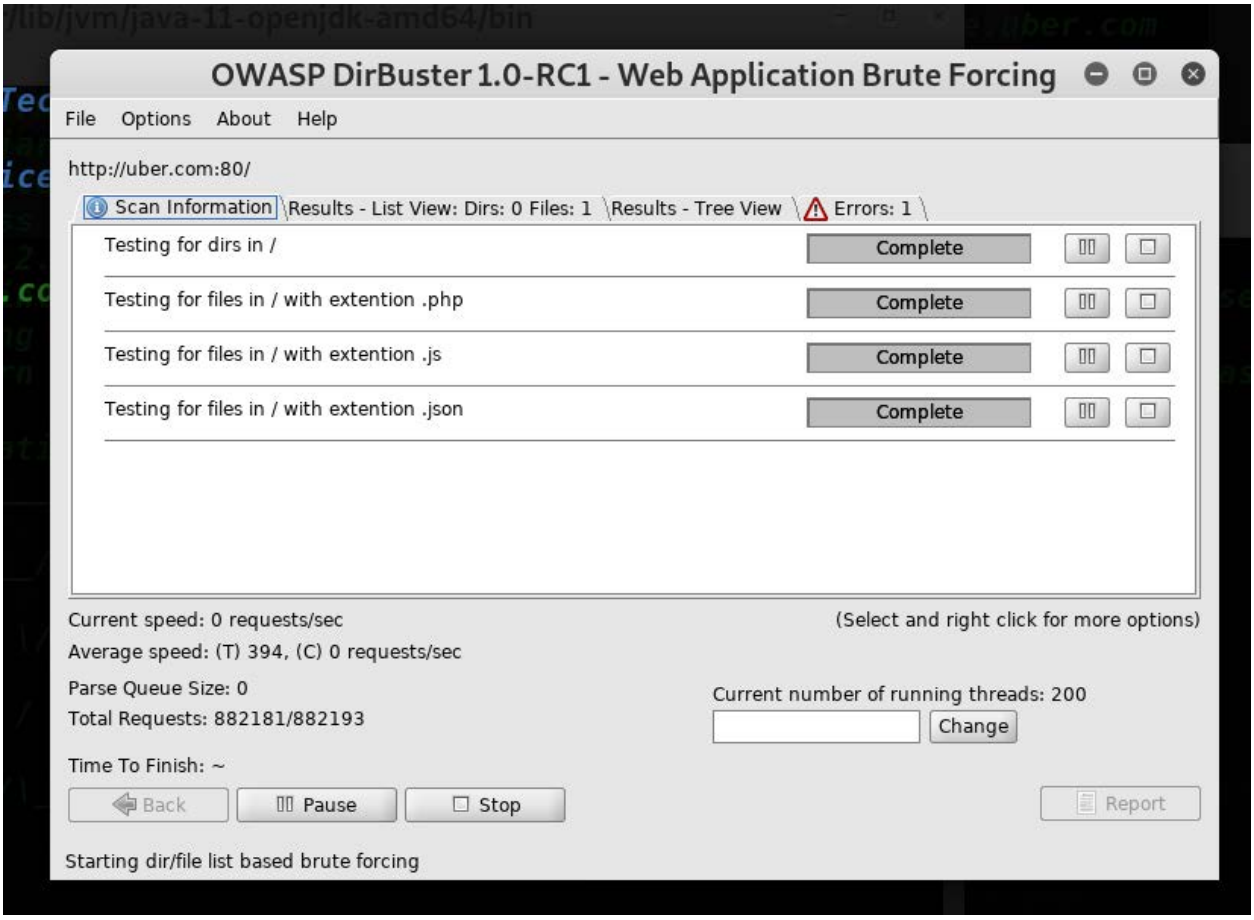
```
root@kali:~/Desktop/uber.com# cat dirb.txt
dirb https://www.uber.com/lk/en/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Oct 19 10:20:18 2020
URL_BASE: https://www.uber.com/lk/en/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://www.uber.com/lk/en/ ----
+ https://www.uber.com/lk/en/robots.txt (CODE:200|SIZE:58514)
+ https://www.uber.com/lk/en/sitemap.xml (CODE:200|SIZE:34064)

-----------------
END_TIME: Mon Oct 19 10:54:53 2020
DOWNLOADED: 4612 - FOUND: 2
root@kali:~/Desktop/uber.com#
```

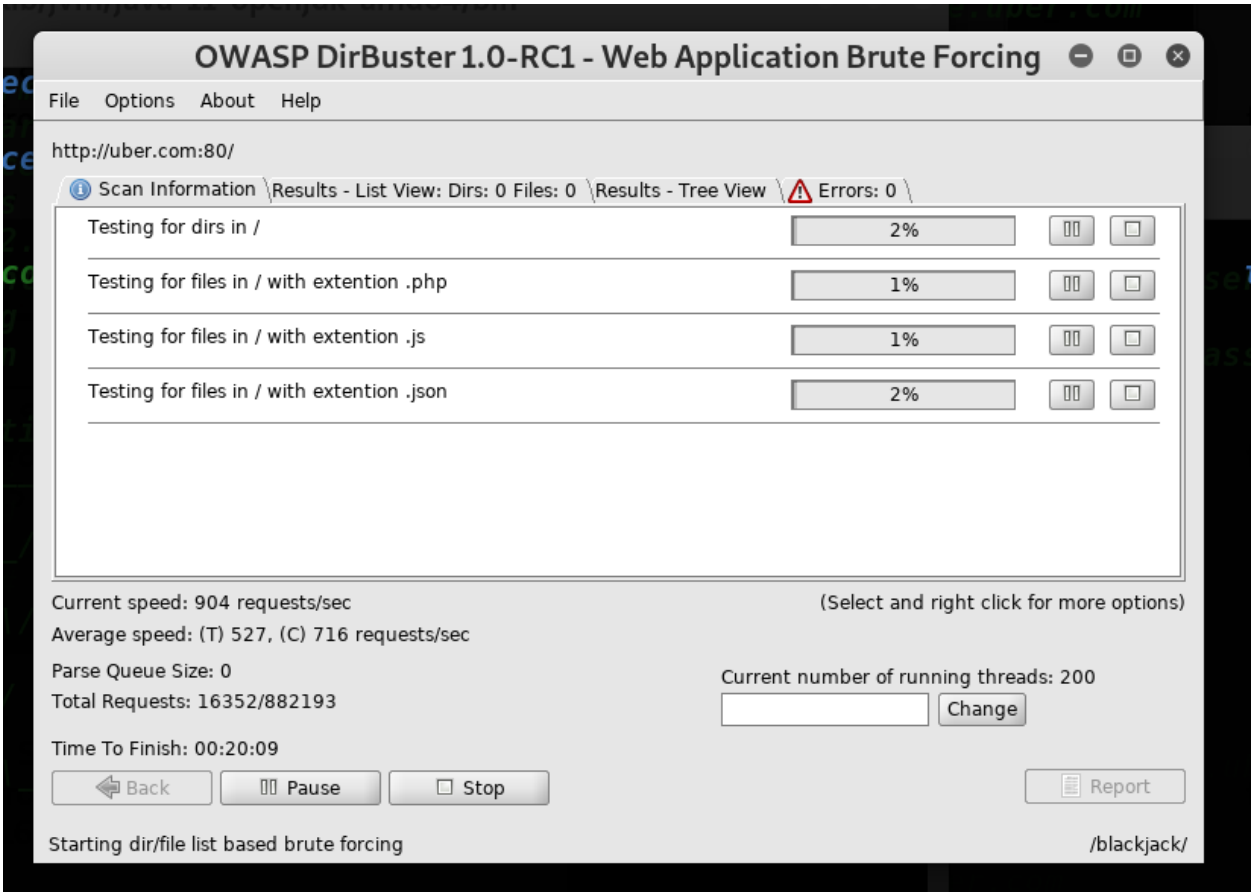
```
root@kali:~/Desktop/uber.com# cat dirb_marketplace.txt
dirb https://marketplace.uber.com/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Oct 19 11:12:51 2020
URL_BASE: https://marketplace.uber.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://marketplace.uber.com/ ----
+ https://marketplace.uber.com/favicon.ico (CODE:200|SIZE:1150)
+ https://marketplace.uber.com/index (CODE:200|SIZE:70684)
+ https://marketplace.uber.com/news (CODE:200|SIZE:43403)
+ https://marketplace.uber.com/pricing (CODE:200|SIZE:70578)

-----------------
END_TIME: Mon Oct 19 11:44:34 2020
DOWNLOADED: 4612 - FOUND: 4
root@kali:~/Desktop/uber.com#
```

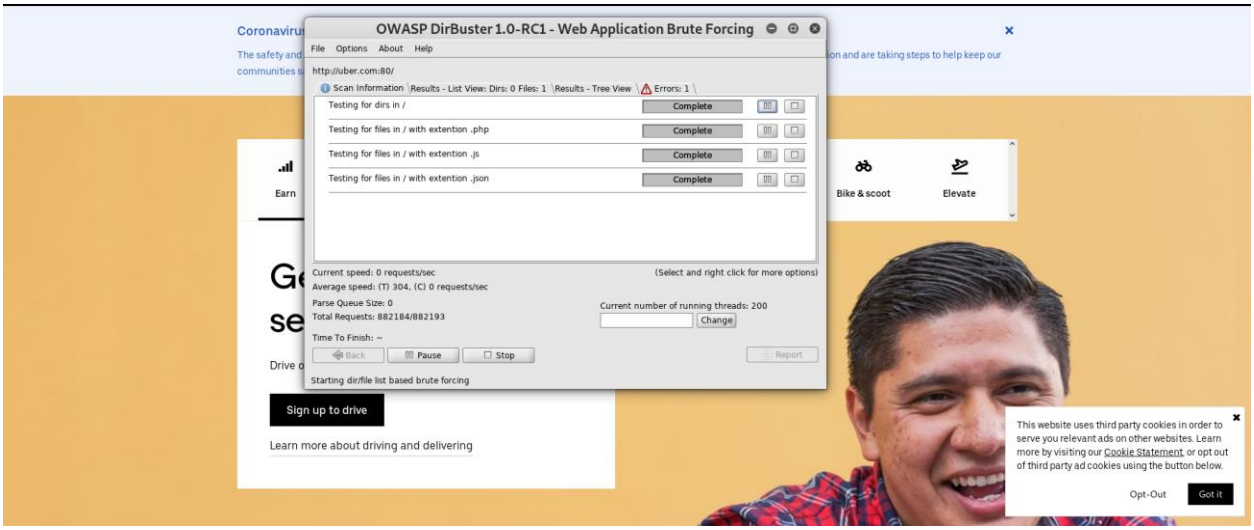
3. OWASP Dirbuster

DirBuster is a multi-threaded java application designed to brute force directories and files names on web/application servers. Often is the case now of what looks like a web server in a state of default installation is not, and has pages and applications hidden within. DirBuster attempts to find these. However, tools of this nature are often as only good as the directory and file list they come with. A different approach was taken to generating this. The list was generated from scratch, by crawling the Internet and collecting the directory and files that are used by developers. DirBuster comes a total of 9 different lists, this makes DirBuster extremely effective at finding those hidden files and directories. And if that was not enough DirBuster also has the option to perform a pure brute force, which leaves the hidden directories and files nowhere to hide.

To brute force the directories I used DirBuster but it makes a lot of time to brute forcing it.




OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://uber.com:80/
Scan Information
Results - List View: Dirs: 0 Files: 0
Results - Tree View
Errors: 0
Testing for dirs in /
2%
Testing for files in / with extention .php
1%
Testing for files in / with extention .js
1%
Testing for files in / with extention .json
2%
Current speed: 904 requests/sec
(Select and right click for more options)
Average speed: (T) 527, (C) 716 requests/sec
Parse Queue Size: 0
Total Requests: 16352/882193
Current number of running threads: 200
Change
Time To Finish: 00:20:09
Back
Pause
Stop
Report
Starting dir/file list based brute forcing
/blackjack/

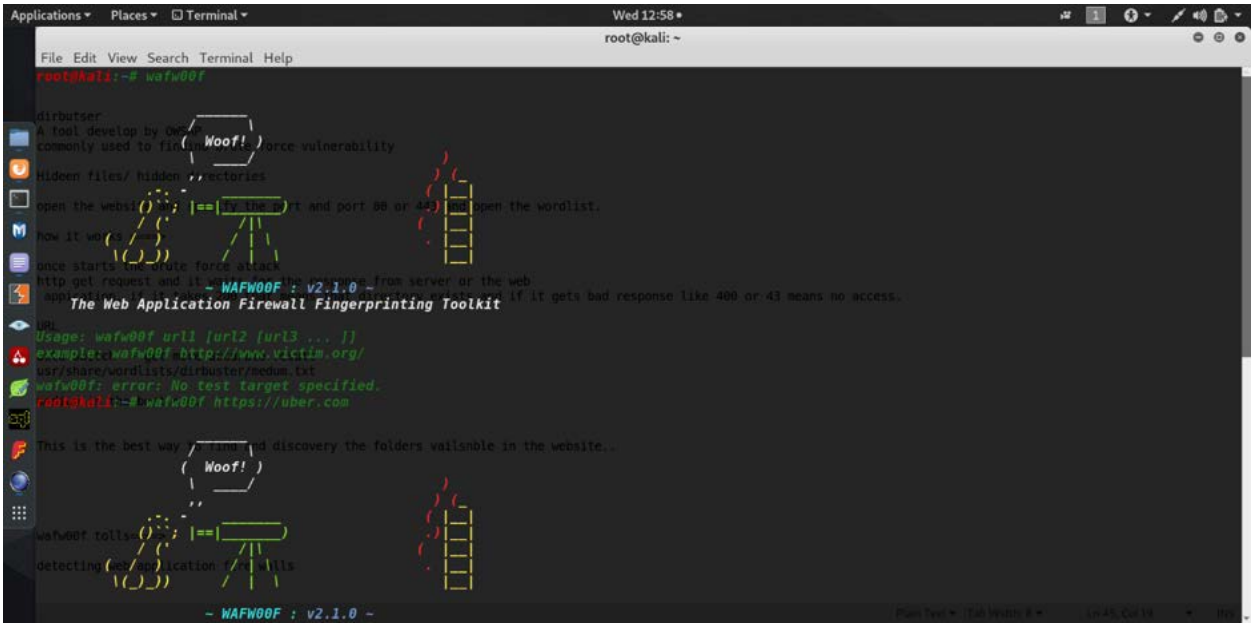

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
Sign up to drive
Learn more about driving and delivering
This website uses third party cookies in order to serve you relevant ads on other websites. Learn more by visiting our Cookie Statement, or opt out of third party ad cookies using the button below.
Opt-Out
Got it

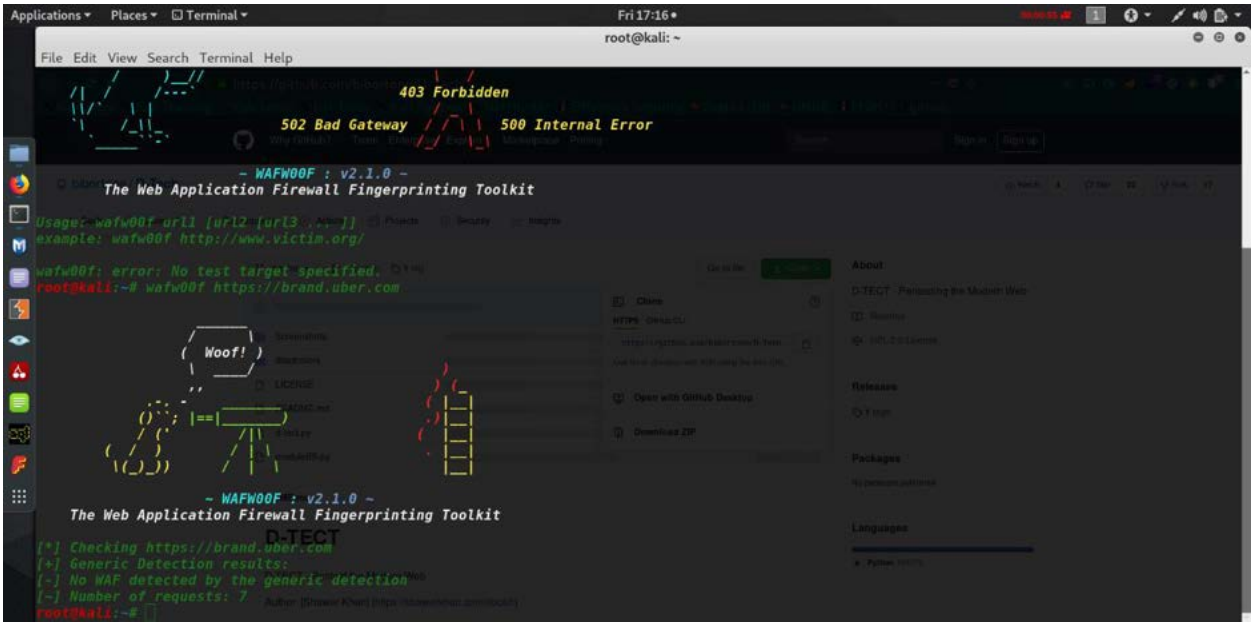
Find the target domain has firewall protection

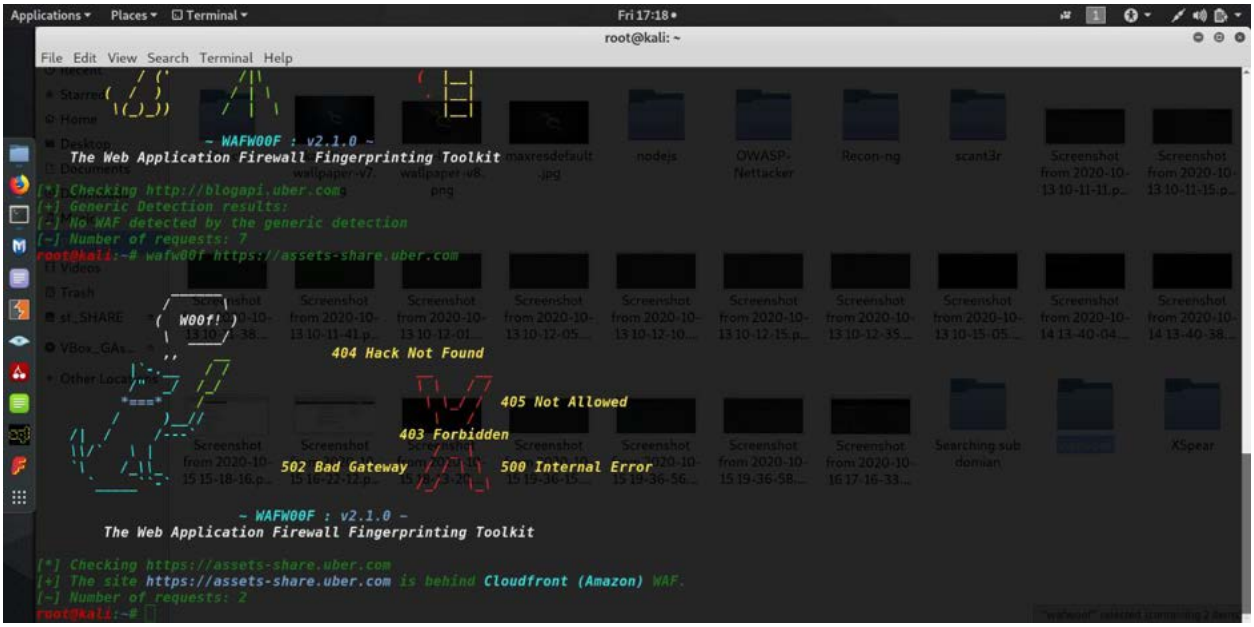
1. Wafw00f

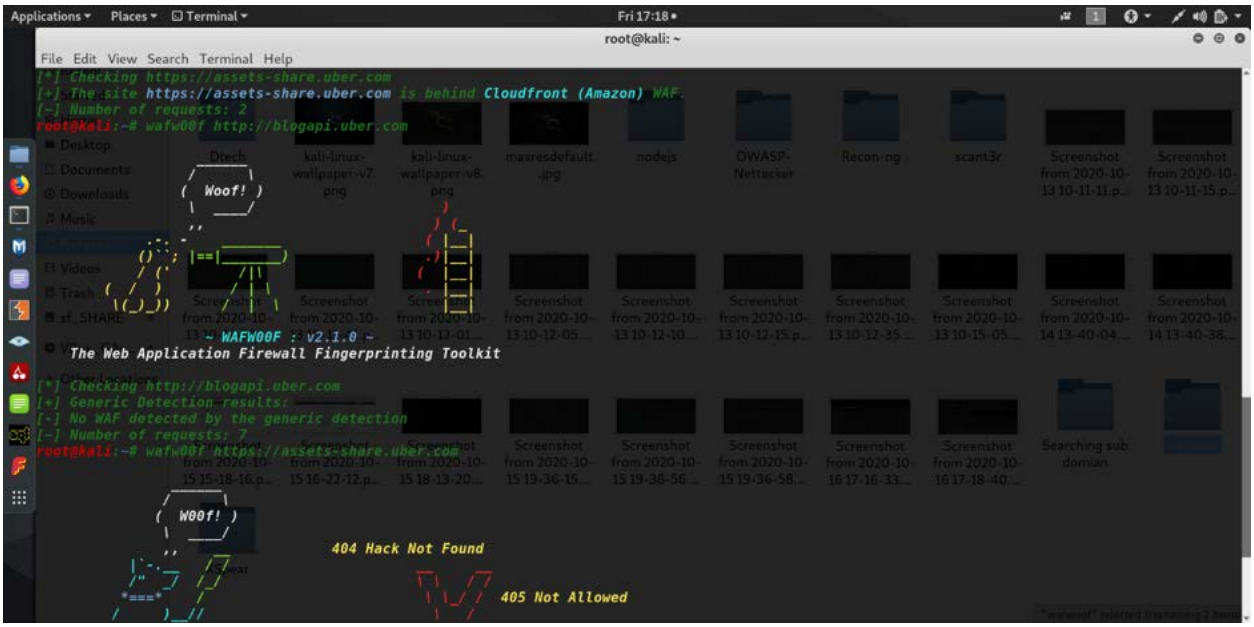
Wafw00f is a Web Application firewall detection tool available in Kali Linux. It can detect around the Top 22 web application firewall, so wafw00f is a phase of information gathering initially.

I use this tool to detect my target URL whether protected behind a firewall.






