



Web Security – IE2062

6. Uber Bug Bounty

*A D A Ihansa*

*IT22899606*

# **Web Audit**

## ***uber.com***

## Contents

Introduction to Bug Bounty program and audit scope.....	4
Information gathering phase.....	5
Finding active subdomains and their states .....	6
Sublist3r .....	6
HTTPProbe .....	8
Netcraft.....	9
Spiderfoot.....	12
Google Dorks .....	15
Directory and services enumeration.....	18
Dirbuster.....	18
Nmap .....	20
Automated Testing .....	21
OWASP ZAP .....	22
Conclusion.....	31
References .....	31

## Introduction to Bug Bounty program and audit scope

Uber.com is the official website of Uber Technologies, Inc., an American multinational company that provides various services worldwide. The platform connects drivers with riders, enabling users to request rides and drivers to earn money based on completed trips.

Uber is known for its ride-hailing services, but it also offers courier services, food delivery, and freight transport. It operates in approximately 70 countries and 10,500 cities worldwide. As of 2023, Uber had over 150 million monthly active users and facilitated an average of 28 million trips per day.

In addition to its core services, Uber is committed to sustainability, aiming to become a fully electric, zero-emission platform by 2040. The company is also dedicated to safety, using technology to improve the safety of both riders and drivers.

Uber's website allows users to learn more about its services, sign up as a driver or rider, and get help with any issues. It also provides information about the company's mission, leadership, and commitment to diversity and integrity.

In hackerone bug bounty program, they defined these subdomains (and all inclusive) as valid subdomains for testing.

uber.com

\*ubereats.com

\*.uberinternal.com

Eligible in-scope subdomains for bug bounty program are mentioned below and they mention that any subdomain under **uber.com** is in scope,

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↑	Bounty ↑	Last update ↑
<b>uber.com</b> Includes all subdomains (*.uber.com) except subdomains listed in out of scope.	Other	In scope	None	Eligible	Jul 13, 2023
<b>Recon Data</b> Uber provides endpoints to determine whether an asset belongs to Uber:  <a href="https://appsec-analysis.uber.com/public/bugbounty/ListDomains">https://appsec-analysis.uber.com/public/bugbounty/ListDomains</a> <a href="https://appsec-analysis.uber.com/public/bugbounty/ListIPs">https://appsec-analysis.uber.com/public/bugbounty/ListIPs</a>  All of the endpoints support offset and limit as optional parameters. Example: <a href="https://appsec-analysis.uber.com/public/bugbounty/ListDomains?offset=0&amp;limit=100">https://appsec-analysis.uber.com/public/bugbounty/ListDomains?offset=0&amp;limit=100</a> .  The public endpoints for asset information are for recon purposes. Information returned by those endpoints (or not) does not mean a bounty is guaranteed.					
<b>*ubereats.com</b> Includes all subdomains (*.ubereats.com) except subdomains listed in out of scope.	Other	In scope	None	Eligible	Jul 13, 2023
<b>*.uberinternal.com</b>	Other	In scope	None	Eligible	Jul 13, 2023

## Information gathering phase.

The information gathering phase, also known as reconnaissance or recon, is critical as it involves gathering information about the target to understand its nature and behavior. This phase is indispensable during audits or attacks because the more insights we gain into the target's behavior, the easier it becomes to identify potential vulnerabilities that could be exploited.

There exist two primary types of information gathering scan methods:

1. Active Scanning: This method generates significant activity on the target system, often resulting in the retrieval of extensive information.
2. Passive Scanning: Unlike active scanning, this approach minimizes disturbance on the target system, though it typically yields fewer comprehensive results compared to active scanning.

In bug bounty programs, where details about the underlying architecture of systems are usually not disclosed (referred to as black box pentesting), specific tools and techniques become crucial for gathering insights into their services, devices, and exposed information. This allows testers to gain a better understanding of the systems they are assessing.