Applications Places Terminal Fri 17:18
root@kali: ~
File Edit View Search Terminal Help
~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking http://blogapi.uber.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
root@kali:~# wafw00f https://assets-share.uber.com
404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error
~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://assets-share.uber.com
[+] The site https://assets-share.uber.com is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2


Applications Places Terminal Fri 17:18
root@kali: ~
File Edit View Search Terminal Help
[*] Checking https://assets-share.uber.com
[+] The site https://assets-share.uber.com is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2
root@kali:~# wafw00f http://blogapi.uber.com
~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking http://blogapi.uber.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
root@kali:~# wafw00f https://assets-share.uber.com
404 Hack Not Found
405 Not Allowed

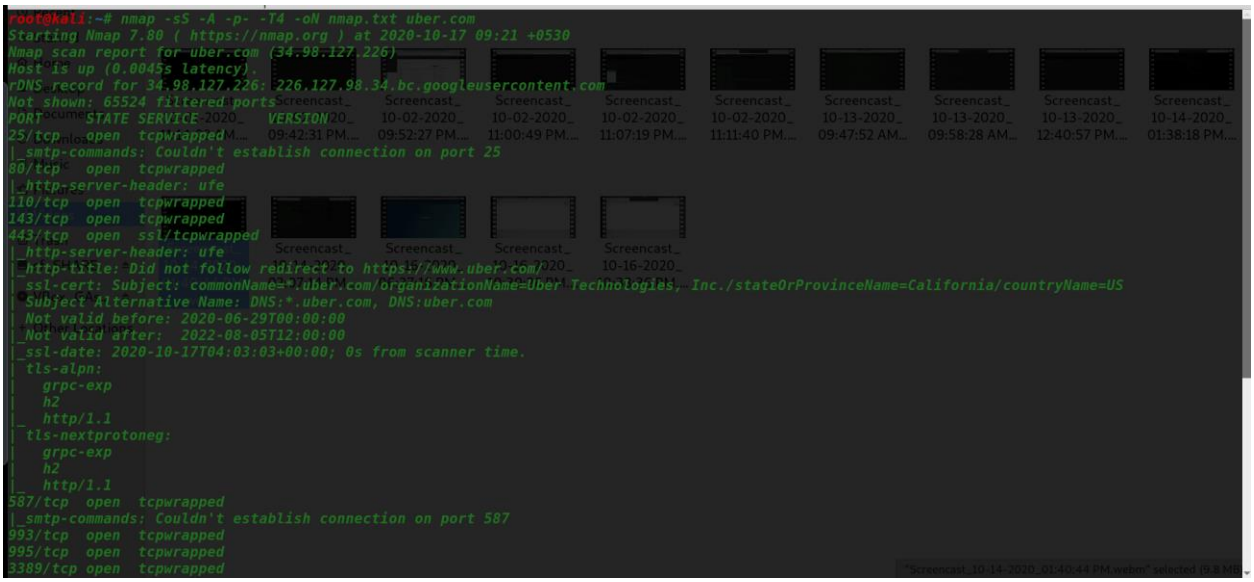
Find Open ports and running devices on the target network

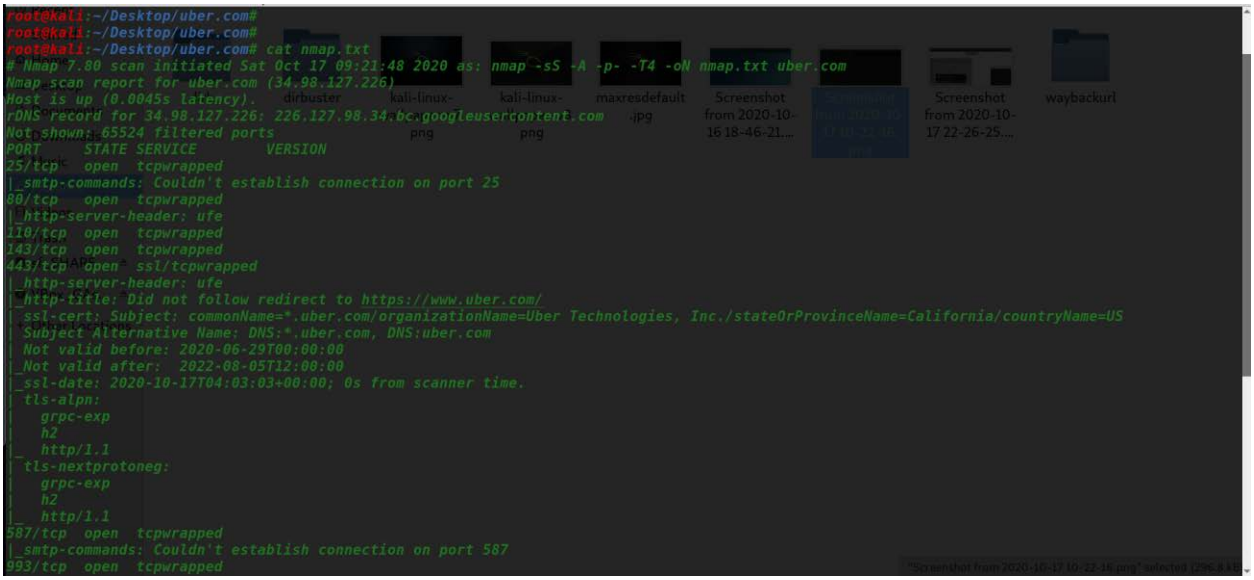
1. Nmap

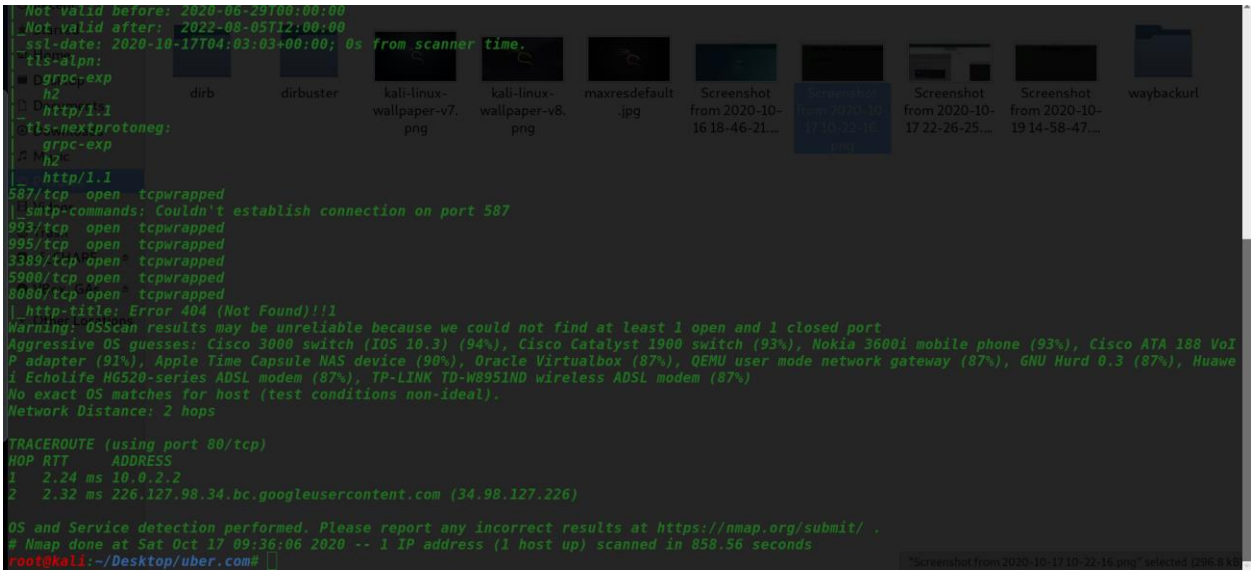
Usage:

```
nmap -sS -A -p- -T4 -oN nmap.txt uber.com
```

Proof of concept:




root@kali:~/Desktop/uber.com#
root@kali:~/Desktop/uber.com#
root@kali:~/Desktop/uber.com# cat nmap.txt
Nmap 7.80 scan initiated Sat Oct 17 09:21:48 2020 as: nmap -sS -A -p- -T4 -oN nmap.txt uber.com
Nmap scan report for uber.com (34.98.127.226)
Host is up (0.0045s latency).
rDNS record for 34.98.127.226: 226.127.98.34.bc.googleusercontent.com
Not shown: 65524 filtered ports
PORT STATE SERVICE VERSION
25/tcp open tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp open tcpwrapped
|_http-server-header: ufe
110/tcp open tcpwrapped
143/tcp open tcpwrapped
443/tcp open ssl/tcpwrapped
|_http-server-header: ufe
|_http-title: Did not follow redirect to https://www.uber.com/
| ssl-cert: Subject: commonName=*.uber.com/organizationName=Uber Technologies, Inc./stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:*.uber.com, DNS:uber.com
| Not valid before: 2020-06-29T00:00:00
|_Not valid after: 2022-08-05T12:00:00
|_ssl-date: 2020-10-17T04:03:03+00:00; 0s from scanner time.
| tls-alpn:
| grpc-exp
| h2
|_ http/1.1
| tls-nextprotoneg:
| grpc-exp
| h2
|_ http/1.1
587/tcp open tcpwrapped
|_smtp-commands: Couldn't establish connection on port 587
993/tcp open tcpwrapped
dirb
dirbuster
kali-linux-wallpaper-v7.png
kali-linux-wallpaper-v8.png
maxresdefault.jpg
Screenshot from 2020-10-16 18-46-21....
Screenshot from 2020-10-17 22-26-25....
waybackurl


| Not valid before: 2020-06-29T00:00:00
|_Not valid after: 2022-08-05T12:00:00
|_ssl-date: 2020-10-17T04:03:03+00:00; 0s from scanner time.
| tls-alpn:
| grpc-exp
| h2
|_ http/1.1
| tls-nextprotoneg:
| grpc-exp
| h2
|_ http/1.1
587/tcp open tcpwrapped
|_smtp-commands: Couldn't establish connection on port 587
993/tcp open tcpwrapped
995/tcp open tcpwrapped
3389/tcp open tcpwrapped
5900/tcp open tcpwrapped
8080/tcp open tcpwrapped
|_http-title: Error 404 (Not Found)!!1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Cisco 3000 switch (IOS 10.3) (94%), Cisco Catalyst 1900 switch (93%), Nokia 3600i mobile phone (93%), Cisco ATA 188 VoIP adapter (91%), Apple Time Capsule NAS device (90%), Oracle Virtualbox (87%), QEMU user mode network gateway (87%), GNU Hurd 0.3 (87%), Huawei Echolife HG520-series ADSL modem (87%), TP-LINK TD-W8951ND wireless ADSL modem (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 2.24 ms 10.0.2.2
2 2.32 ms 226.127.98.34.bc.googleusercontent.com (34.98.127.226)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Sat Oct 17 09:36:06 2020 -- 1 IP address (1 host up) scanned in 858.56 seconds
root@kali:~/Desktop/uber.com#
dirb
dirbuster
kali-linux-wallpaper-v7.png
kali-linux-wallpaper-v8.png
maxresdefault.jpg
Screenshot from 2020-10-16 18-46-21....
Screenshot from 2020-10-17 22-26-25....
Screenshot from 2020-10-19 14-58-47....
waybackurl

Vulnerability Analyzing Phrase & Recommendation

- To scan OWASP TOP 10 vulnerabilities I used **Netsparker** Professional version.
- Netsparker is a web application security scanner that automatically detects SQL injection, Cross-site Scripting (XSS), and other web application vulnerabilities. We can generate a Details report, summary report, and OWASP Top 10 Security risk report for our scope.
- Below domains was scanned by Netsparker and vulnerabilities are categorized under OWASP Top 10.

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

Cross-Site Scripting (XSS)

a) [Possible] Cross-site Scripting

- Severity: MEDIUM
- Method: GET

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact:

Many different attacks can be leveraged through the use of XSS, including

- Hijacking a user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

Proof of Concepts:

A3 - CROSS-SITE SCRIPTING (XSS)

[Possible] Cross-site Scripting	GET	https://www.uber.com/bh/en/drive/basics/%27%22%20ns%3dnetsparker(0x003CD2)%20/	MEDIUM
[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/ride/javascript%3anetsparker(0x00A38D)/scooters-and-jump-bikes/#main	MEDIUM
[Possible] Cross-site Scripting	GET	https://www.uber.com/be/en/deliver/basics/%2527%253e%253cnet%2bsparker%253dnetsparker(0x00562E)%253e/	MEDIUM
[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/about/%2526%252339%253b%252bnetsparker(0x00BB8A)%252b%2526%252339%253b/#main	MEDIUM
[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/ride/how-it-works/change-location/'ns='netsparker(0x000BB9)/	MEDIUM
[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/deliver/basics/before-you-start/how-to-get-support/%20ns=netsparker(0x002EE9)/	MEDIUM
[Possible] Cross-site Scripting	GET	https://www.uber.com/jo/ar/ride/how-it-works/change-location/%22ns=%22netsparker(0x000716)/	MEDIUM
[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/en/about/diversity/able-at-uber/%22ns=%22netsparker(0x01A20B)/	MEDIUM
[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/ride/%3chtml%20xmlns%3d%22http%3a%2f%2fwww.w3.org%2f1999%2fxhtml%22%3e%3cscript%3enetsparker(0x00BA87)%3c%2fscript%3e%3c%2fhtml%3e/scooters-and-jump-bikes/#main	MEDIUM
[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/ar/deliver/basics/%2527%2522--%253e%253c%252fstyle%253e%253c%252fscRipt%253e%253cscRipt%253enetsparker(0x006644)%253c%252fscRipt%253e/	MEDIUM
[Possible] Cross-site Scripting	GET	https://www.uber.com/be/en/drive/%20netsparker(0x008EDD)%20/inspections/	MEDIUM
[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/ride/how-it-works/%0anetsparker(0x00C05F)%3b/#main	MEDIUM
[Possible] Cross-site Scripting	GET	https://www.uber.com/lk/en/about/1%2bns%253dnetsparker(0x00AF9C)%255cu0020/#main	MEDIUM
[Possible] Cross-site Scripting	GET	https://www.uber.com/ar/en/deliver/basics/making-deliveries/back-to-back-trips/'%22@--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003805)%3C/scRipt%3E/	MEDIUM

Recommendations:

Remedy

This issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered / encoded. Output should be filtered / encoded according to the output format and location.

There are a number of pre-defined, well structured whitelist libraries available for many different environments. Good examples of these include OWASP Reformand Microsoft Anti-Cross-site Scriptinglibraries.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

Security Misconfiguration

a) [Possible]HTTP Strict Transport Security (HSTS) Errors and Warnings

- Severity: MEDIUM
- Method: GET

Impact:

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

Recommendations:

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:

187 / 231

  - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
  - The `max-age` must be at least 31536000 seconds (1 year)
  - The `includeSubDomains` directive must be specified
  - The `preload` directive must be specified
  - If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

b) [Possible] Cookie Not Marked as HttpOnly

- Severity: LOW
- Method: GET
-

Impact:

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Recommendations:

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnelto bypass HTTPOnly protection.

Proof of Concepts:

Sensitive Data Exposure

a) **[Possible] Password Transmitted over Query String**

- Severity: MEDIUM
- Method: GET

Impact:

A password is sensitive data and shouldn't be transmitted over the query string. There are several information-leakage scenarios:

If your website has external links or even external resources (such as image, javascript, etc), then your query string would be leaked.

- The query string is generally stored in server logs.
- Browsers will cache the query string.

Recommendations:

Do not send any sensitive data through the query string.

b) **[Possible] Weak Ciphers Enabled**

- Severity: MEDIUM
- Method: GET

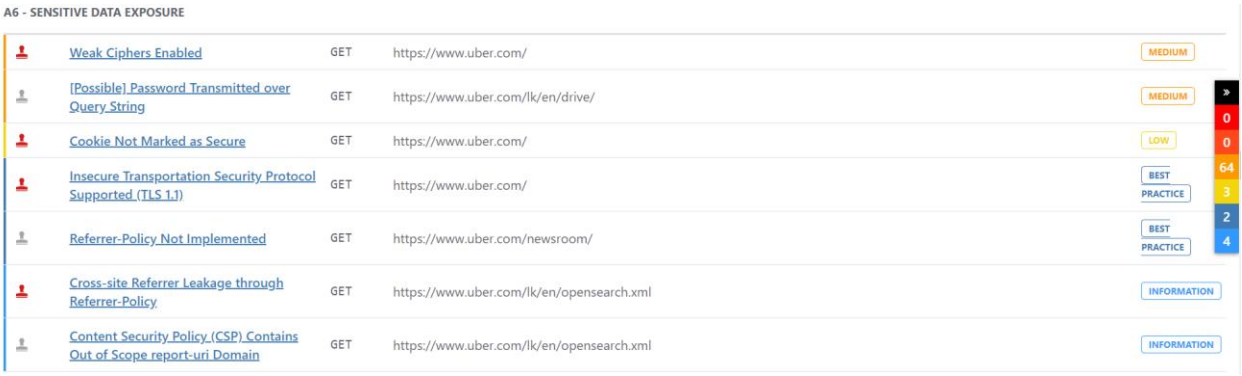
Impact:

Attackers might decrypt SSL traffic between your server and your visitors.

Recommendations:

Configure your webserver to disallow using weak ciphers.

Proof of Concepts:



Using Components with Known Vulnerabilities

a) [Possible] BREACH Attack Detected

- Severity: MEDIUM
- Method: GET

Impact:

Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

- Inject partial plaintext they have uncovered into a victim's requests
- Measure the size of encrypted traffic

Recommendations:

Remedy

Netsparker reported a Possible BREACH Attack issue because the target web page meets the following conditions that facilitate it:

- Served from a server that uses HTTP-level compression (ie. gzip)
- Reflects user-input in the HTTP response bodies
- Contains sensitive information (such as a CSRF token) in HTTP response bodies

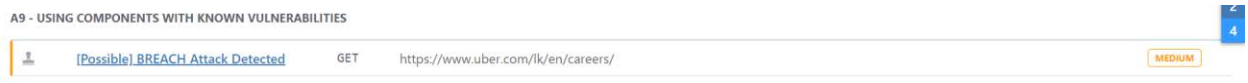
To mitigate the issue, we recommend the following solutions:

1. If possible, disable HTTP level compression

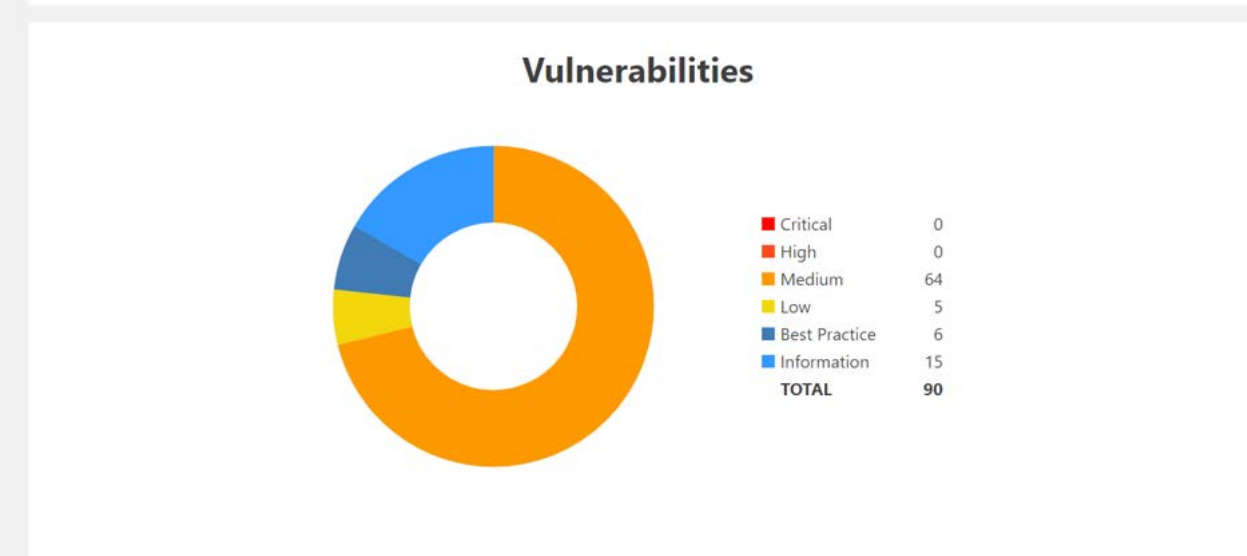
---

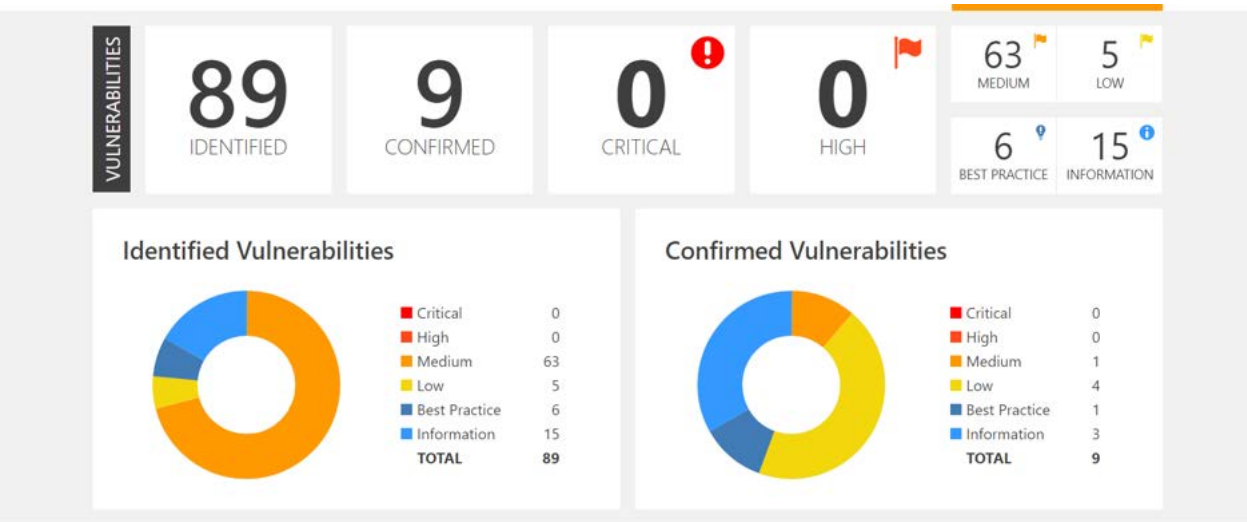
2. Separate sensitive information from user input
3. Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
4. Hide the length of the traffic by adding a random number of bytes to the responses.
5. Add in a rate limit, so that the page maximum is reached five times per minute.

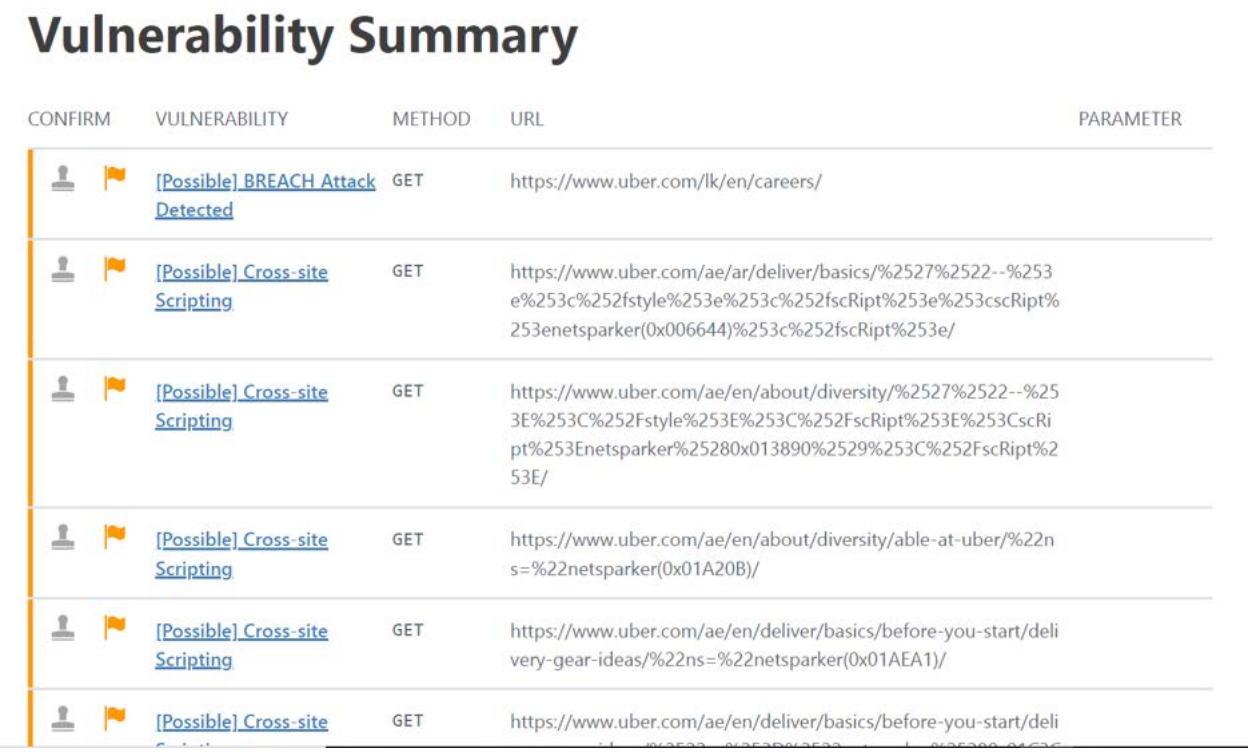
Proof of Concepts:



Overview Summary:


Vulnerabilities
Critical 0
High 0
Medium 64
Low 5
Best Practice 6
Information 15
TOTAL 90


VULNERABILITIES
89
IDENTIFIED
9
CONFIRMED
0
CRITICAL
0
HIGH
63
MEDIUM
5
LOW
6
BEST PRACTICE
15
INFORMATION
Identified Vulnerabilities
Critical 0
High 0
Medium 63
Low 5
Best Practice 6
Information 15
TOTAL 89
Confirmed Vulnerabilities
Critical 0
High 0
Medium 1
Low 4
Best Practice 1
Information 3
TOTAL 9



Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	[Possible] BREACH Attack Detected	GET	https://www.uber.com/lk/en/careers/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/ar/deliver/basics/%2527%2522--%253e%253c%252fstyle%253e%253c%252fscRipt%253e%253cscRipt%253enetsparker(0x006644)%253c%252fscRipt%253e/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/en/about/diversity/%2527%2522--%253E%253C%252Fstyle%253E%253C%252FscRipt%253E%253CscRipt%253Enetsparker%25280x013890%2529%253C%252FscRipt%253E/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/en/about/diversity/able-at-uber/%22ns=%22netsparker(0x01A20B)/	
	[Possible] Cross-site Scripting	GET	https://www.uber.com/ae/en/deliver/basics/before-you-start/delivery-gear-ideas/%22ns=%22netsparker(0x01AEA1)/	
	[Possible] Cross-site	GET	https://www.uber.com/ae/en/deliver/basics/before-you-start/deli	

2. Target Domain: **https://www.marketplace.uber.com**

Security Misconfiguration

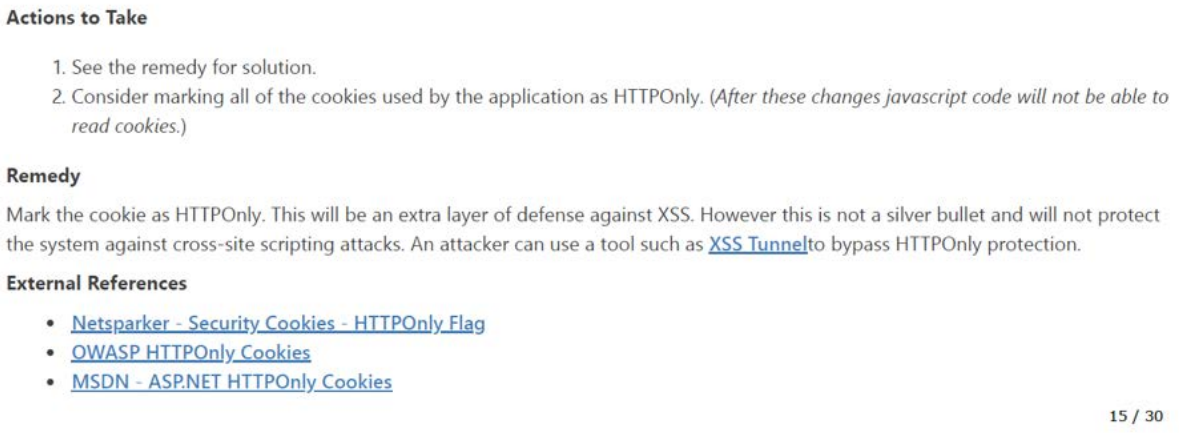
a) Cookie Not Marked as HttpOnly

- Severity: LOW
- Method: GET

Impact:

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Recommendations:



Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnelto bypass HTTPOnly protection.

External References

- Netsparker - Security Cookies - HTTPOnly Flag
- OWASP HTTPOnly Cookies
- MSDN - ASP.NET HTTPOnly Cookies

15 / 30

b) Missing X-Frame-Options Header

- Severity: LOW
- Method: GET

Impact:

Clickjacking is when 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 were intending to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Recommendations:

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

External References

- Clickjacking
- Can I Use X-Frame-Options
- X-Frame-Options HTTP Header

20 / 30

c) Version Disclosure (Nginx)

- Severity: LOW
- Method: GET

Impact:

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Recommendations:

Remedy

Add the following line to your nginx.conf file to prevent information leakage from the `SERVER`header of its HTTP response:

```
server_tokens off
```

Proof of Concepts:

Sensitive Data Exposure

a) Weak Ciphers Enabled

- Severity: MEDIUM
- Method: GET

Impact:

Attackers might decrypt SSL traffic between your server and your visitors.

b) HTTP Strict Transport Security (HSTS) Policy Not Enabled

- Severity: MEDIUM
- Method: GET

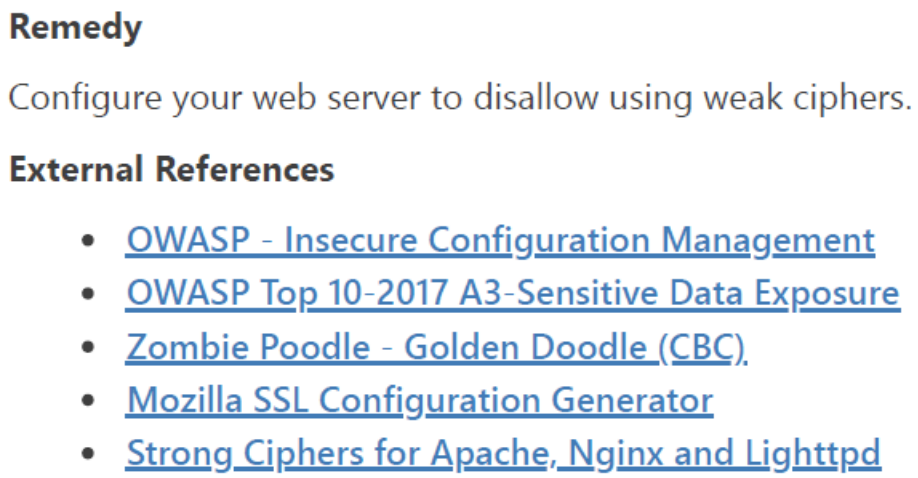
HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via an HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period during which the user agent shall access the server in only a 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. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)

If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Recommendations:



Remedy

Configure your web server to disallow using weak ciphers.

External References

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- Zombie Poodle - Golden Doodle (CBC)
- Mozilla SSL Configuration Generator
- Strong Ciphers for Apache, Nginx and Lighttpd

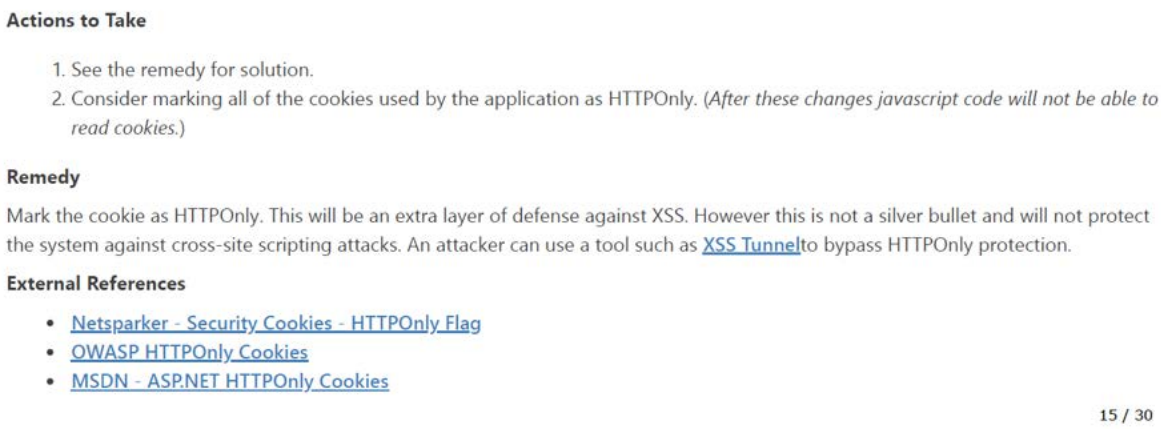
c) Cookie Not Marked as HttpOnly

- Severity: LOW
- Method: GET

Impact:

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Recommendations:



Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnelto bypass HTTPOnly protection.

External References

- Netsparker - Security Cookies - HTTPOnly Flag
- OWASP HTTPOnly Cookies
- MSDN - ASP.NET HTTPOnly Cookies

15 / 30

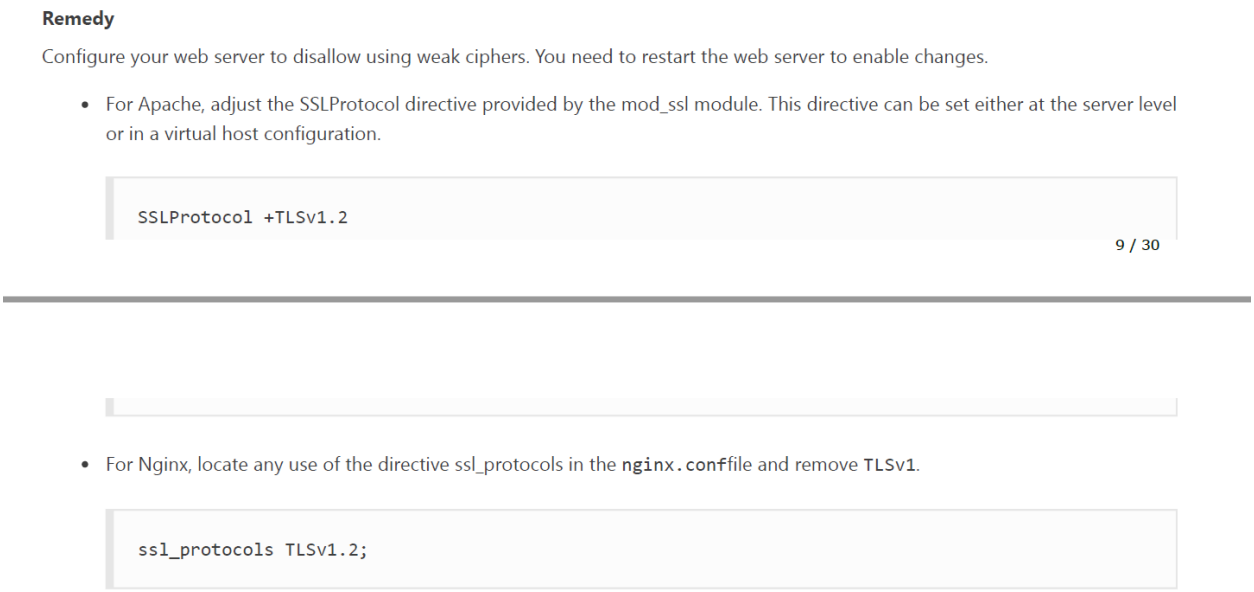
d) Insecure Transportation Security Protocol Supported (TLS 1.0)

- Severity: LOW
- Method: GET

Impact:

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Recommendations:



Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

9 / 30

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf`file and remove `TLSv1`.

```
ssl_protocols TLSv1.2;
```

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf`file and remove `TLSv1`.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on 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.**
    1. Click on Start and then Run, type `regedt32`or `regedit`, and then click OK.
    2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\
```

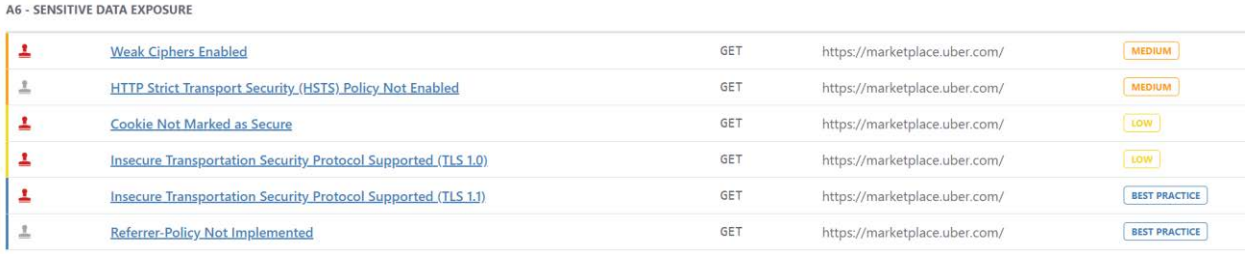
    3. Locate a key named `Server`or create if it doesn't exist.
    4. Under the `Server`key, locate a DWORD value named `Enabled`or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

External References

- How to Disable TLS v1.0
- OWASP - Insecure Configuration Management
- OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
- How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services
- IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012
- Date Change for Migrating from SSL and Early TLS
- Browser Exploit Against SSL/TLS Attack (BEAST)
- Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS

Proof of Concepts:



Using Components with Known Vulnerabilities

a) Out-of-date Version (Nginx)

- Severity: INFORMATION
- Method: GET

Impact:

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

Recommendations:

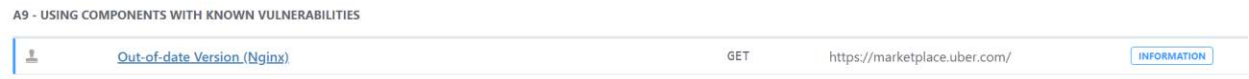
Remedy

Please upgrade your installation of Nginx to the latest stable version.

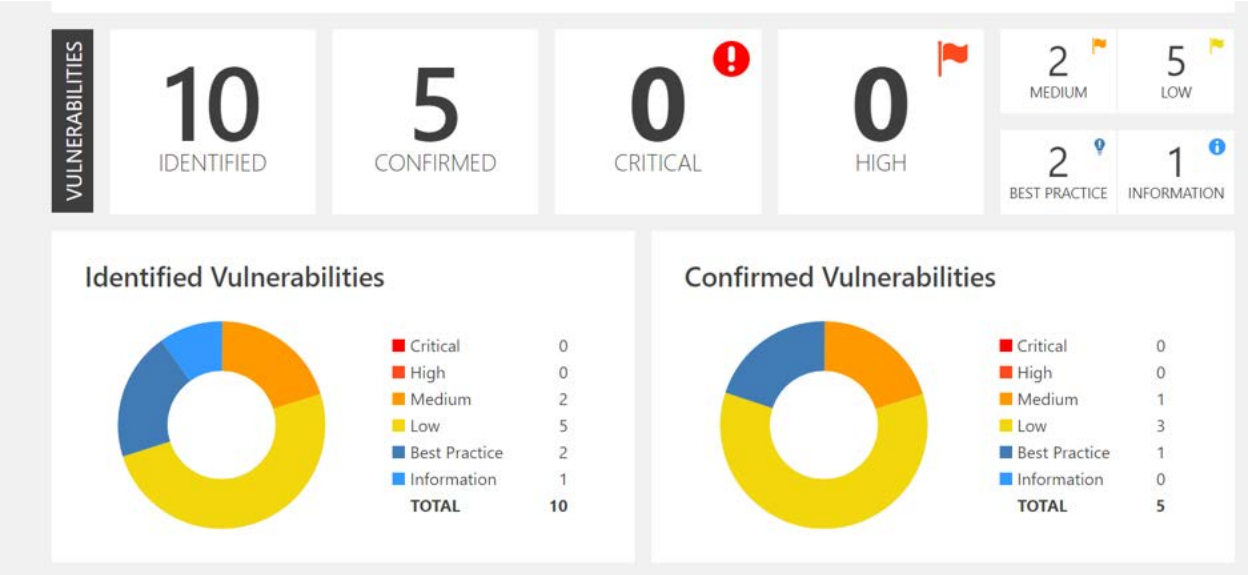
Remedy References

- Downloading Nginx

Proof of Concepts:

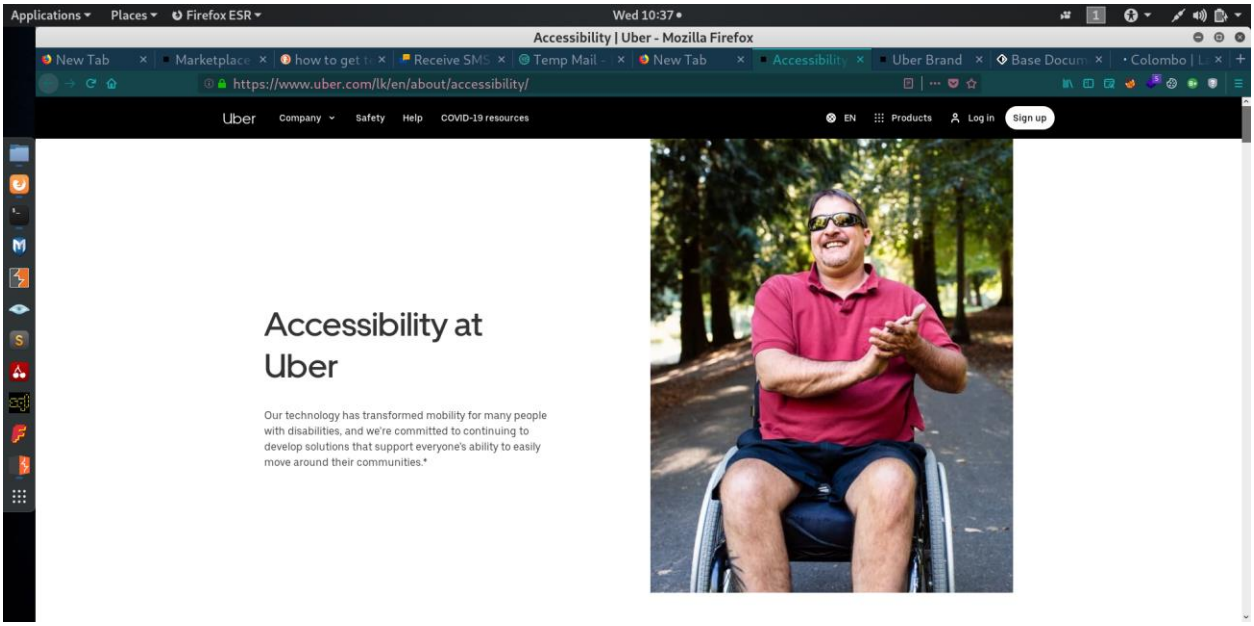


Overview Summary:



- Below domains are scanned by the Acunetix Consultant version.
- Acunetix is an automated web app security testing tool that tests for vulnerabilities including SQL injection, cross-site scripting, and other exploitable vulnerabilities for the auditing of your web application. Acunetix uses the HTTP / HTTPS protocol to search any websites or web applications that are accessible through a web browser.

3. Target Domain: **https://accessibility.uber.com**



Scan of https://www.uber.com:443/lk/en/about/accessibility/

Scan details

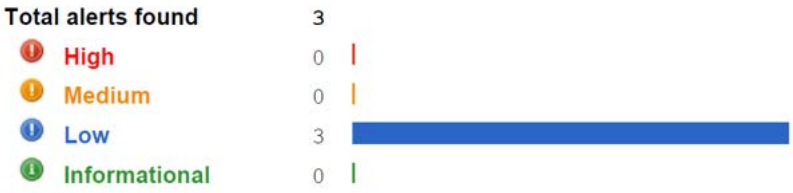
Scan information	
Start time	10/21/2020 1:42:45 AM
Finish time	10/21/2020 1:50:12 AM
Scan time	7 minutes, 26 seconds
Profile	Default
Server information	
Responsive	True
Server banner	ufe
Server OS	Unknown

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution



a) Cookie without HttpOnly flag set

Severity:	**Low**
Type:	Informational
Reported by module:	Crawler
Classification:	CVSS: Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
	CWE-16

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.

Cookie without HttpOnly flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.

Affected items

/
Details
Cookie name: "marketing_vistor_id" Cookie domain: "uber.com"
Request headers
`GET / HTTP/1.1`

/
Details
Cookie name: "_ua" Cookie domain: "www.uber.com"
Request headers
`GET / HTTP/1.1`

b) Slow response time

Severity:	**Low**
Type:	Informational
Reported by module:	Crawler
Classification:	CVSS: Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: Partial
	CVSS3: Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: High
	CWE-400

Description

This page had a slow response time. This type of file can be targeted in denial of service attacks. An attacker can request this page repeatedly from multiple computers until the server becomes overloaded.

Impact

Possible denial of service.

Recommendation

Investigate if it's possible to reduce the response time for this page.

Slow response time

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This page had a slow response time. This type of files can be targeted in denial of service attacks. An attacker can request this page repeatedly from multiple computers until the server becomes overloaded.

Impact

Possible denial of service.

Recommendation

Investigate if it's possible to reduce the response time for this page.

Affected items

/lk/en/about/accessibility

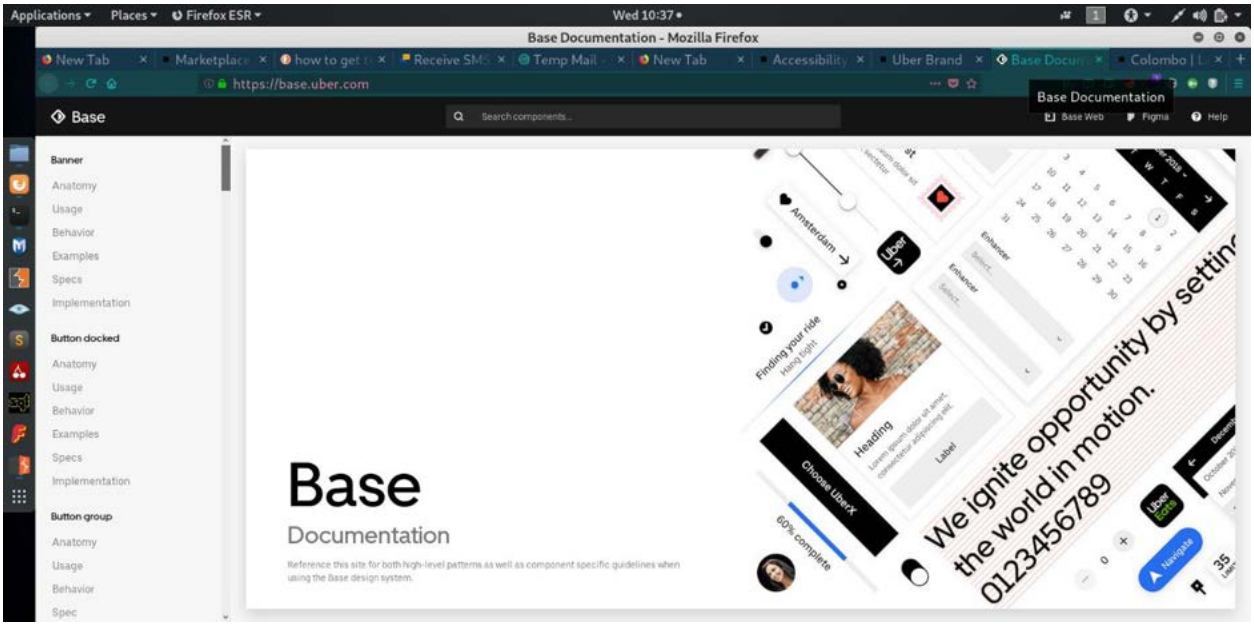
Details

The response time for this page was 6094 ms while the average response time for this site is 611.13 ms

Request headers