## Finding active subdomains and their states

### Sublist3r

Sublist3r, a Python-based tool, is designed to discover subdomains associated with a specified target website. Leveraging search engines and online web services, it scours the web for available subdomains linked to the designated target domain. Given the freedom to scrutinize any subdomain under reddit.com, it's prudent to identify additional subdomains for testing purposes.

To install Sublist3r, navigate to its GitHub repository at <https://github.com/aboul3la/Sublist3r.git>. This repository hosts all the necessary files required for installing the tool. Execute the following command in your shell to download it:

...

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

...

Please note that Sublist3r necessitates either Python 2.7 or Python 3.4 to operate smoothly.

After downloading the files, go inside the 'Sublist3r' directory and install the requirements by entering,

***sudo pip install -r requirements.txt***

After installing the requirements, enter

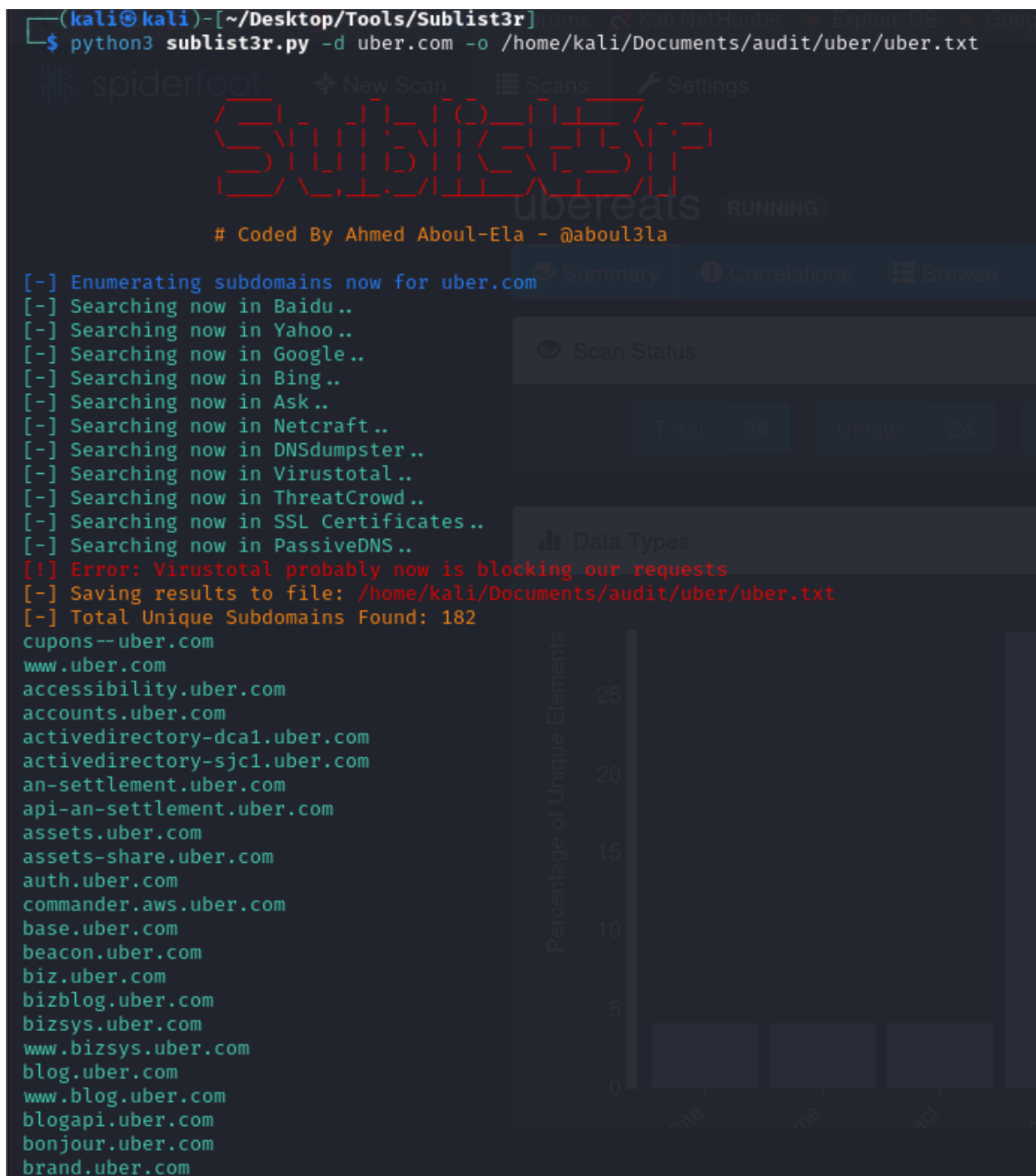
`python3 sublist3r.py -d <domain_name>`

to find subdomains under the mentioned domain.

*\*In some Linux distributions, there will be an error saying that "[!] Error: Virustotal probably now is blocking our requests". To avoid this you will need to get the API key from VirusTotal by creating an account. After the API key has been obtained, export it to an environment variable using, export VT\_APIKEY=<API key>. This will work most of the time, but this is not a must.*

Since I need to check the subdomains after, I am writing the results to a file using -o switch.

```
(kali㉿kali)-[~/Desktop/Tools/Sublist3r]
$ python3 sublist3r.py -d uber.com -o /home/kali/Documents/audit/uber/uber.txt
```



```
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for uber.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Saving results to file: /home/kali/Documents/audit/uber/uber.txt
[-] Total Unique Subdomains Found: 182
cupons--uber.com
www.uber.com
accessibility.uber.com
accounts.uber.com
activedirectory-dca1.uber.com
activedirectory-sjc1.uber.com
an-settlement.uber.com
api-an-settlement.uber.com
assets.uber.com
assets-share.uber.com
auth.uber.com
commander.aws.uber.com
base.uber.com
beacon.uber.com
biz.uber.com
bizblog.uber.com
bizsys.uber.com
www.bizsys.uber.com
blog.uber.com