```
GET /lk/en/about/accessibility/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Host: www.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

4. Target Domain: **https://base.uber.com:443/**



Scan of https://base.uber.com:443/

Scan details

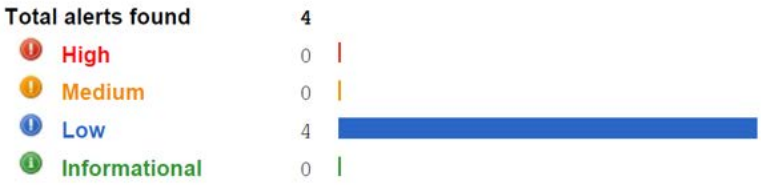
Scan information	
Start time	10/21/2020 1:05:03 AM
Finish time	10/21/2020 1:21:45 AM
Scan time	16 minutes, 42 seconds
Profile	Default
Server information	
Responsive	True
Server banner	Vercel
Server OS	Unknown

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution



a) Clickjacking: X-Frame-Options header missing

Severity:	**Low**
Type:	Configuration
Reported by module:	Scripting (Clickjacking_X_Frame_Options.script)
Classification:	CVSS: Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial

	- Availability Impact: Partial
	CWE-693

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your webserver to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

Alerts summary

Clickjacking: X-Frame-Options header missing

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-693

Affected items	Variation
Web Server	1

Alert details

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Type	Configuration
Reported by module	Scripting (Clickjacking_X_Frame_Options.script)

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

Clickjacking
OWASP Clickjacking
Defending with Content Security Policy frame-ancestors directive
Frame Buster Buster
Clickjacking Protection for Java EE
The X-Frame-Options response header

Affected items

Web Server
Details
No details are available.
Request headers

```
GET / HTTP/1.1
Host: base.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

b) Insecure response with wildcard '*' in Access-Control-Allow-Origin

Severity:	**Low**
Type:	Configuration
Reported by module:	Scripting (Access_Control_Allow_Origin_Dir.script)
Classification:	CVSS :Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
	CWE-16

Description

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based on returning the value of the Origin request header, "*", or "null" in the response.

If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin.

Therefore, any website can make XHR (XMLHTTPRequest) requests to your site and access the responses. It's not recommended to use the Access-Control-Allow-Origin: * header.

Impact

Any website can make XHR requests to your site and access the responses.

Recommendation

Is recommended not to use Access-Control-Allow-Origin: *. Instead, the Access-Control-Allow-Origin header should contain the list of origins that can make COR requests.

Insecure response with wildcard '*' in Access-Control-Allow-Origin

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/	1
/_next/data/URrrrIxD9ZYM1pG8A4ibJ	1
/_next/static/URrrrIxD9ZYM1pG8A4ibJ/pages	1

Insecure response with wildcard '*' in Access-Control-Allow-Origin

Severity	**Low**
Type	Configuration
Reported by module	Scripting (Access_Control_Allow_Origin_Dir.script)

Description

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based by returning the value of the Origin request header, "*", or "null" in the response.

If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin. Therefore, any website can make XHR (XMLHTTPRequest) requests to your site and access the responses. It's not recommended to use the Access-Control-Allow-Origin: * header.

Impact

Any website can make XHR requests to your site and access the responses.

Recommendation

Is recommended not to use Access-Control-Allow-Origin: *. Instead the Access-Control-Allow-Origin header should contain the list of origins that can make COR requests.

References

CrossOriginRequestSecurity

Affected items

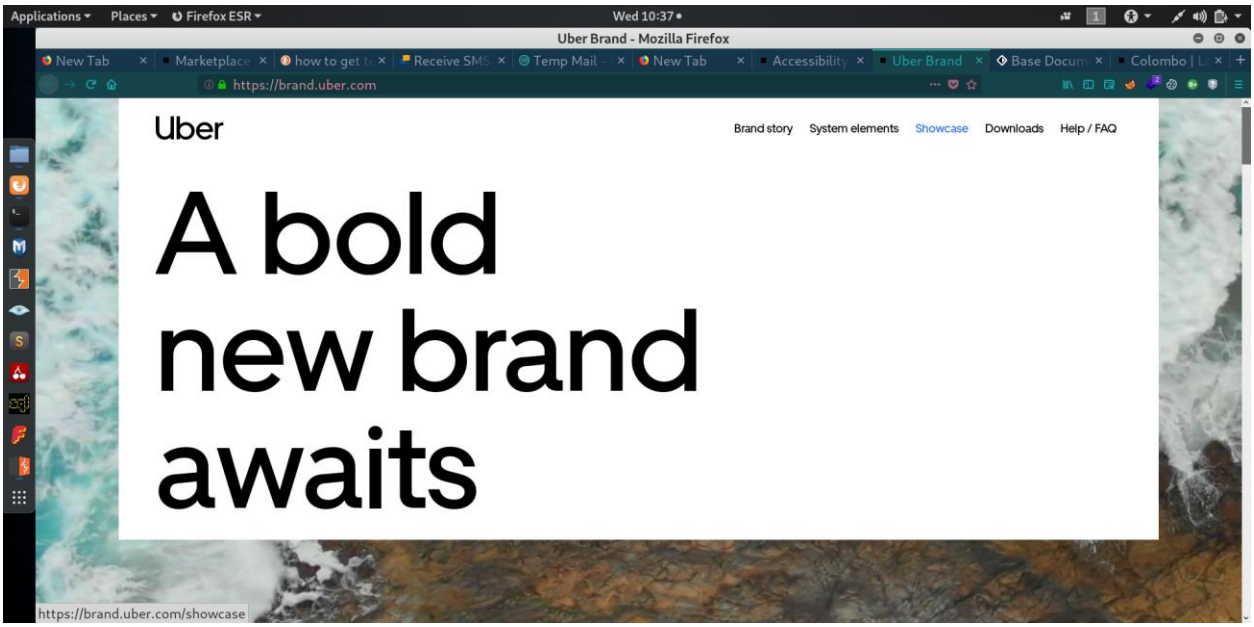
/
Details
No details are available.
Request headers

```
GET / HTTP/1.1
Host: base.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/_next/data/URrrrIxD9ZYM1pG8A4ibJ
Details
No details are available.
Request headers

```
GET /_next/data/URrrrIxD9ZYM1pG8A4ibJ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://base.uber.com/_next/data
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
```

5. Target Domain: **https://brand.uber.com:443/**



Scan of https://brand.uber.com:443/

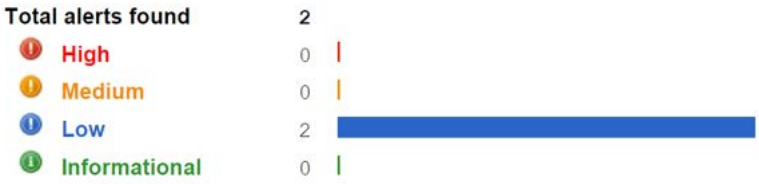
Scan details

Scan information	
Start time	10/21/2020 2:07:52 AM
Finish time	10/21/2020 2:23:16 AM
Scan time	15 minutes, 23 seconds
Profile	Default
Server information	
Responsive	True
Server banner	ufe
Server OS	Unknown

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution



a) Cookie without HttpOnly flag set

Severity:	**Low**
Type:	Informational
Reported by module:	Crawler
Classification:	CVSS : Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None

	- Integrity Impact: None - Availability Impact: None
	CWE-16

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is important security protection.

for session cookies.

Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.

Alert details

Cookie without HttpOnly flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

b) Slow response time

Severity:	**Low**
Type:	Informational
Reported by module:	Crawler
Classification:	CVSS: Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: Partial
	CVSS3: Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: High
	CWE-400

Description

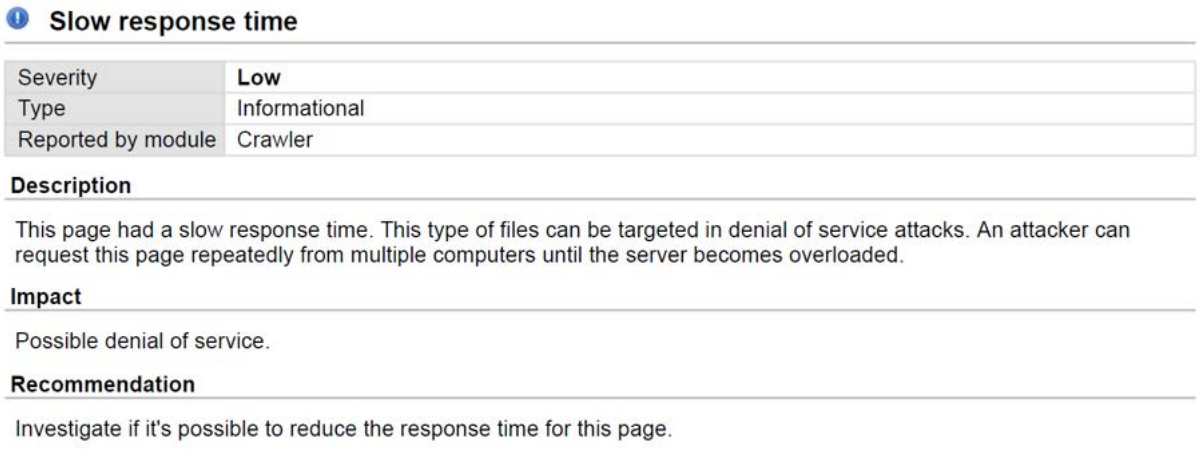
This page had a slow response time. This type of file can be targeted in denial of service attacks. An attacker can request this page repeatedly from multiple computers until the server becomes overloaded.

Impact

Possible denial of service.

Recommendation

Investigate if it's possible to reduce the response time for this page.



Slow response time

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This page had a slow response time. This type of files can be targeted in denial of service attacks. An attacker can request this page repeatedly from multiple computers until the server becomes overloaded.

Impact

Possible denial of service.

Recommendation

Investigate if it's possible to reduce the response time for this page.

6. Target Domain: **http://drive.uber.com**

Scan of https://www.uber.com:443/lk/en/drive/

Scan details

Scan information	
Start time	10/21/2020 2:40:35 AM
Finish time	10/21/2020 3:01:40 AM
Scan time	21 minutes, 5 seconds
Profile	Default
Server information	
Responsive	True
Server banner	ufe
Server OS	Unknown

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

a) HTML form without CSRF protection

Severity:	**Medium**
Type:	Informational
Reported by module:	Crawler
Classification:	CVSS Base Score: 2.6 - Access Vector: Network

	- Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
	CVSS3 Base Score: 4.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: Required - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: Low - Availability Impact: None
	CWE-352

Description

This alert may be a false positive, manual confirmation is required.

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Acunetix WVS found an HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end-user data and operation in the case of a normal user. If the targeted end-user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

HTML form without CSRF protection

Severity	**Medium**
Type	Informational
Reported by module	Crawler

Description

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker"s choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Affected items

/lk/en/drive (64adbddee16dbd3ed58373c9670b7daa)

Details

Form name: <empty>
Form action: https://www.uber.com/lk/en/drive/
Form method: GET

Form inputs:

- firstName [Text]
- lastName [Text]
- email [Text]
- password [Password]
- contactInfo [Text]
- city [Text]
- inviterCode [Text]

Request headers

```
GET /lk/en/drive/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
```

- firstName [Text]
- lastName [Text]
- email [Text]
- password [Password]
- contactInfo [Text]
- city [Text]
- inviterCode [Text]

Request headers

```
GET /lk/en/drive/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie:
_ua={"session_id":"7c623c6e-ad18-4cfc-aeee-0482967db0f3","session_time_ms":1603273235856
}; marketing_vistor_id=dde45f96-66fb-4bd4-82e9-7db318c54bd6;
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDMyNzMyMzUsImV4cCI6MTYwMzM
1OTYzNX0._7yeE_FeFmM10Ils27Im2763nuyPjJVm6aPKX9Y-8HY
Host: www.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept: */*
```

b) Cookie without HttpOnly flag set

Severity:	**Low**
Type:	Informational
Reported by module:	Crawler
Classification:	CVSS Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
	CWE-16

Description

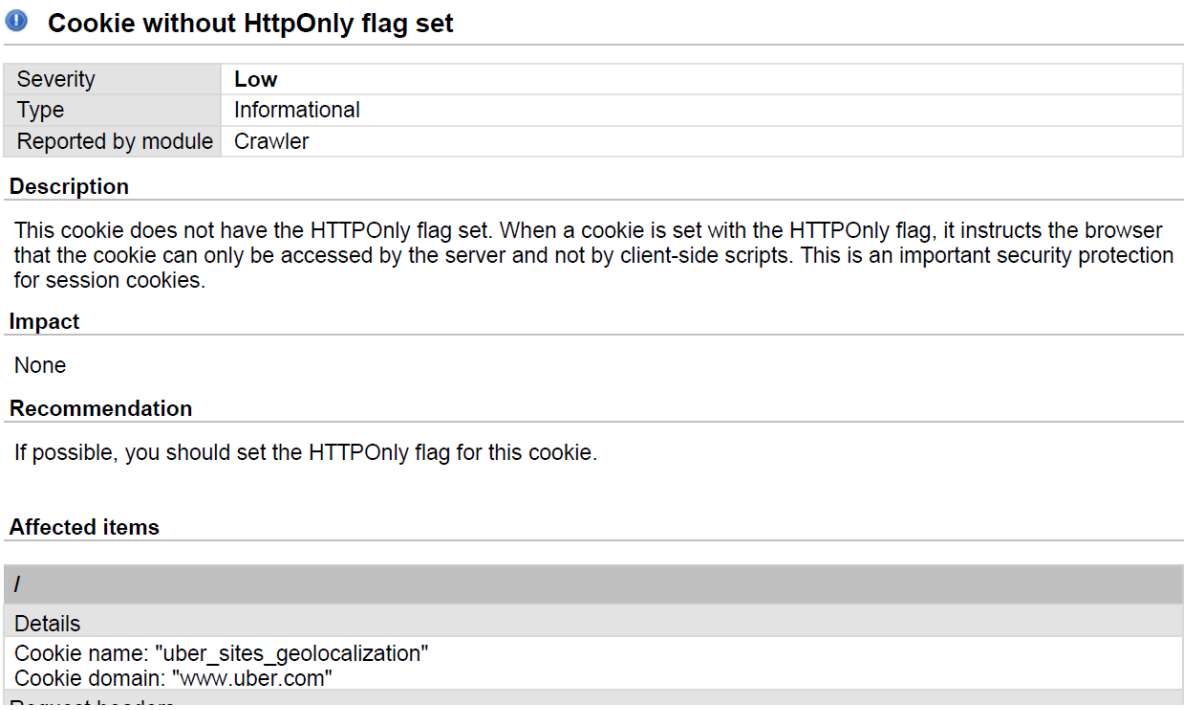
This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.



Cookie without HttpOnly flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.

Affected items

/
Details
Cookie name: "uber_sites_geolocalization" Cookie domain: "www.uber.com"

Request headers
GET / HTTP/1.1

/
Details
Cookie name: "marketing_vistor_id" Cookie domain: "uber.com"
Request headers
GET / HTTP/1.1

/
Details
Cookie name: "_ua" Cookie domain: "www.uber.com"
Request headers
GET / HTTP/1.1

c) Cookie without Secure flag set

Severity:	**Low**
Type:	Informational
Reported by module:	Crawler
Classification:	CVSSBase Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
	CWE-16

Description

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the Secure flag for this cookie.

Cookie without Secure flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the Secure flag for this cookie.

Affected items

/
Details
Cookie name: "uber_sites_geolocalization" Cookie domain: "www.uber.com"
Request headers
`GET / HTTP/1.1`

d) Login page password-guessing attack

Severity:	**Low**
Type:	Validation
Reported by module:	Scripting (Html_Authentication_Audit.script)
	CVSS Base Score: 5.0

Classification:	- Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
	CVSS3 Base Score: 5.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: Low
	CWE-307

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

Login page password-guessing attack

Severity	**Low**
Type	Validation
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

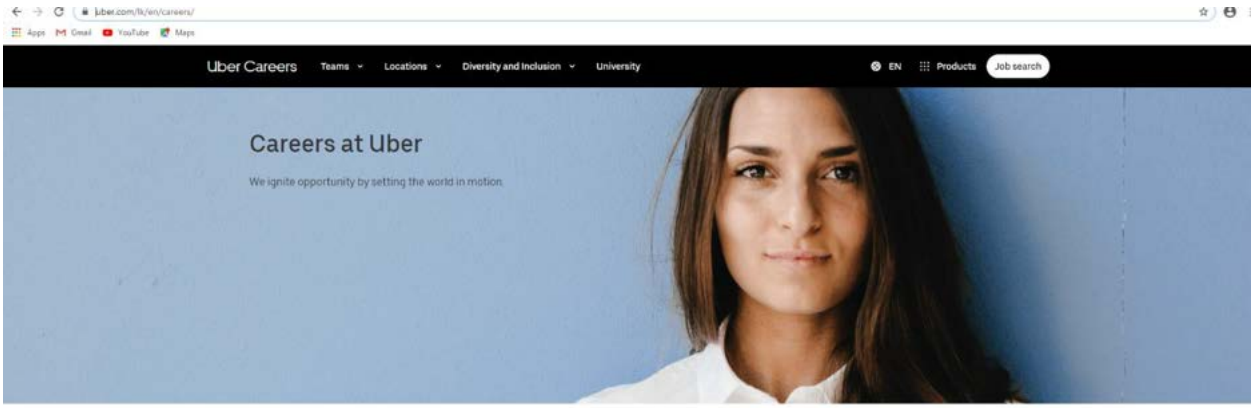
Blocking Brute Force Attacks

Affected items

/lk/en/drive/
Details
The scanner tested 10 invalid credentials and no account lockout was detected.
Request headers

```
GET
/lk/en/drive/?city=Colombo%2c%20Sri%20Lanka&contactInfo=1&email=UDP6U548%40www.uber.com&
firstName=tyouyljg&inviterCode=94102&lastName=rjvlvtic&password=tQchPJp8 HTTP/1.1
User-Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Referer: https://www.uber.com:443/lk/en/drive/
Host: www.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept: */*
```

7. Target Domain: **http://careersinfo.uber.com**



Scan details

Scan information	
Start time	10/21/2020 7:17:06 AM
Finish time	10/21/2020 7:24:02 AM
Scan time	6 minutes, 56 seconds
Profile	Default
Server information	
Responsive	True
Server banner	ufe
Server OS	Unknown

Alerts distribution

Total alerts found	2
High	0
Medium	0
Low	2
Informational	0

a) Cookie without HttpOnly flag set

Severity:	**Low**
Type:	Informational
Reported by module:	Crawler
Classification:	CVSS: Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
	CWE-16

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is important security protection for session cookies.

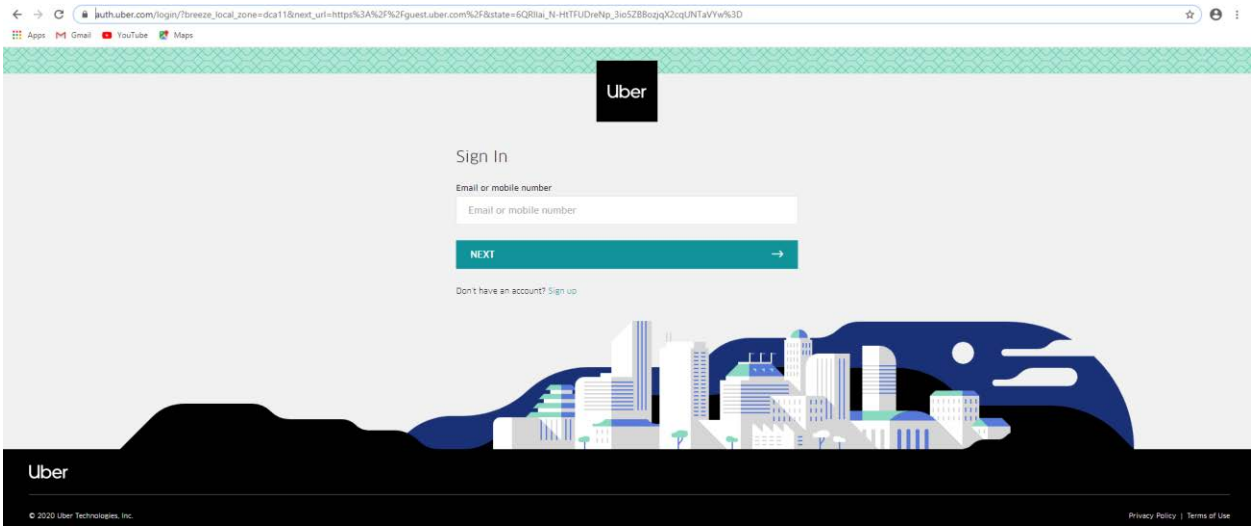
Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.

8. Target Domain: **https://auth.uber.com:443/login/**



https://auth.uber.com:443/login/?breeze_local_zone=dca11&next_url=https%3A%2F%2Fguest.uber.com%2F&state=6QRIlai_N-HtTFUDreNp_3io5ZBBozjqX2cqUNTaVYw%3D

Scan details

Scan information	
Start time	10/21/2020 3:12:23 AM
Finish time	The scan was aborted
Scan time	4 hours, 2 minutes
Profile	Default
Server information	
Responsive	True
Server banner	ufe
Server OS	Unknown

Alerts distribution

Total alerts found	11
High	0
Medium	2
Low	4
Informational	5

a) BREACH attack

Severity:	**Medium**
Type:	Configuration
Reported by module:	Scripting (XSS.script)
Classification:	CVSS Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
	CVSS3 Base Score: 9.1 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: High - Availability Impact: None
	CWE-310
	CVE-2013-3587
Affected items	**/login/session**

Description

This web application is potentially vulnerable to the BREACH attack.

An attacker with the ability to:

- Inject partially chosen plaintext into a victim's requests
- Measure the size of encrypted traffic that can leverage information leaked by compression to recover targeted parts of the plaintext.

BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) is a category of vulnerabilities and not a specific instance affecting a specific piece of software. To be vulnerable, a web application must:

- Be served from a server that uses HTTP-level compression
- Reflect user-input in HTTP response bodies
- Reflect a secret (such as a CSRF token) in HTTP response bodies

Impact

An attacker can leverage information leaked by compression to recover targeted parts of the plaintext.

Recommendation

The mitigations are ordered by effectiveness (not by their practicality - as this may differ from one application to another).