www.blog.uber.com
blogapi.uber.com
bonjour.uber.com
brand.uber.com
```

Upon examining for accessible subdomains, the next step involves identifying those that are operational. This can be accomplished by employing an additional tool known as 'httprobe'.

## HTTPProbe

This tool can find domains that are up and running. To find active subdomains under this site, I am using the text file generated before by the sublist3r and writing the active subdomains to another new file.

```
(kali㉿kali)-[~/Desktop/Tools/Sublist3r]
$ httpprobe < /home/kali/Documents/audit/uber/uber.txt > /home/kali/Documents/audit/uber/active_uber.txt
```

Following the completion of the scan, the findings reveal that the majority of the subdomains are indeed active.

```
(kali㉿kali)-[~/Desktop/Tools/Sublist3r]
$ cat /home/kali/Documents/audit/uber/active_uber.txt
https://accounts.uber.com
https://accessibility.uber.com
http://accessibility.uber.com
http://accounts.uber.com
https://www.uber.com
https://beacon.uber.com
https://auth.uber.com
http://www.uber.com
http://beacon.uber.com
http://auth.uber.com
https://biz.uber.com
http://biz.uber.com
https://assets.uber.com
https://bonjour.uber.com
https://bizblog.uber.com
https://bizsys.uber.com
http://bonjour.uber.com
https://blog.uber.com
https://www.blog.uber.com
https://base.uber.com
https://business.uber.com
http://bizblog.uber.com
https://blogapi.uber.com
http://business.uber.com
http://assets.uber.com
https://central.uber.com
http://blog.uber.com
https://cn-geo1.uber.com
https://charter.uber.com
http://base.uber.com
http://central.uber.com
http://www.blog.uber.com
http://charter.uber.com
https://brand.uber.com
http://cn-geo1.uber.com
http://blogapi.uber.com
http://brand.uber.com
https://businesses.uber.com
https://comarketing.uber.com
https://direct.uber.com
https://developer.uber.com
https://discover-dish-static.uber.com
http://direct.uber.com
http://discover-dish-static.uber.com
http://developer.uber.com
https://drive.uber.com
```

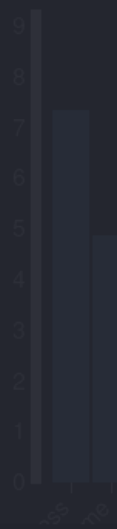
ubereats

Summary

Scan Status

Data Types

Percentage of Unique Elements






## Netcraft

Netcraft, an internet services firm, offers online security solutions. Their services encompass automated vulnerability scanning and application security. No downloads or intricate setups are necessary as these services are accessible online.