- Disabling HTTP compression
- Separating secrets from user input
- Randomizing secrets per request
- Masking secrets (effectively randomizing by XORing with a random secret per request)
- Protecting vulnerable pages with CSRF
- Length hiding (by adding a random number of bytes to the responses)
- -Rate-limiting the requests

References

- CVE-2013-3587
- BREACH attack

BREACH attack

Severity	**Medium**
Type	Configuration
Reported by module	Scripting (XSS.script)

Description

This web application is potentially vulnerable to the BREACH attack.

An attacker with the ability to:

- Inject partial chosen plaintext into a victim's requests
- Measure the size of encrypted traffic

can leverage information leaked by compression to recover targeted parts of the plaintext.

BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) is a category of vulnerabilities and not a specific instance affecting a specific piece of software. To be vulnerable, a web application must:

- Be served from a server that uses HTTP-level compression
- Reflect user-input in HTTP response bodies
- Reflect a secret (such as a CSRF token) in HTTP response bodies

Impact

An attacker can leverage information leaked by compression to recover targeted parts of the plaintext.

Recommendation

The mitigations are ordered by effectiveness (not by their practicality - as this may differ from one application to another).

- Disabling HTTP compression
- Separating secrets from user input
- Randomizing secrets per request
- Masking secrets (effectively randomizing by XORing with a random secret per request)
- Protecting vulnerable pages with CSRF
- Length hiding (by adding random number of bytes to the responses)
- Rate-limiting the requests

References

CVE-2013-3587
BREACH attack

Affected items

/login/session

Details

This alert was issued because the following conditions were met:

- The page content is served via HTTPS
- The server is using HTTP-level compression
- URL encoded POST input addPassword was reflected into the HTTP response body.
- HTTP response body contains a secret named x-csrf-token

Request headers

```
POST /login/session HTTP/1.1
Content-Length: 3719
Content-Type: application/x-www-form-urlencoded
Referer:
https://auth.uber.com:443/login/?breeze_local_zone=dca11&next_url=https%3A%2F%2Fguest.ub
```

```
(line truncated)
...K0nhA%3D%3DPrj97OuNIS2Yr1RViwlydw%3D%3D8qAraL31AS6x29b1MJQULw6OENJRJe2McDh%2FJkkJtLY%
3D;
_ua=%7B%22id%22%3A%2245f4d390-c9d6-474a-bf08-31e725d82c53%22%2C%22ts%22%3A1603275163215%
7D; _cc=ARvEsqMInSFEPHrejkm2AjxE;
udi-fingerprint=qMqquWHtavdr%2BnM7qRqb3P4xp1qENXkmBztzU8pWPh4jju3GL5xyN3mOL12dIMdlvgfF5O
NZDdCEZeHbVwmFWQ%3D%3Db3H1wKvJvlBJ4shOGrXg5lBDAVLpftIv5DDGnzwTK8k%3D;
marketing_vistor_id=bba10375-b595-421c-9d24-67361f95fa62;
_cc-x=ZGQyODkwNWUtNTNkOS00YWQyLTg2OWEtNWM4NWRkY2UyY2M2OjE2MDMyNzUxNjQ2Mzc
Host: auth.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

addPassword=g00dPa%2524%2524w0rD_9782&autoSMSVerificationSupported=false&countryCode=1&e
mail=sample%40email.tst&firstName=xluhnmuh&firstPartyClientID=&in ...
```

b) HTML form without CSRF protection

Severity:	**Medium**
Type:	Informational
Reported by module:	Crawler
Classification:	CVSS Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None

	CVSS3 Base Score: 4.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: Required - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: Low - Availability Impact: None
	CWE-352

Description

This alert may be a false positive, manual confirmation is required.

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Acunetix WVS found an HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end-user data and operation in the case of a normal user. If the targeted end-user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

HTML form without CSRF protection

Severity	**Medium**
Type	Informational
Reported by module	Crawler

Description

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker"s choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Affected items

/login (8363fac6c7655f235e9ddbc9bd46fad0)

Details

Form name: <empty>
Form action: https://auth.uber.com/login/
Form method: POST

Form inputs:

- textInputValue [Text]

Request headers

```
GET
/login/?breeze_local_zone=dca11&next_url=https://guest.uber.com/&state=6QRlIai_N-HtTFUDr
eNp_3io5ZBBozjqX2cqUNTaVYw%3D HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Host: auth.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

c) Cookie without HttpOnly flag set

Severity:	**Low**
Type:	Informational
Reported by module:	Crawler
Classification:	CVSS: Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
	CWE-16

Description

This cookie does not have the secure flag set. When a cookie is set with the secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the secure flag for this cookie.

Cookie without Secure flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the Secure flag for this cookie.

Affected items

/
Details
Cookie name: "udi-fingerprint" Cookie domain: "uber.com"
Request headers
`GET / HTTP/1.1`

/
Details
Cookie name: "marketing_vistor_id" Cookie domain: "uber.com"
Request headers
`GET / HTTP/1.1`

d) Email address found

Severity:	**Informational**
Type:	Informational
Reported by module:	Scripting (Text_Search_Dir.script)
Classification:	CVSS Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None

	- Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
	CVSS3 Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
	CWE-200

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

Email address found

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_Dir.script)

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

Email Address Disclosed on Website Can be Used for Spam

Affected items

/login

Details

Pattern found: support@jump.com
business-support@uber.com
u003Esupport@uber.com
example@ubereats.com
u002Fuber@auth.uber.com

Request headers

```
GET /login/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...izgjmRwKivu19H-kaxXMd2VpkH8rTeJGq9GNd3s21DID9kSaVPFfq5BWdb87_blBcNK88i9lYpVKf8vpb2sRN
JuxFo2om-9J5JEfSaAUNeVSnsL82kKZOw7HVASryCPusFtKEO67pfvA_j_gygu7R_FnIjMRHbw5gKqAyIs2Sfmzu
Q5ald6Gn31WIh2R7mpN_DR8GeYTUrTrCyycJ1s6MeuESrGhCf7Y8AdgYF05OcofQXU3tRlW6j9SigtNI9Fo8Jzj3
Yp-w3vklqTnweWL_IsZvVjORVgniCdCzwEhdJ9X3cOTqPBBO2FQXyk_aDv1EzMPTL7KzDF131iYrthyzw0LZxoBN
cv5aZ3LJrdmpkzdDVtaCGR4d0RPxNne4nYjR_dBrCNnbJ1J3xY0p1_oi3xNVpW5nFhaG4yaqdhQwBlLMOb.16032
75144104.1209600000.tWSXr0t_qe29eyfbib2GpqtGb3uUC6GErnsN7G57YTs
Host: auth.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/login/

Details

Tested on URI: /login/YZCUSwJbex.jsp

Pattern found in response: support@jump.com business-support@uber.com u003Esupport@uber.com example@ubereats.com u002Fuber@auth.uber.com

Request headers

```
GET /login/YZCUSwJbex.jsp HTTP/1.1
(line truncated)
...K0nhA%3D%3DPrj97OuNIS2Yr1RViwlydw%3D%3D8qAraL31AS6x29b1MJQULw6OENJRJe2McDh%2FJkkJtLY%
3D;
```



```
_ua=%7B%22id%22%3A%2245f4d390-c9d6-474a-bf08-31e725d82c53%22%2C%22ts%22%3A1603275163215%
7D; _cc=ARvEsqMInSFEPHrejkm2AjxE;
udi-fingerprint=qMqquWHtavdr%2BnM7qRqb3P4xp1qENXkmBztzU8pWPh4jju3GL5xyN3mOL12dIMdlvgfF5O
NZDdCEZeHbVwmFWQ%3D%3Db3H1wKvJvlBJ4shOGrXg5lBDAVLpftIv5DDGnzwTK8k%3D;
marketing_vistor_id=bba10375-b595-421c-9d24-67361f95fa62;
_cc-x=ZGQyODkwNWUtNTNkOS00YWQyLTg2OWEtNWM4NWRkY2UyY2M2OjE2MDMyNzUxNjQ2Mzc
Host: auth.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/login/session

Details

Pattern found: support@jump.com
business-support@uber.com
u003Esupport@uber.com
example@ubereats.com
u002Fuber@auth.uber.com

Request headers

```
GET /login/session HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://auth.uber.com/login/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...izgjmRwKivu19H-kaxXMd2VpkH8rTeJGq9GNd3s21DID9kSaVPFfq5BWdb87_blBcNK88i9lYpVKf8vpb2sRN
JuxFo2om-9J5JEfSaAUNeVSnsL82kKZOw7HVASryCPusFtKEO67pfvA_j_gygu7R_FnIjMRHbw5gKqAyIs2Sfmzu
Q5ald6Gn31WIh2R7mpN_DR8GeYTUrTrCyycJ1s6MeuESrGhCf7Y8AdgYF05OcofQXU3tRlW6j9SigtNI9Fo8Jzj3
Yp-w3vklqTnweWL_IsZvVjORVgniCdCzwEhdJ9X3cOTqPBBO2FQXyk_aDv1EzMPTL7KzDF131iYrthyzw0LZxoBN
cv5aZ3LJrdmpkzdDVtaCGR4d0RPxNne4nYjR_dBrCNnbJ1J3xY0p1_oi3xNVpW5nFhaG4yaqdhQwBlLMOb.16032
75144104.1209600000.tWSXr0t_qe29eyfbib2GpqtGb3uUC6GErnsN7G57YTs
Host: auth.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/login/udimeta

Details

Pattern found: support@jump.com
business-support@uber.com
u003Esupport@uber.com
example@ubereats.com
u002Fuber@auth.uber.com

Request headers

```
GET /login/udimeta HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://auth.uber.com/login/session
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...K0nhA%3D%3DPrj97OuNIS2Yr1RViwlydw%3D%3D8qAraL31AS6x29b1MJQULw6OENJRJe2McDh%2FJkkJtLY%
3D;
_ua=%7B%22id%22%3A%2245f4d390-c9d6-474a-bf08-31e725d82c53%22%2C%22ts%22%3A1603275163215%
7D; _cc=ARvEsqMInSFEPHrejkm2AjxE;
udi-fingerprint=qMqquWHtavdr%2BnM7qRqb3P4xp1qENXkmBztzU8pWPh4jju3GL5xyN3mOL12dIMdlvgfF5O
NZDdCEZeHbVwmFWQ%3D%3Db3H1wKvJvlBJ4shOGrXg51BDAVLpftIv5DDGnzwTK8k%3D;
marketing_vistor_id=bba10375-b595-421c-9d24-67361f95fa62;
```



```
_cc-x=ZGQyODkwNWUtNTNkOS00YWQyLTg2OWEtNWM4NWRkY2UyY2M2OjE2MDMyNzUxNjQ2Mzc
Host: auth.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

e) Password type input with auto-complete enabled

Severity:	**Informational**
Type:	Informational
Reported by module:	Crawler
Classification:	CVSS Base: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None

	- Availability Impact: None
	CVSS Base: 3 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
	CWE-200

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the clear text password from the browser cache.

Impact

Possible sensitive information disclosure.

Recommendation

The password auto-complete should be disabled in sensitive applications.

To disable auto-complete, you may use a code similar to:

<INPUT TYPE="password" AUTOCOMPLETE="off">

Password type input with auto-complete enabled

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure.

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:
<INPUT TYPE="password" AUTOCOMPLETE="off">

Affected items

/login (bc6f7ffc5a7dc1c3d567d7f49fdddbf0)

Details

Password type input named addPassword from form with ID answerForm with action /login/session has autocomplete enabled.

Request headers

```
GET /login/?next_url=https://guest.uber.com/&source=auth&uber_client_name=riderSignUp
HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer:
https://auth.uber.com/login/?breeze_local_zone=dca11&next_url=https://guest.uber.com/&st
ate=6QRlIai_N-HtTFUDreNp_3iO
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...izgjmRwKivul9H-kaxXMd2VpkH8rTeJGq9GNd3s21DID9kSaVPFfq5BWdb87_blBcNK88i9lYpVKf8vpb2sRN
JuxFo2om-9J5JEfSaAUNeVSnsL82kKZOw7HVASryCPusFtKEO67pfvA_j_gygu7R_FnIjMRHbw5gKqAyIs2Sfmzu
Q5ald6Gn31WIh2R7mpN_DR8GeYTUrTrCyycJ1s6MeuESrGhCf7Y8AdgYF05OcofQXU3tRlW6j9SigtNI9Fo8Jzj3
Yp-w3vklqTnweWL_IsZvVjORVgniCdCzwEhdJ9X3cOTqPBBO2FQXyk_aDv1EzMPTL7KzDF131iYrthyzw0LZxoBN
cv5aZ3LJrdmpkzdDVtaCGR4d0RPxNne4nYjR_dBrCNnbJ1J3xY0p1_oi3xNVpW5nFhaG4yaqdhQwBlLMOb.16032
75144104.1209600000.tWSXr0t_qe29eyfbib2GpqtGb3uUC6GErnsN7G57YTs
Host: auth.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Scanned items (coverage report)

Scanned 3 URLs. Found 3 vulnerable.

URL: https://auth.uber.com/login/

Vulnerabilities have been identified for this URL

8 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
breeze_local_zone	URL encoded GET
next_url	URL encoded GET
state	URL encoded GET

Input scheme 2	
Input name	Input type
textInputValue	URL encoded POST

Input scheme 3	
Input name	Input type
next_url	URL encoded GET
source	URL encoded GET
uber_client_name	URL encoded GET

Input scheme 4	
Input name	Input type
Host	HTTP Header

URL: https://auth.uber.com/login/session

Vulnerabilities have been identified for this URL

58 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
addPassword	URL encoded POST
autoSMSVerificationSupported	URL encoded POST
countryCode	URL encoded POST
email	URL encoded POST
firstName	URL encoded POST
firstPartyClientID	URL encoded POST
inAuthSessionID	URL encoded POST
lastName	URL encoded POST
meta	URL encoded POST
nextURL	URL encoded POST
phoneNumber	URL encoded POST
promoCode	URL encoded POST
promotionValueString	URL encoded POST
sess	URL encoded POST
type	URL encoded POST
uberClientName	URL encoded POST
x-csrf-token	URL encoded POST

Input scheme 2	
Input name	Input type
textInputValue	URL encoded POST

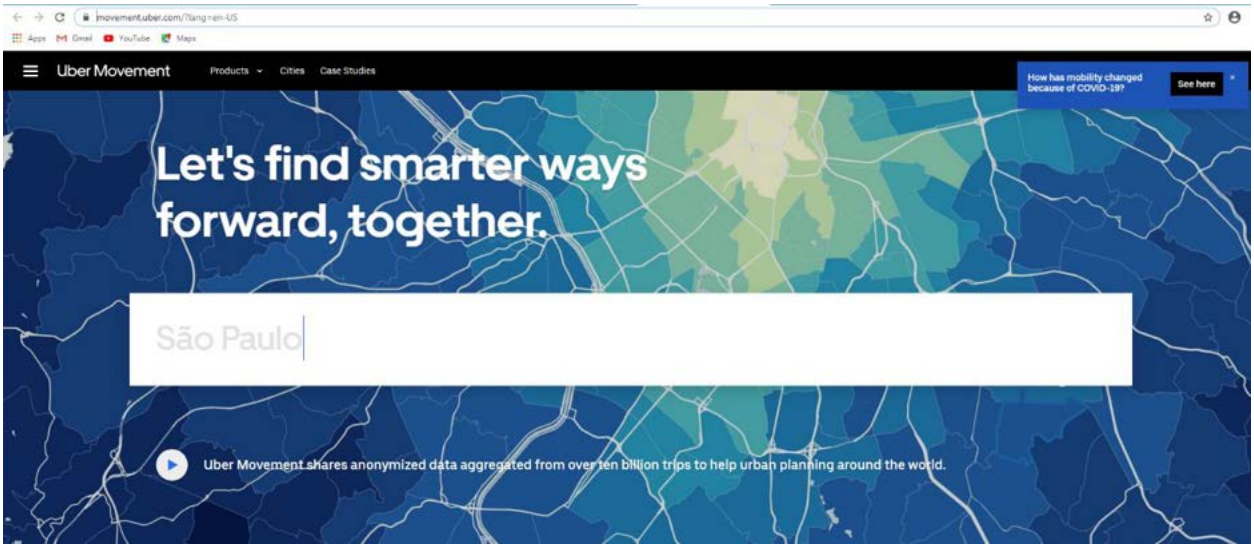
x-csrf-token	URL encoded POST

URL: https://auth.uber.com/login/udimeta
Vulnerabilities have been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
Acunetix Website Audit	16
meta	JSON

9. Target Domain: **https://movement.uber.com**



Scan details

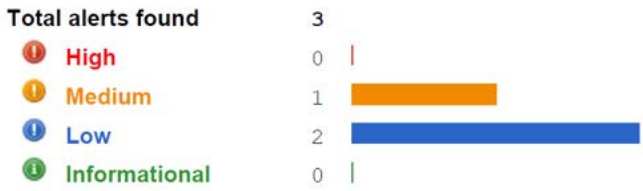
Scan information	
Start time	10/21/2020 8:56:20 AM
Finish time	10/21/2020 9:01:38 AM
Scan time	5 minutes, 17 seconds
Profile	Default
Server information	
Responsive	True
Server banner	ufe
Server OS	Unknown

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution



a) URL redirection

Severity:	**Medium**
Type:	Validation
Reported by module:	Scripting (Open_Redirect.script)
Classification:	CVSS Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial

	- Availability Impact: None
	CVSS3 Base Score: 0 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
	CWE-601

Description

This script is possibly vulnerable to URL redirection attacks.

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

Impact

A remote attacker can redirect users from your website to a specified URL. This problem may assist an attacker to conduct phishing attacks, Trojan distribution, spammers.

Recommendation

Your script should properly sanitize user input.

URL redirection

Severity	**Medium**
Type	Validation
Reported by module	Scripting (Open_Redirect.script)

Description

This script is possibly vulnerable to URL redirection attacks.

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

Impact

A remote attacker can redirect users from your website to a specified URL. This problem may assist an attacker to conduct phishing attacks, trojan distribution, spammers.

Recommendation

Your script should properly sanitize user input.

References

HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics
URL Redirection Security Vulnerability

Affected items

Web Server

Details

URI was set to //vulnweb.com.

Request headers

```
GET //vulnweb.com HTTP/1.1
Host: movement.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

b) Cookie without HttpOnly flag set

Severity:	**Low**
Type:	Informational
Reported by module:	Crawler
Classification:	CVSS: Base Score: 0.0 - Access Vector: Network

	- Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
	CWE-16

Description

This cookie does not have the secure flag set. When a cookie is set with the secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the secure flag for this cookie.

Cookie without HttpOnly flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.

Affected items

/

Details

Cookie name: "_ua"
Cookie domain: "movement.uber.com"

Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie:
_ua={"session_id":"30bd05ce-7d5b-4b84-856b-4c11d9b264e2","session_time_ms":1603295782035
}; cookieSession={"rateLimitingID":"fce3f120-5508-4853-87f9-ec5dff3f0b38"};
jwt-session=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2MDMyOTU3ODIsImV4cCI6MTYwMzM
4MjE4Mn0.YArY08cCwNtIN_V2wmbduvF86nyp6UnbntyX0un6mWQ
Host: movement.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

c) OPTIONS method is enabled

Severity:	**Low**
Type:	Validation
Reported by module:	Scripting (Options_Server_Method.script)
Classification:	CVSS: Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
	CVSS3 Base Score: 7.5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
	CWE-200

Description

HTTP OPTIONS method is enabled on this webserver. The OPTIONS method provides a list of the methods that are supported by the webserver, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI.

Impact

The OPTIONS method may expose sensitive information that may help a malicious user to prepare more advanced attacks.

Recommendation

It's recommended to disable OPTIONS Method on the webserver.

OPTIONS method is enabled

Severity	**Low**
Type	Validation
Reported by module	Scripting (Options_Server_Method.script)

Description

HTTP OPTIONS method is enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI.

Impact

The OPTIONS method may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

It's recommended to disable OPTIONS Method on the web server.

References

Testing for HTTP Methods and XST (OWASP-CM-008)

Affected items

Web Server

Details

Methods allowed: GET,HEAD

Request headers

```
OPTIONS / HTTP/1.1
Host: movement.uber.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

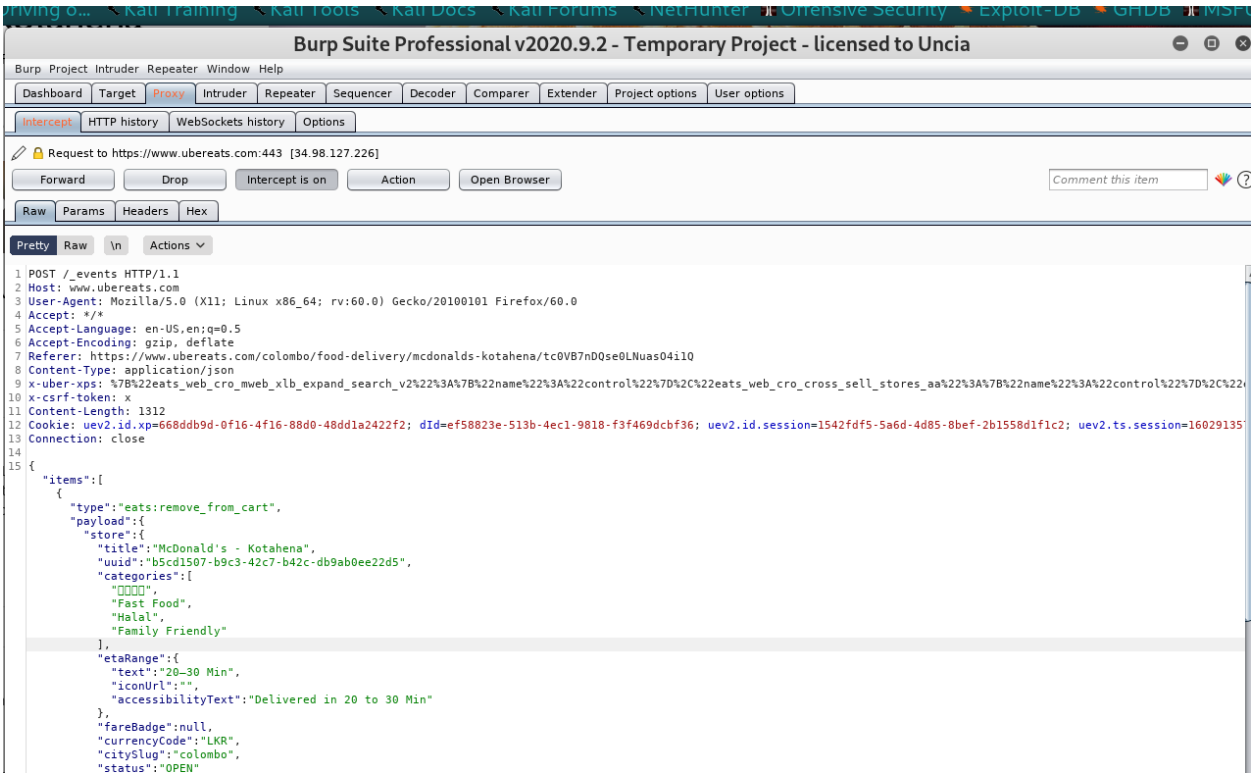
https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_(OWASP-CM-008)

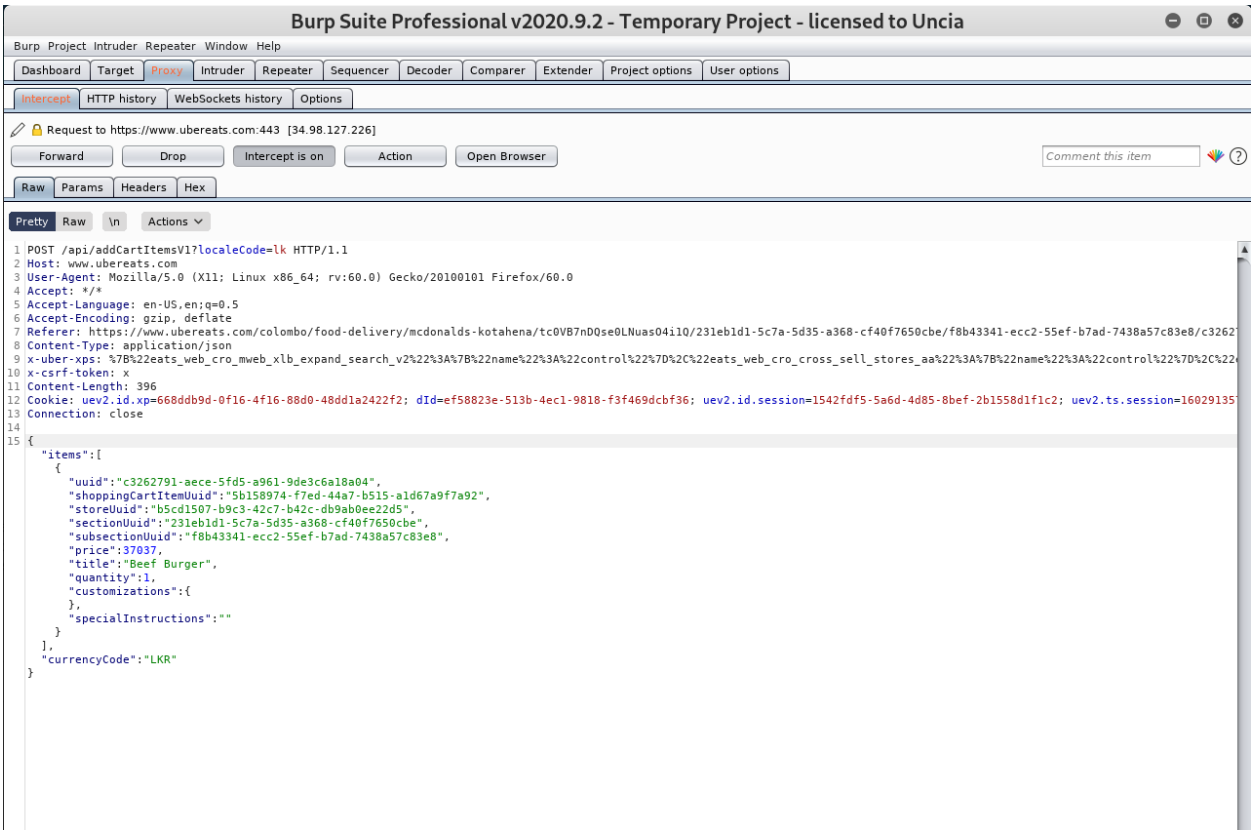
- For scanning below domains is used **Burp suite Professional** Vulnerability Scanner
-

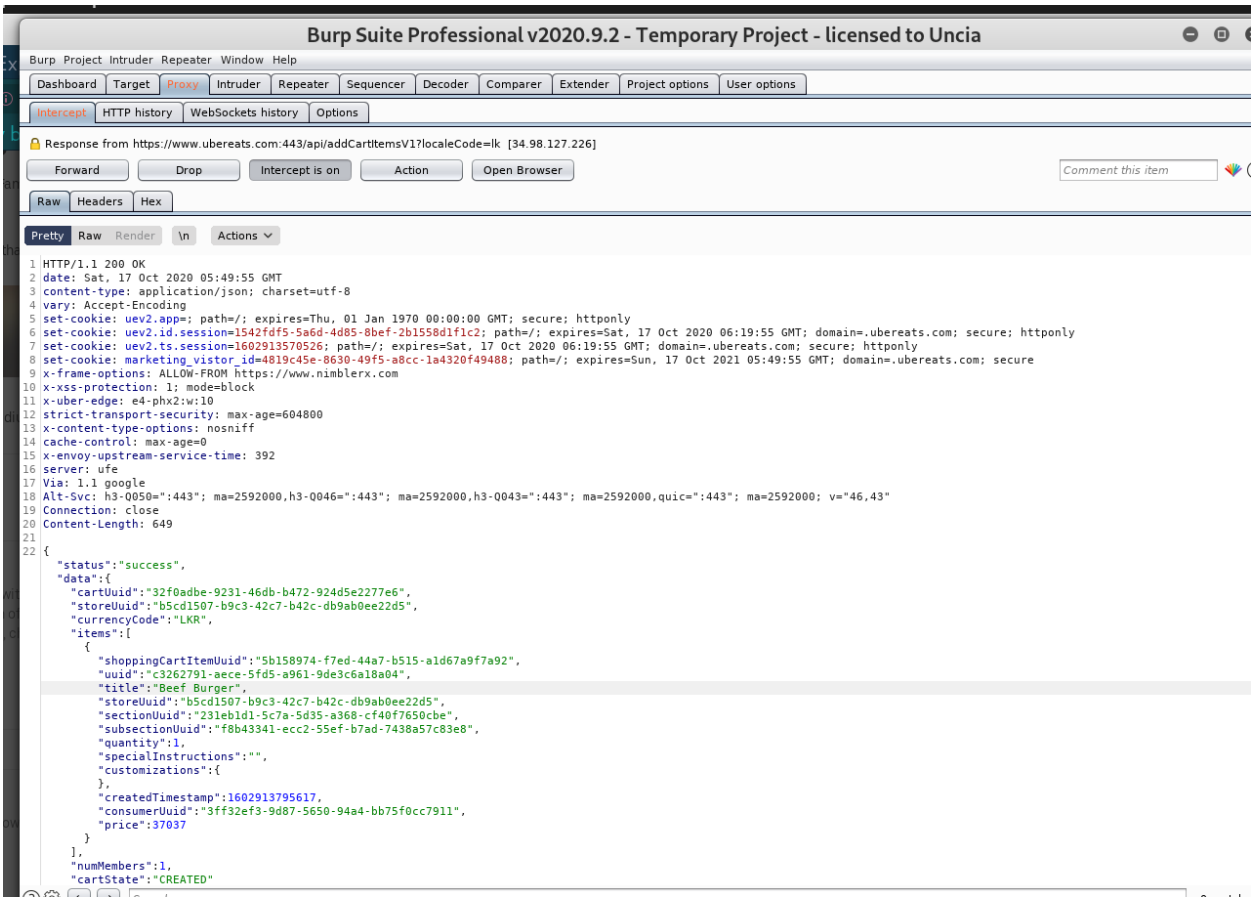
10. Target Domain - **https://www.ubereats.com/lk**

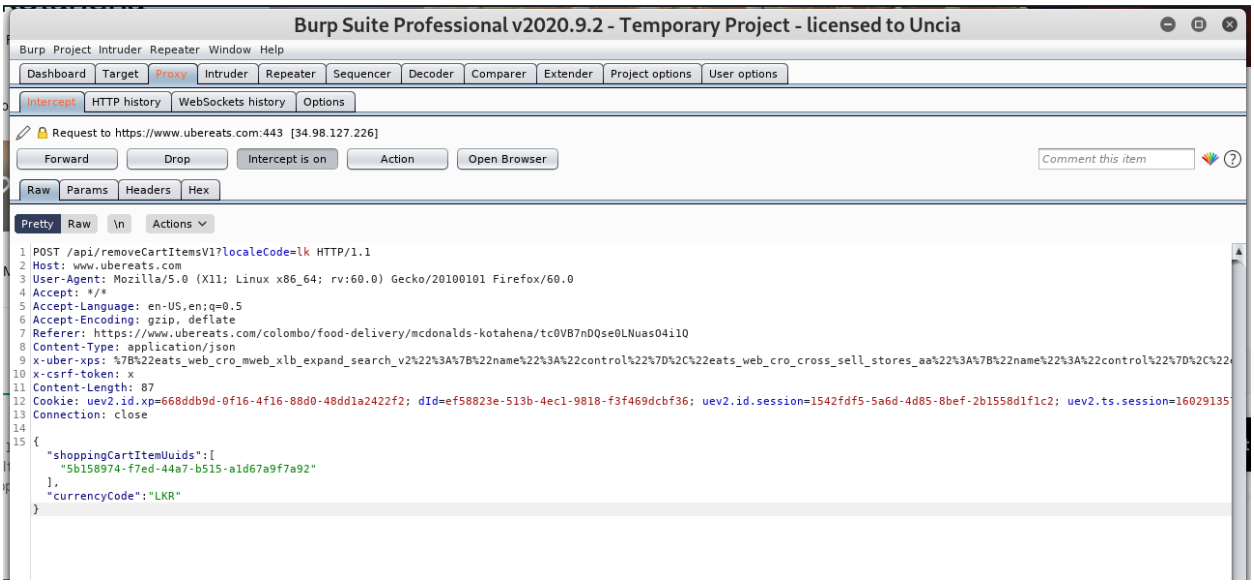
- Test Case: Adding Items to the cart as non-authenticated user

Send the web request through the burp suite and get the response. I have added one item and remove that item from the cart.




Burp Suite Professional v2020.9.2 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to https://www.ubereats.com:443 [34.98.127.226]
Forward Drop Intercept is on Action Open Browser
Comment this item
Raw Params Headers Hex
Pretty Raw \n Actions
POST /api/addCartItemsV1?localeCode=lk HTTP/1.1
Host: www.ubereats.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.ubereats.com/colombo/food-delivery/mcdonalds-kotahena/tc0VB7nDQse0LNuasO4ilQ/231eb1d1-5c7a-5d35-a368-cf40f7650cbe/f8b43341-ecc2-55ef-b7ad-7438a57c83e8/c3262
Content-Type: application/json
x-uber-xps: %7B%22eats_web_cro_mweb_xlb_expand_search_v2%22%3A%7B%22name%22%3A%22control%22%7D%2C%22eats_web_cro_cross_sell_stores_aa%22%3A%7B%22name%22%3A%22control%22%7D%2C%22
x-csrf-token: x
Content-Length: 396
Cookie: uev2.id.xp=668ddb9d-0f16-4f16-88d0-48dd1a2422f2; dId=ef58823e-513b-4ec1-9818-f3f469dcbf36; uev2.id.session=1542fdf5-5a6d-4d85-8bef-2b1558d1f1c2; uev2.ts.session=16029135
Connection: close
{
"items":[
{
"uuid":"c3262791-aece-5fd5-a961-9de3c6a18a04",
"shoppingCartItemUuid":"5b158974-f7ed-44a7-b515-a1d67a9f7a92",
"storeUuid":"b5cd1507-b9c3-42c7-b42c-db9ab0ee22d5",
"sectionUuid":"231eb1d1-5c7a-5d35-a368-cf40f7650cbe",
"subsectionUuid":"f8b43341-ecc2-55ef-b7ad-7438a57c83e8",
"price":37037,
"title":"Beef Burger",
"quantity":1,
"customizations":{
},
"specialInstructions":""
}
],
"currencyCode":"LKR"
}


Burp Suite Professional v2020.9.2 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Response from https://www.ubereats.com:443/api/addCartItemsV1?localeCode=lk [34.98.127.226]
Forward Drop Intercept is on Action Open Browser
Comment this item
Raw Headers Hex
Pretty Raw Render \n Actions
HTTP/1.1 200 OK
date: Sat, 17 Oct 2020 05:49:55 GMT
content-type: application/json; charset=utf-8
vary: Accept-Encoding
set-cookie: uev2.app=; path=/; expires=Thu, 01 Jan 1970 00:00:00 GMT; secure; httponly
set-cookie: uev2.id.session=1542fdf5-5a6d-4d85-8bef-2b1558d1f1c2; path=/; expires=Sat, 17 Oct 2020 06:19:55 GMT; domain=.ubereats.com; secure; httponly
set-cookie: uev2.ts.session=1602913570526; path=/; expires=Sat, 17 Oct 2020 06:19:55 GMT; domain=.ubereats.com; secure; httponly
set-cookie: marketing_vistor_id=4819c45e-8630-49f5-a8cc-1a4320f49488; path=/; expires=Sun, 17 Oct 2021 05:49:55 GMT; domain=.ubereats.com; secure
x-frame-options: ALLOW-FROM https://www.nimblerx.com
x-xss-protection: 1; mode=block
x-uber-edge: e4-phx2:w:10
strict-transport-security: max-age=604800
x-content-type-options: nosniff
cache-control: max-age=0
x-envoy-upstream-service-time: 392
server: ufe
Via: 1.1 google
Alt-Svc: h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"
Connection: close
Content-Length: 649
{
"status":"success",
"data":{
"cartUuid":"32f0adbe-9231-46db-b472-924d5e2277e6",
"storeUuid":"b5cd1507-b9c3-42c7-b42c-db9ab0ee22d5",
"currencyCode":"LKR",
"items":[
{
"shoppingCartItemUuid":"5b158974-f7ed-44a7-b515-a1d67a9f7a92",
"uuid":"c3262791-aece-5fd5-a961-9de3c6a18a04",
"title":"Beef Burger",
"storeUuid":"b5cd1507-b9c3-42c7-b42c-db9ab0ee22d5",
"sectionUuid":"231eb1d1-5c7a-5d35-a368-cf40f7650cbe",
"subsectionUuid":"f8b43341-ecc2-55ef-b7ad-7438a57c83e8",
"quantity":1,
"specialInstructions":"",
"customizations":{
},
"createdTimestamp":1602913795617,
"consumerUuid":"3ff32ef3-9d87-5650-94a4-bb75f0cc7911",
"price":37037
}
],
"numMembers":1,
"cartState":"CREATED"


Burp Suite Professional v2020.9.2 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to https://www.ubereats.com:443 [34.98.127.226]
Forward Drop Intercept is on Action Open Browser
Comment this item
Raw Params Headers Hex
Pretty Raw \n Actions
POST /api/removeCartItemsV1?localeCode=lk HTTP/1.1
Host: www.ubereats.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.ubereats.com/colombo/food-delivery/mcdonalds-kotahena/tc0VB7nDQse0LNuasO4i1Q
Content-Type: application/json
x-uber-xps: %7B%22eats_web_cro_mweb_xlb_expand_search_v2%22%3A%7B%22name%22%3A%22control%22%7D%2C%22eats_web_cro_cross_sell_stores_aa%22%3A%7B%22name%22%3A%22control%22%7D%2C%22
x-csrf-token: x
Content-Length: 87
Cookie: uev2.id.xp=668ddb9d-0f16-4f16-88d0-48dd1a2422f2; dId=ef58823e-513b-4ec1-9818-f3f469dcbf36; uev2.id.session=1542fdf5-5a6d-4d85-8bef-2b1558d1f1c2; uev2.ts.session=16029135
Connection: close
{
"shoppingCartItemUuids":[
"5b158974-f7ed-44a7-b515-a1d67a9f7a92"
],
"currencyCode":"LKR"
}

a) Cacheable HTTP response

Issue	Cacheable HTTP response
Severity	Information
Confidence	Certain
Host	https://www.ubereats.com
Path	/api/addCartItemsV1

Description:

Applications may use caches to improve efficiency when communicating with remote entities or performing intensive calculations. A cache maintains a pool of objects, threads, connections, pages, financial data, passwords, or other resources to minimize the time it takes to initialize and access these resources. If the cache is accessible to unauthorized actors, attackers can read the cache and obtain this sensitive information.

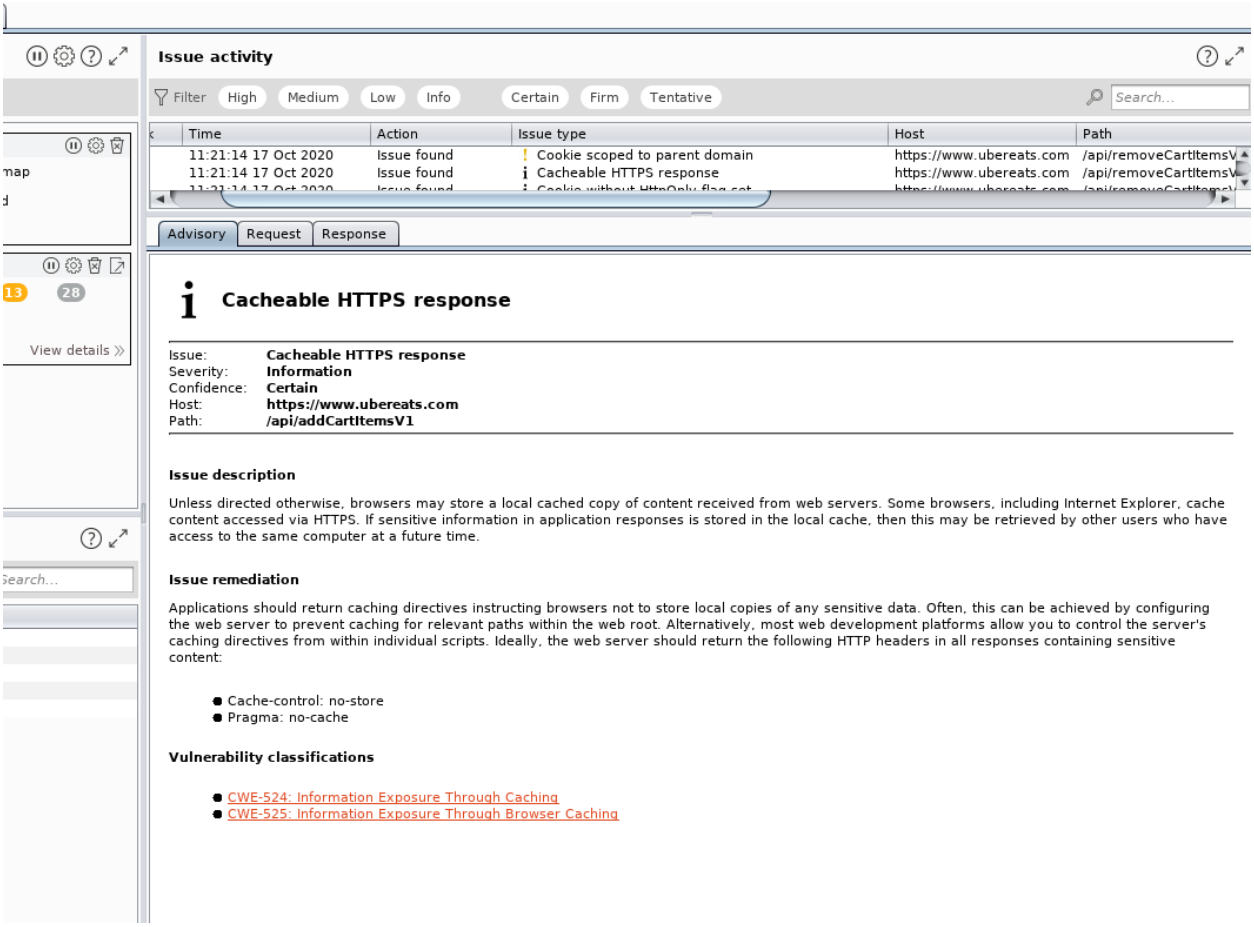
Vulnerability classifications:

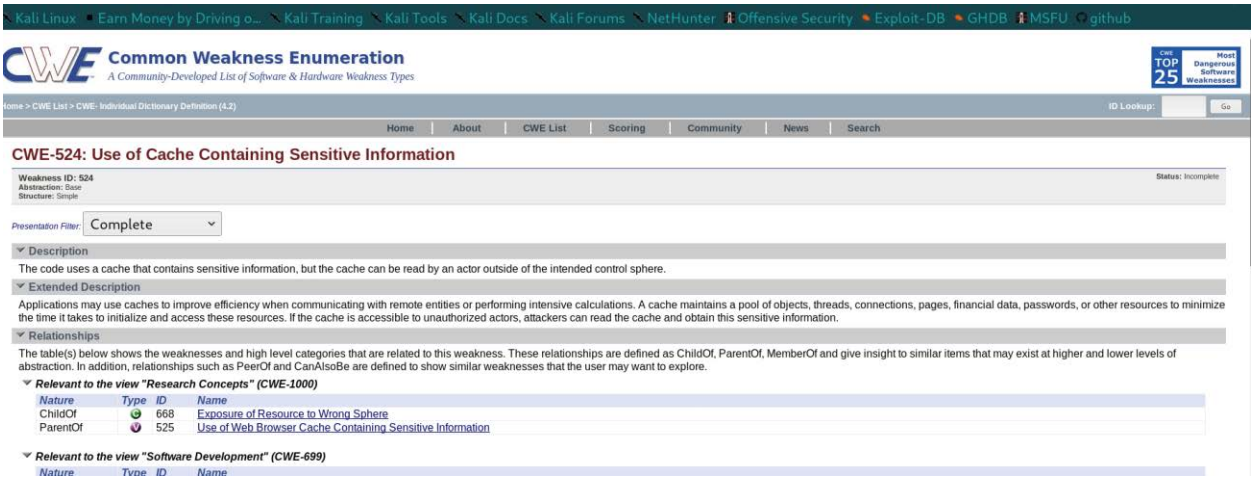
- CWE-524: Information Exposure Through Caching
- CWE-525: Information Exposure Through Browser Caching

Remediation: Cacheable HTTPS response

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the webserver to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the webserver should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache


Issue activity
Filter
High
Medium
Low
Info
Certain
Firm
Tentative
Search...
Time
Action
Issue type
Host
Path
11:21:14 17 Oct 2020
Issue found
Cookie scoped to parent domain
https://www.ubereats.com
/api/removeCartItemsV
11:21:14 17 Oct 2020
Issue found
Cacheable HTTPS response
https://www.ubereats.com
/api/removeCartItemsV
Advisory
Request
Response
Cacheable HTTPS response
Issue: Cacheable HTTPS response
Severity: Information
Confidence: Certain
Host: https://www.ubereats.com
Path: /api/addCartItemsV1
Issue description
Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.
Issue remediation
Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:
Cache-control: no-store
Pragma: no-cache
Vulnerability classifications
CWE-524: Information Exposure Through Caching
CWE-525: Information Exposure Through Browser Caching


Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
github
Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types
Home
About
CWE List
Scoring
Community
News
Search
CWE-524: Use of Cache Containing Sensitive Information
Weakness ID: 524
Abstraction: Base
Structure: Simple
Status: Incomplete
Presentation Filter: Complete
Description
The code uses a cache that contains sensitive information, but the cache can be read by an actor outside of the intended control sphere.
Extended Description
Applications may use caches to improve efficiency when communicating with remote entities or performing intensive calculations. A cache maintains a pool of objects, threads, connections, pages, financial data, passwords, or other resources to minimize the time it takes to initialize and access these resources. If the cache is accessible to unauthorized actors, attackers can read the cache and obtain this sensitive information.
Relationships
The table(s) below shows the weaknesses and high level categories that are related to this weakness. These relationships are defined as ChildOf, ParentOf, MemberOf and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as PeerOf and CanAlsoBe are defined to show similar weaknesses that the user may want to explore.
Relevant to the view "Research Concepts" (CWE-1000)
Nature Type ID Name
ChildOf 668 Exposure of Resource to Wrong Sphere
ParentOf 525 Use of Web Browser Cache Containing Sensitive Information
Relevant to the view "Software Development" (CWE-699)

b) Cookie without HttpOnly flag set

Issue	Cookie without HttpOnly flag set
Severity	LOW
Confidence	Certain
Host	https://www.ubereats.com
Path	/_events

Description:

If the HttpOnly attribute is set on a cookie, then the cookies' value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting. Slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

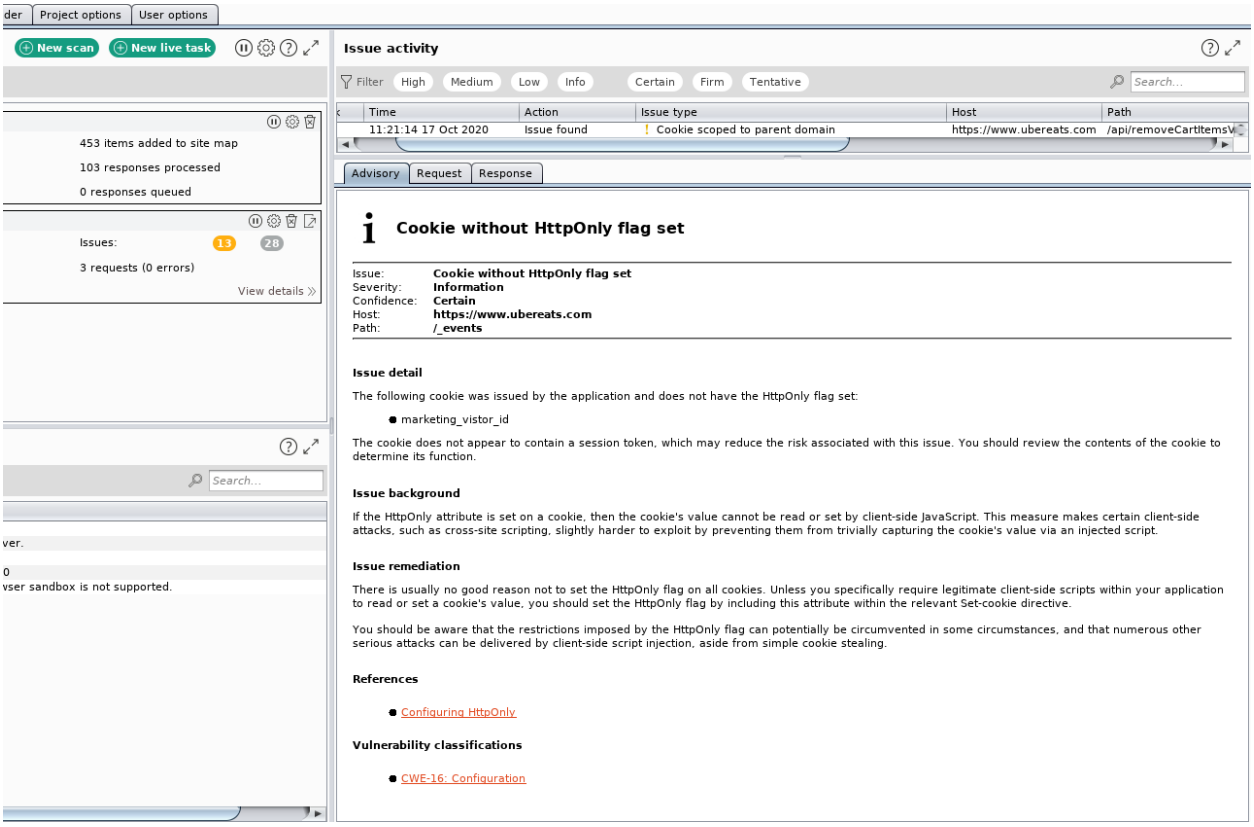
Vulnerability classifications:

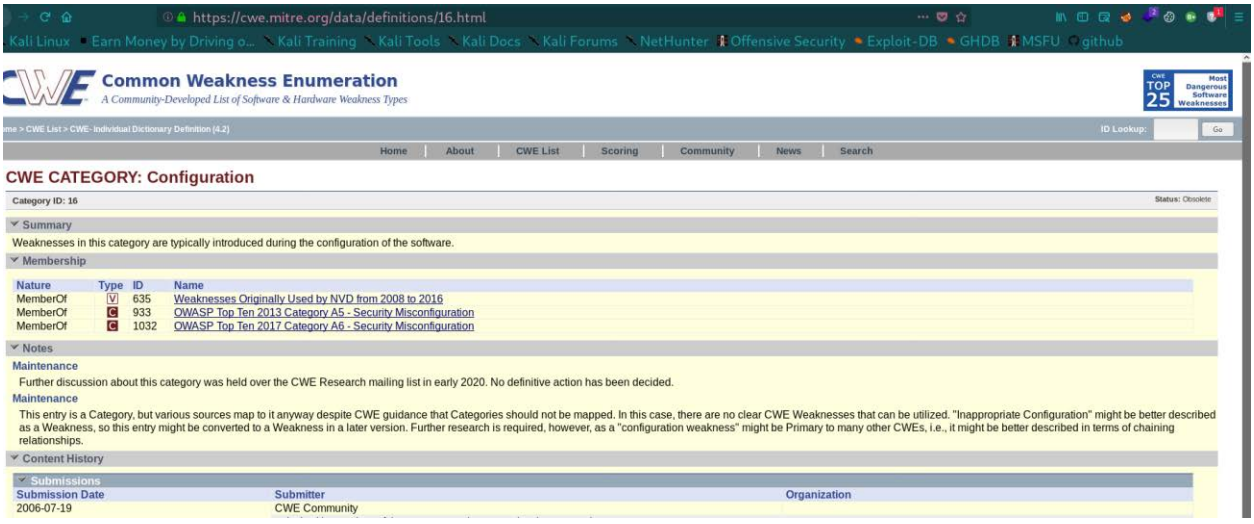
- CWE-16-Configuration

Remediation: Cookie without HttpOnly flag set

There is usually no good reason not to set the HttpOnly flag on all cookies. Unless you specifically require legitimate client-side scripts within your application to read or set a cookie's value, you should set the HttpOnly flag by including this attribute within the relevant Set-cookie directive.

You should be aware that the restrictions imposed by the HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.

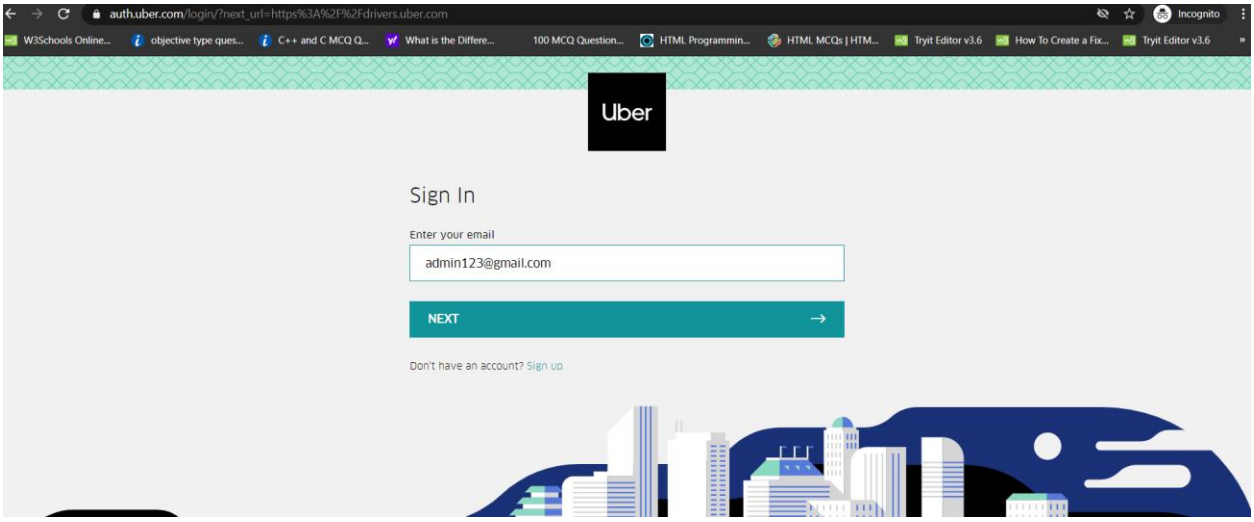

der
Project options
User options
New scan
New live task
453 items added to site map
103 responses processed
0 responses queued
Issues:
13
28
3 requests (0 errors)
View details
Search...
ver.
0
vser sandbox is not supported.
Issue activity
Filter
High
Medium
Low
Info
Certain
Firm
Tentative
Search...
Time
Action
Issue type
Host
Path
11:21:14 17 Oct 2020
Issue found
Cookie scoped to parent domain
https://www.ubereats.com
/api/removeCartItemsV
Advisory
Request
Response
Cookie without HttpOnly flag set
Issue: Cookie without HttpOnly flag set
Severity: Information
Confidence: Certain
Host: https://www.ubereats.com
Path: /_events
Issue detail
The following cookie was issued by the application and does not have the HttpOnly flag set:
marketing_vistor_id
The cookie does not appear to contain a session token, which may reduce the risk associated with this issue. You should review the contents of the cookie to determine its function.
Issue background
If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.
Issue remediation
There is usually no good reason not to set the HttpOnly flag on all cookies. Unless you specifically require legitimate client-side scripts within your application to read or set a cookie's value, you should set the HttpOnly flag by including this attribute within the relevant Set-cookie directive.
You should be aware that the restrictions imposed by the HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.
References
Configuring HttpOnly
Vulnerability classifications
CWE-16: Configuration


https://cwe.mitre.org/data/definitions/16.html
Kali Linux
Earn Money by Driving o...
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
github
Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types
TOP 25
Most Dangerous Software Weaknesses
ID Lookup:
Go
Home
About
CWE List
Scoring
Community
News
Search
CWE CATEGORY: Configuration
Category ID: 16
Status: Obsolete
Summary
Weaknesses in this category are typically introduced during the configuration of the software.
Membership
Nature
Type
ID
Name
MemberOf
V
635
Weaknesses Originally Used by NVD from 2008 to 2016
MemberOf
C
933
OWASP Top Ten 2013 Category A5 - Security Misconfiguration
MemberOf
C
1032
OWASP Top Ten 2017 Category A6 - Security Misconfiguration
Notes
Maintenance
Further discussion about this category was held over the CWE Research mailing list in early 2020. No definitive action has been decided.
Maintenance
This entry is a Category, but various sources map to it anyway despite CWE guidance that Categories should not be mapped. In this case, there are no clear CWE Weaknesses that can be utilized. "Inappropriate Configuration" might be better described as a Weakness, so this entry might be converted to a Weakness in a later version. Further research is required, however, as a "configuration weakness" might be Primary to many other CWEs, i.e., it might be better described in terms of chaining relationships.
Content History
Submissions
Submission Date
Submitter
Organization
2006-07-19
CWE Community

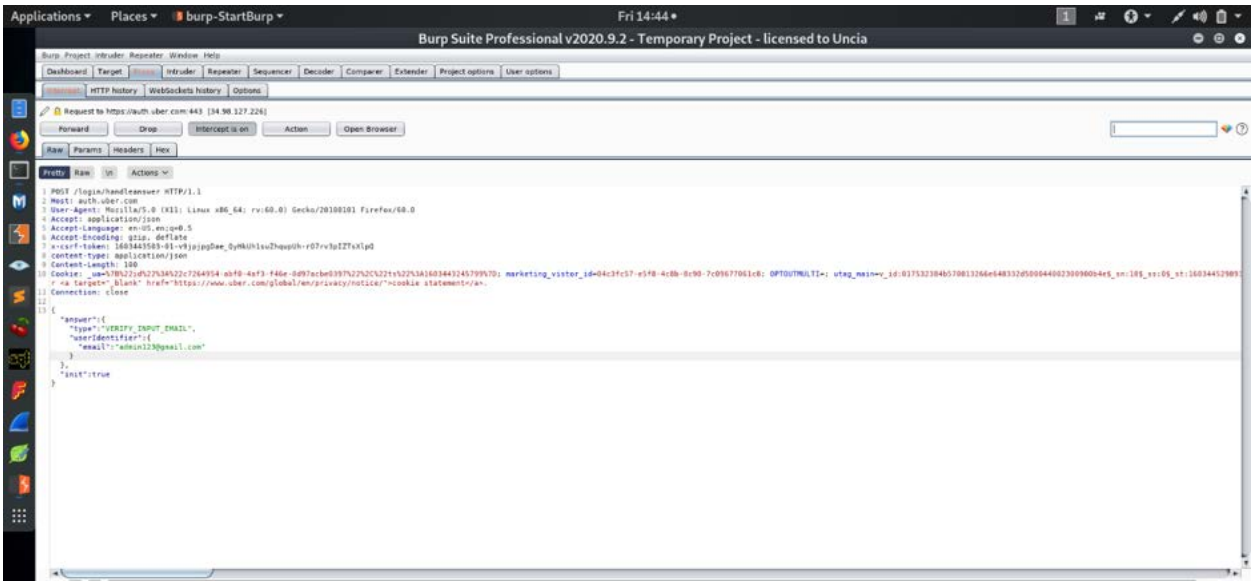
11. Target Domain– **https://www.uber.com**

Checking the target is vulnerable for Brute Force attack

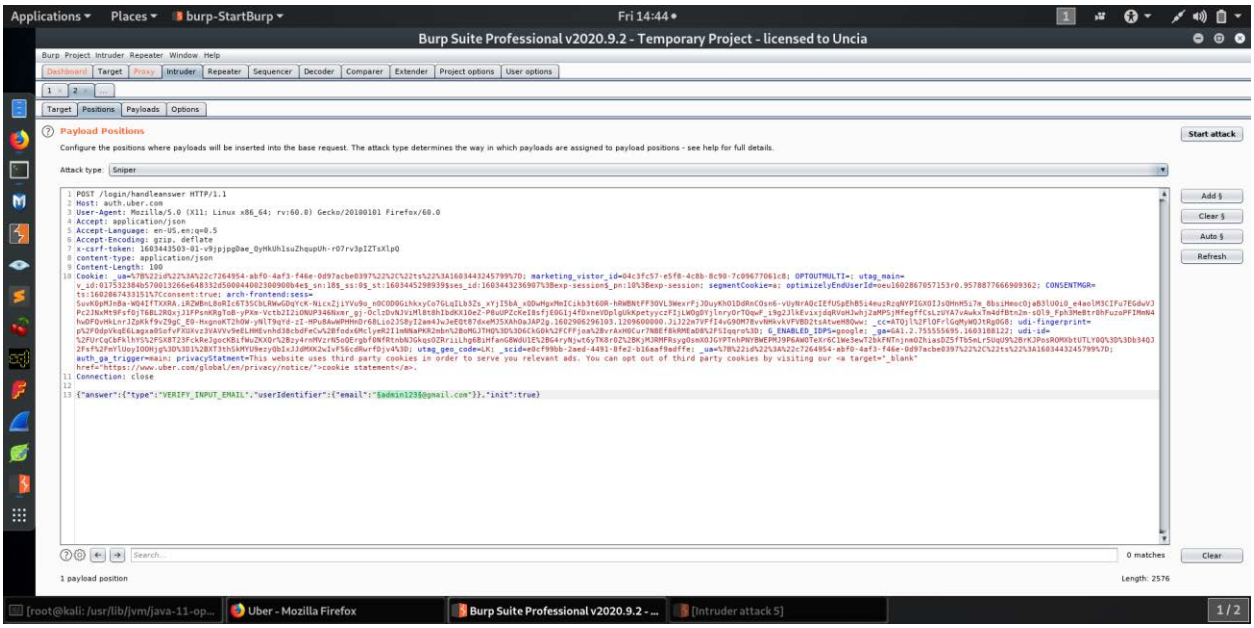
First I tried to log in as a Drive of the target domain by given a test email address for the sign-in.



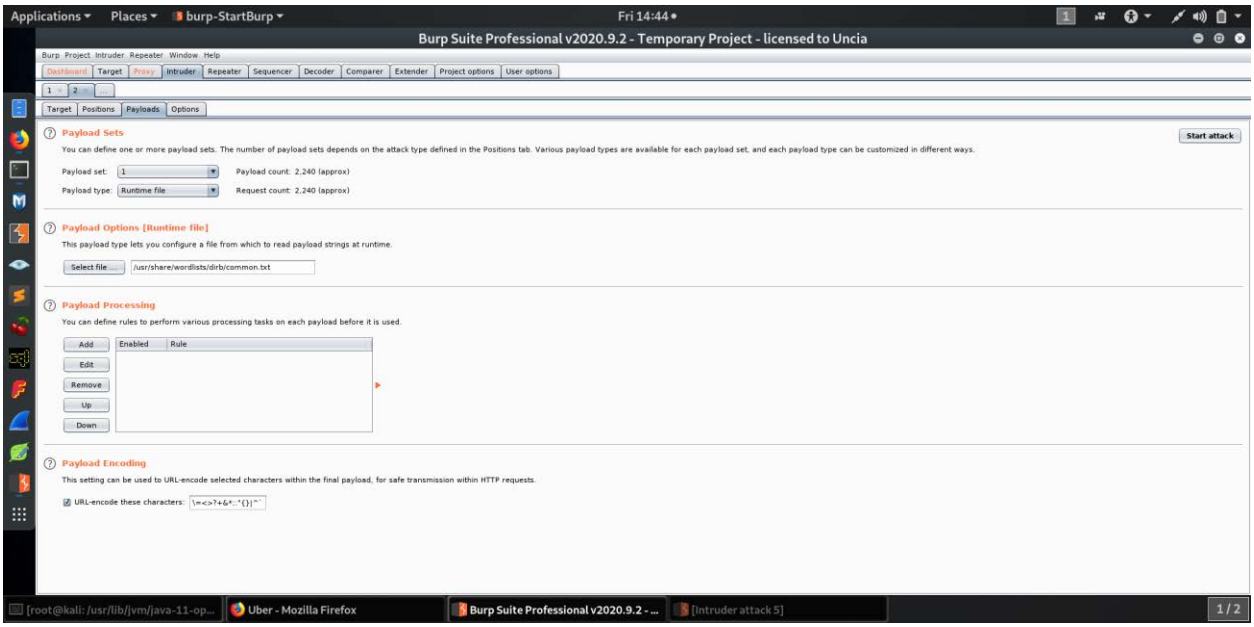
Then I send the capture the web request by the intercepting proxy.

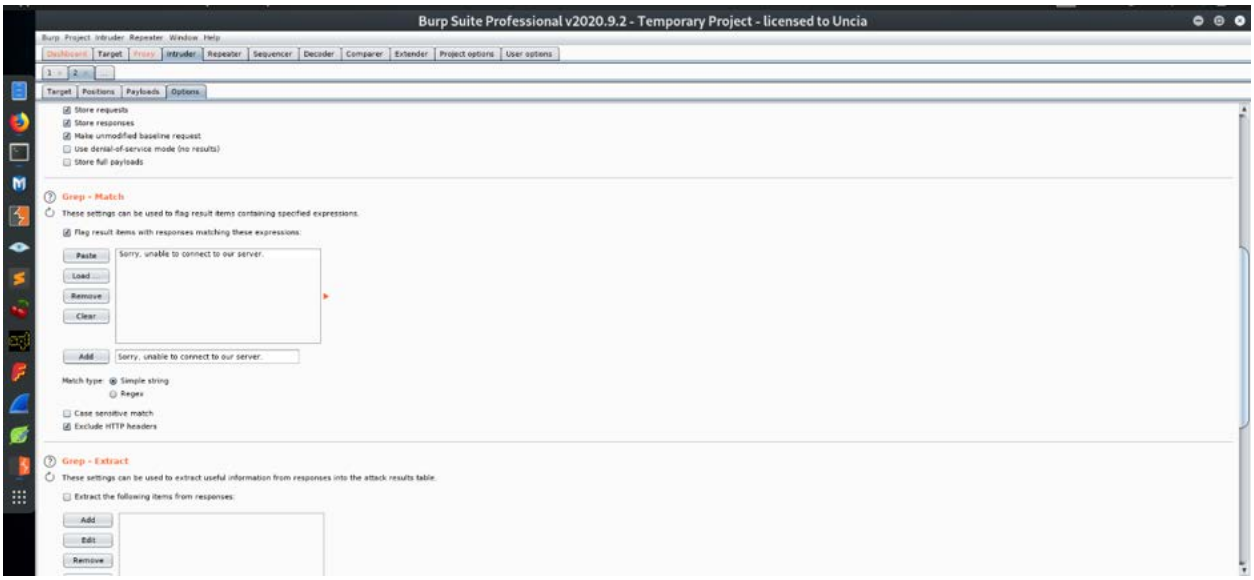


Then I sent the web request to the intruder. After Adding my payload I cleared the default payload and set the payload to the email. Since I only use 1 payload I choose the attack type as **a sniper** attack.

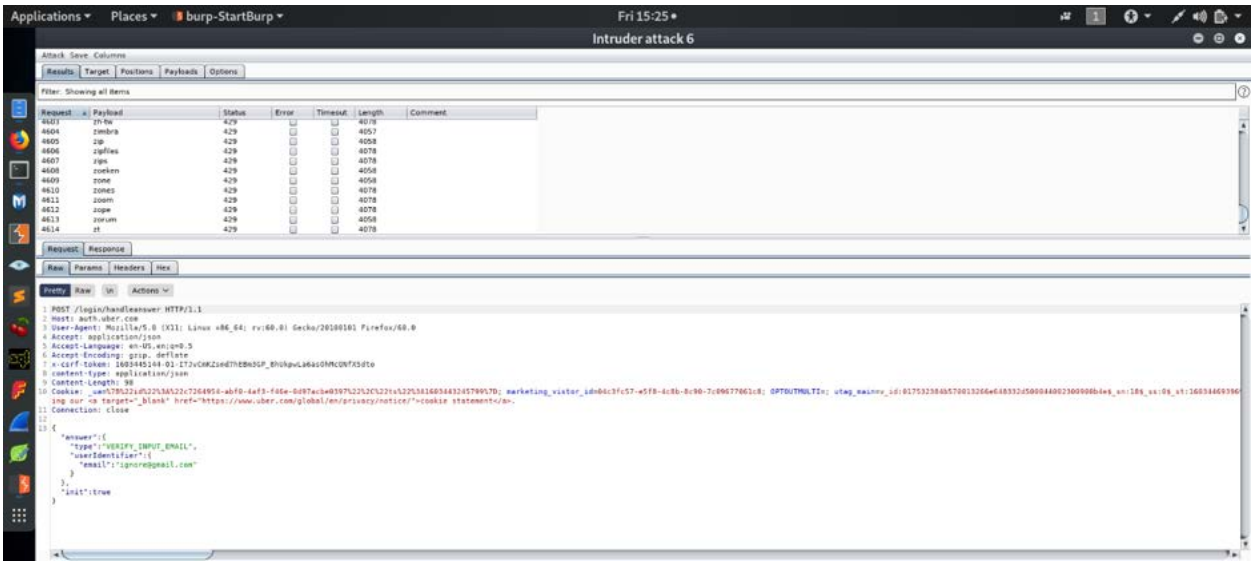


I selected the payload sets as 1 and selected the payload type as **Run-time.** And I have given the **common.txt** as the wordlist file.





Then I start the attack. If the correct email is matching then it gives the status in 200 and different length than other.

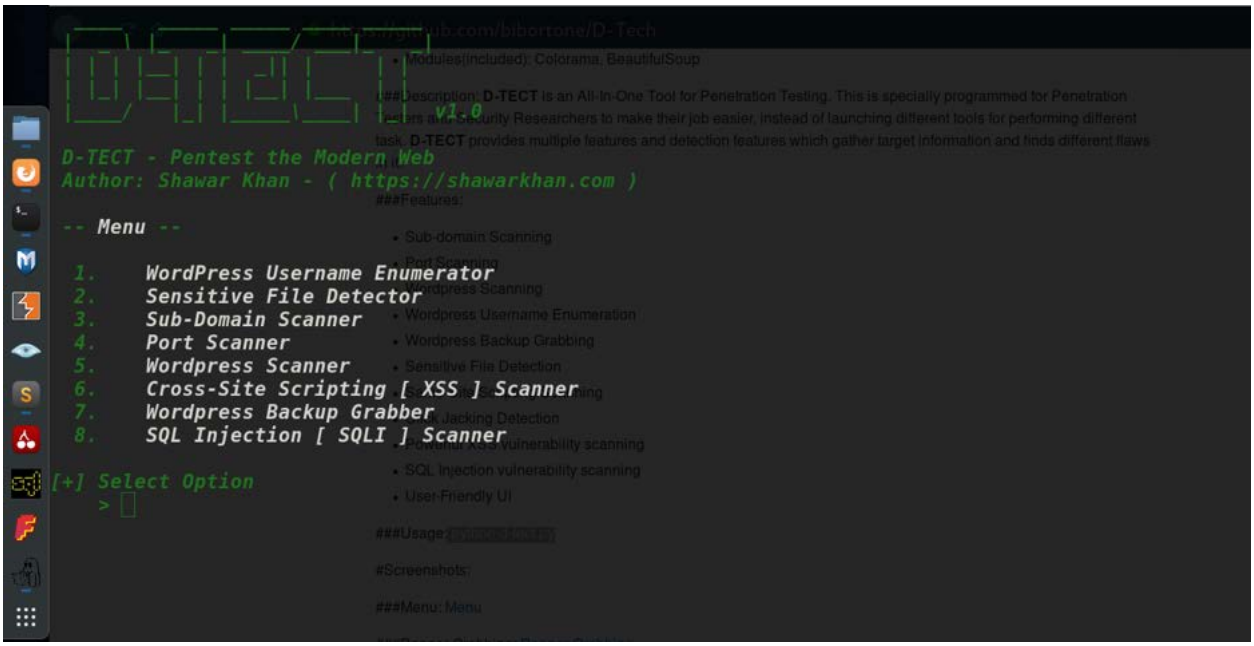


Although I tried, I cannot get any active status results.

Vulnerability Status:

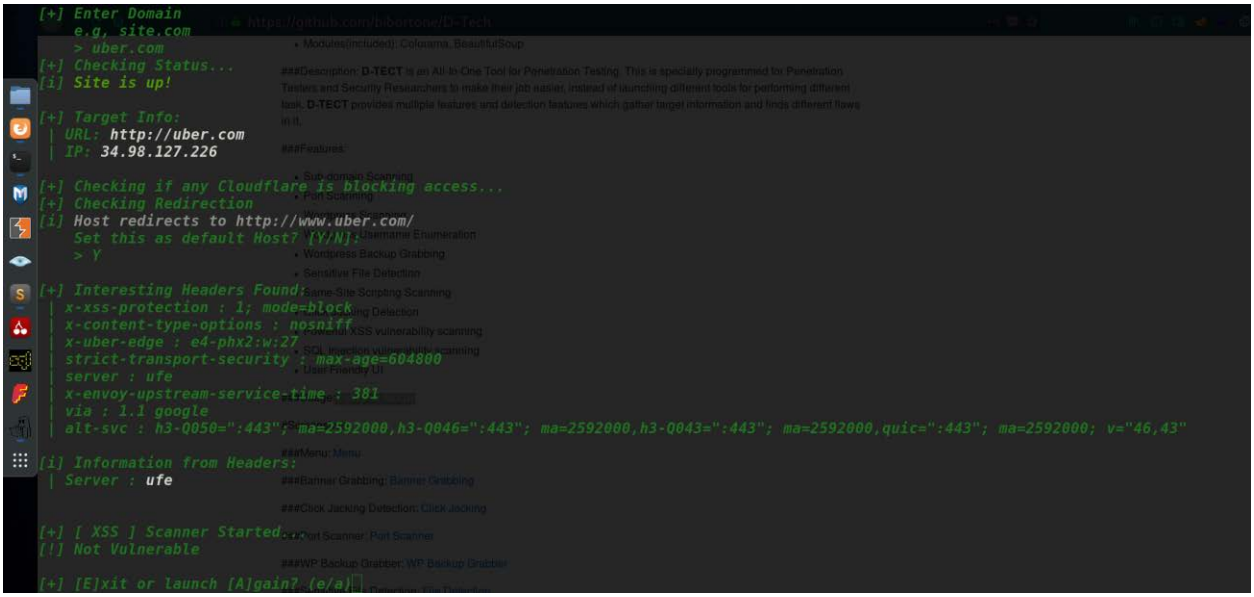
- **Not vulnerable**

- Vulnerability Scanner Tool – D-Tech Tool
- D-Tech is an automated vulnerability scanning tool, which we can use to scan and identified various web application vulnerabilities.
- Github Link: https://github.com/bibortone/D-Tech
- Features of D-Tech Tool
- Below Domain are scanned by the D-Tech tool
    - Sub-domain Scanning
    - Port Scanning
    - Wordpress Scanning
    - Wordpress Username Enumeration
    - Wordpress Backup Grabbing
    - Sensitive File Detection
    - Same-Site Scripting Scanning
    - Click Jacking Detection
    - Powerful XSS vulnerability scanning
    - SQL Injection vulnerability scanning



12. Target Domain: **www.uber.com**

Run XSS Vulnerability with DTech

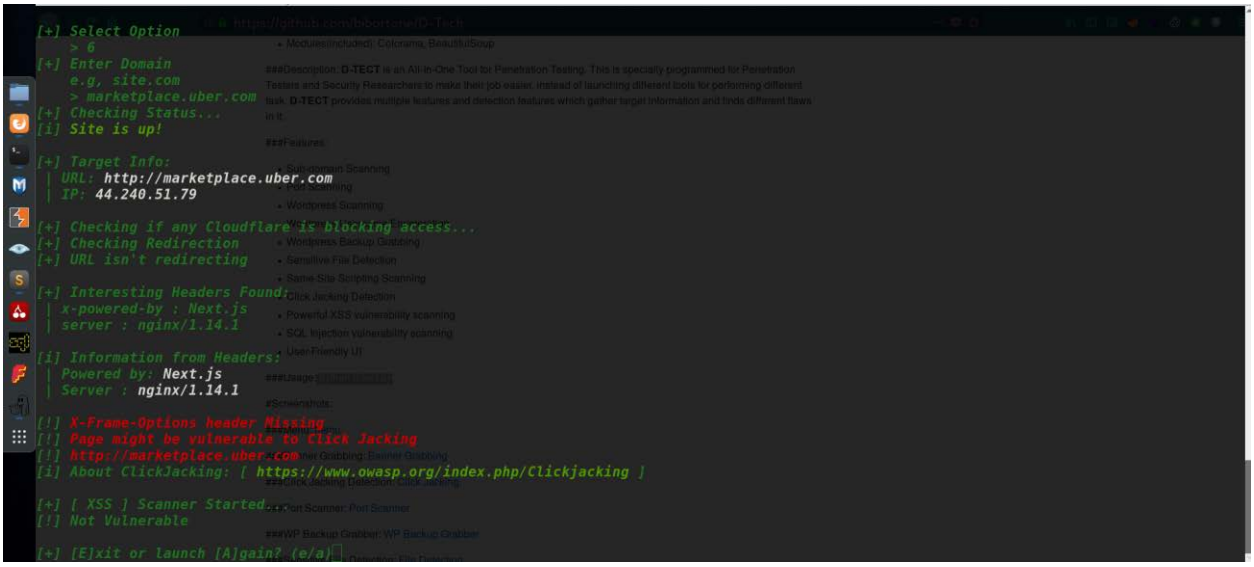


Vulnerability Status:

- **Not Vulnerable**

13. Target Domain: **www.marketplace.uber.com**

Run XSS Vulnerability with DTech



Vulnerability Status:

a) **X-Frame-options header Missing**
b) **The page is vulnerable to click Jacking**

Impact:

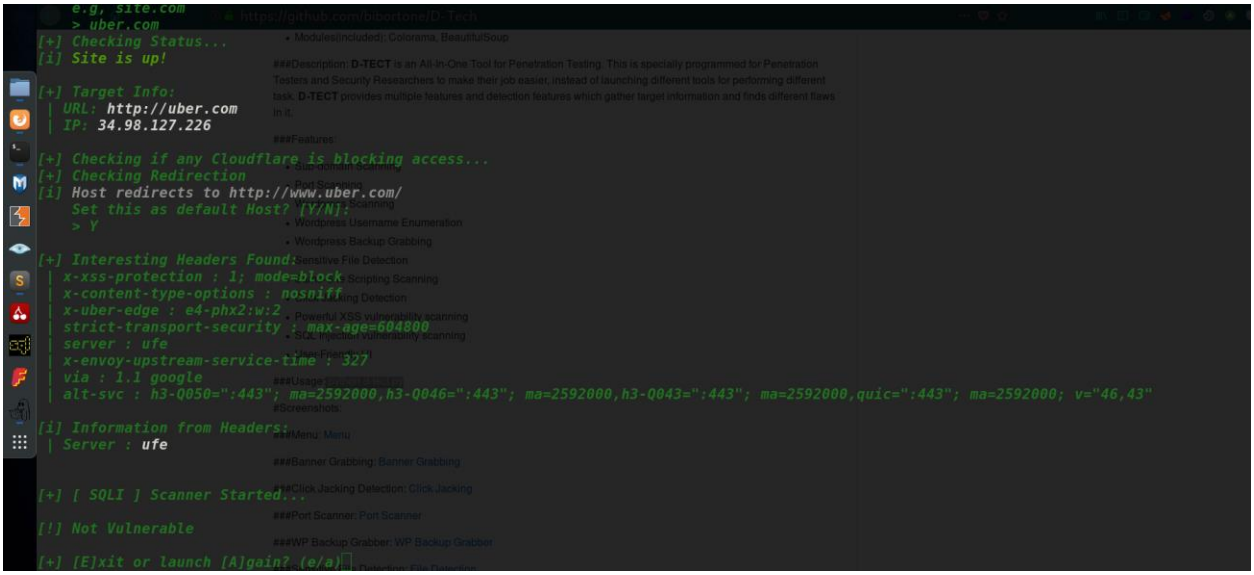
Clickjacking is an attack that tricks a user into clicking a webpage element that is invisible or disguised as another element. Most of the time, click-jacking involve mirroring usernames and passwords.

Remediation:

Configure your webserver to include an X-Frame-Options header and a CSP header with the frame-ancestors directive. Consult Web references for more information about the possible values for this header.

14. Target Domain: **www.uber.com**

Run SQL Injection with DTech

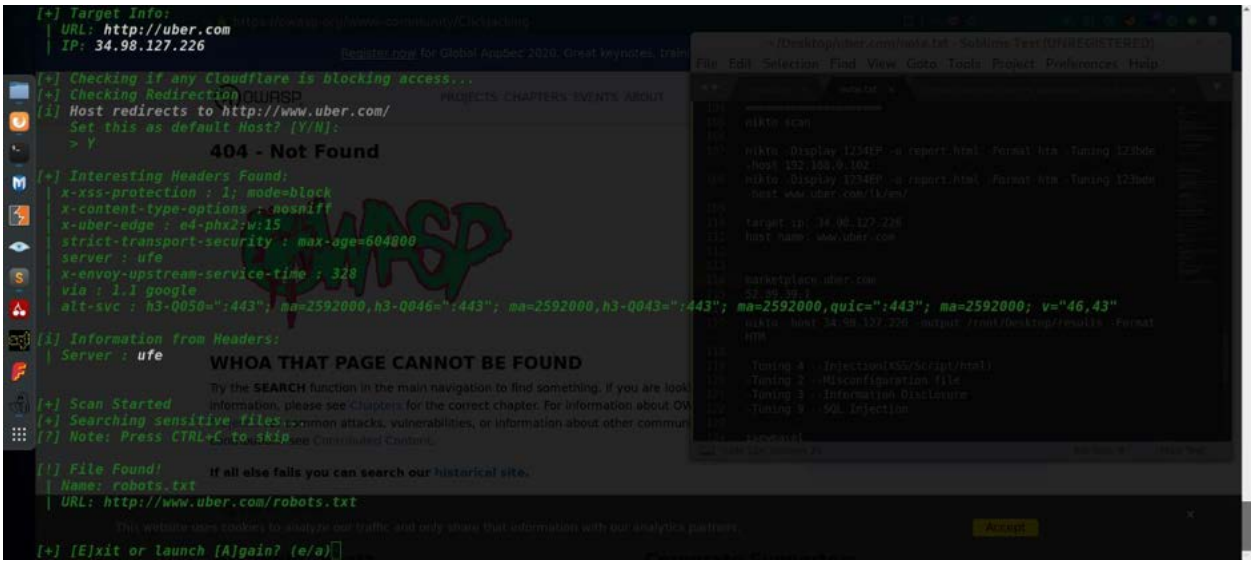


Vulnerability Status:

- **Not Vulnerable.**

15. Target Domain: **www.uber.com**

Run Sensitive File detector Scan



Vulnerability Status:

a) **Find robots.txt file**

- Vulnerability Scanner Tool – **Nikto**
- **Usage:** nikto -host 34.98.127.226 -output /root/Desktop/results -Format HTM

16. Target Domain: **www.uber.com (34.98.127.226)**

Identified Vulnerabilities:

a) **Anti-clickjacking X-Frame-options header is not present**

b) **X-XSS-Protection header is not set.**

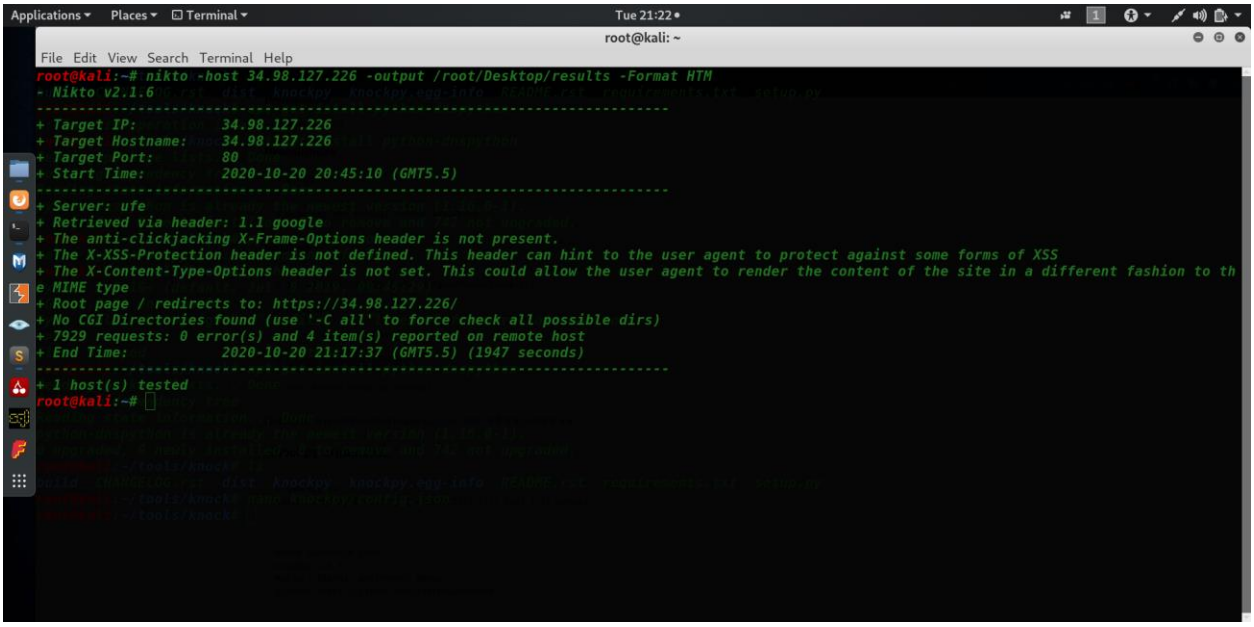
a) **Anti-clickjacking X-Frame-options header is not present**

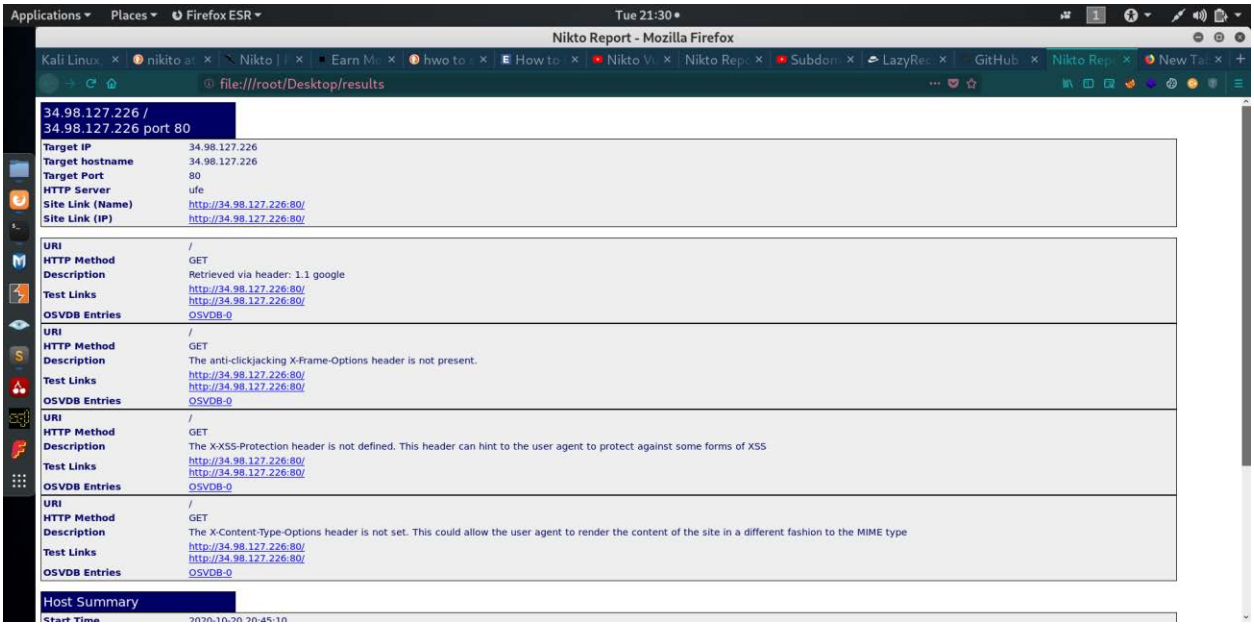
Severity	LOW
Classification	CWE-693 CWE 693 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N
Description	Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.
Remediation	Configure your webserver to include an X-Frame-Options header and a CSP header with the frame-ancestors directive. Consult Web references for more information about the possible values for this header.

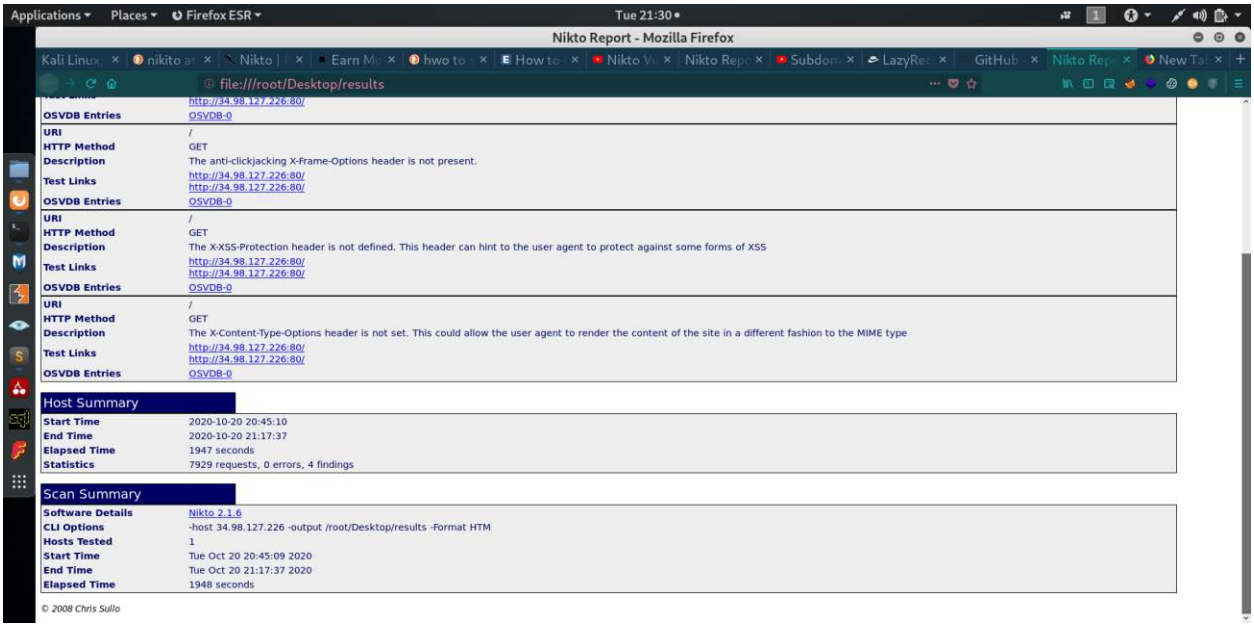
b) X-XSS-Protection header is not set

Severity	-
Classification	-
Description	HTTP headers are used to pass additional information with HTTP response or HTTP requests. The X-XSS-Protection in HTTP header is a feature that stops a page from loading when it detects XSS attacks. This feature is becoming unnecessary with the increasing content-security-policy of sites.
Remediation	Set the X- X-XSS-Protection header

Proof of concepts:







Conclusion

This report has demonstrated the vulnerabilities and essential recommendations for the www.uber.com domain. Vulnerabilities are categorized by severity under critical, high, medium, low, and informational. And also I have significantly explained what tools I have used for this security audit for each reconnaissance, vulnerability analysis phrases.

References

1. https://owasp.org/www-project-top-ten/
2. https://github.com/nahamsec
3. https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters/blob/master/assets/vulns.md
4. https://thehackerish.com/bug-bounty-tools-from-enumeration-to-reporting/
5. https://medium.com/@hackbotone/10-recon-tools-for-bug-bounty-bafa8a5961bd
6. https://pentester.land/podcast/2019/03/01/the-bug-hunter-podcast-02.html
7. https://www.acunetix.com/vulnerabilities/web/clickjacking-x-frame-options-header-missing/

8. https://www.geeksforgeeks.org/http-headers-x-xss-protection/
9. https://portswigger.net/kb/issues/00700100_cacheable-https-response
10. https://portswigger.net/kb/issues/00500600_cookie-without-httponly-flag-set