By utilizing Netcraft search feature on their website, users can retrieve various details including site rank, IP address, SSL/TLS versions in use, hosting country, and hosting company.



[LEARN MORE](#)[REPORT FRAUD ↗](#)

---

### Site report for <https://uber.com>


🔍 Look up another site?

Share: [🐞](#) [🐦](#) [f](#) [in](#) [v](#)

#### Background

Site title	Not Present	Date first seen	February 2011
Site rank	397696	Primary language	English
Description	Not Present		

#### Network

Site	<a href="https://uber.com">https://uber.com</a> ↗	Domain	<a href="https://uber.com">uber.com</a>
Netblock Owner	<a href="#">Google LLC</a>	Nameserver	edns126.ultradns.com
Hosting company	Google	Domain registrar	markmonitor.com
Hosting country	 <a href="#">US</a> ↗	Nameserver organisation	whois.corporatedomains.com
IPv4 address	34.98.127.226 ( <a href="#">VirusTotal ID</a> )	Organisation	Uber Technologies, Inc., United States
IPv4 autonomous systems	<a href="#">AS396982</a> ↗	DNS admin	serviceproviders@uber.com

For full site report: [Site report for https://uber.com | Netcraft](#)

## Site report for https://ubereats.com

► 🔍 Look up another site?

Share: [🌐](#) [🐦](#) [f](#) [in](#) [Y](#)

### Background

Site title	Not Present	Date first seen	July 2016
Site rank	302239	Primary language	English
Description	Not Present		

### Network

Site	<a href="https://ubereats.com">https://ubereats.com</a>	Domain	<a href="https://ubereats.com">ubereats.com</a>
Netblock Owner	Google LLC	Nameserver	edns126.ultradns.com
Hosting company	Google	Domain registrar	markmonitor.com
Hosting country	<a href="#">US</a>	Nameserver organisation	whois.corporatedomains.com
IPv4 address	34.98.127.226 ( <a href="#">VirusTotal</a> )	Organisation	Uber Technologies, Inc., United States
IPv4 autonomous systems	<a href="#">AS396982</a>	DNS admin	serviceproviders@uber.com

For full site report: [Site report for https://ubereats.com | Netcraft](#)

## Site report for https://uberinternal.com.com

► 🔍 Look up another site?

Share: [🌐](#) [🐦](#) [f](#) [in](#) [Y](#)

### Background

Site title	403 Forbidden	Date first seen	March 2017
Site rank	Not Present	Primary language	Dutch
Description	Not Present		

### Network

Site	<a href="https://uberinternal.com.com">https://uberinternal.com.com</a>	Domain	<a href="https://uberinternal.com.com">com.com</a>
Netblock Owner	Akamai Technologies, Inc.	Nameserver	ns1.trafficcontrolrouter.com
Hosting company	Linode - Richardson	Domain registrar	godaddy.com
Hosting country	<a href="#">us</a>	Nameserver organisation	whois.godaddy.com
IPv4 address	45.33.20.235 ( <a href="#">VirusTotal</a> )	Organisation	Unknown

For full site report: [Site report for https://uberinternal.com.com | Netcraft](#)

This data is publicly accessible, and some details regarding the system and its technology can be uncovered through available sources.

Since, many users utilize this website, and considering that the IP addresses match those of my specified targets, I only obtain a Netcraft report for this domain. However, reports for the other mentioned subdomains can also be retrieved from Netcraft.

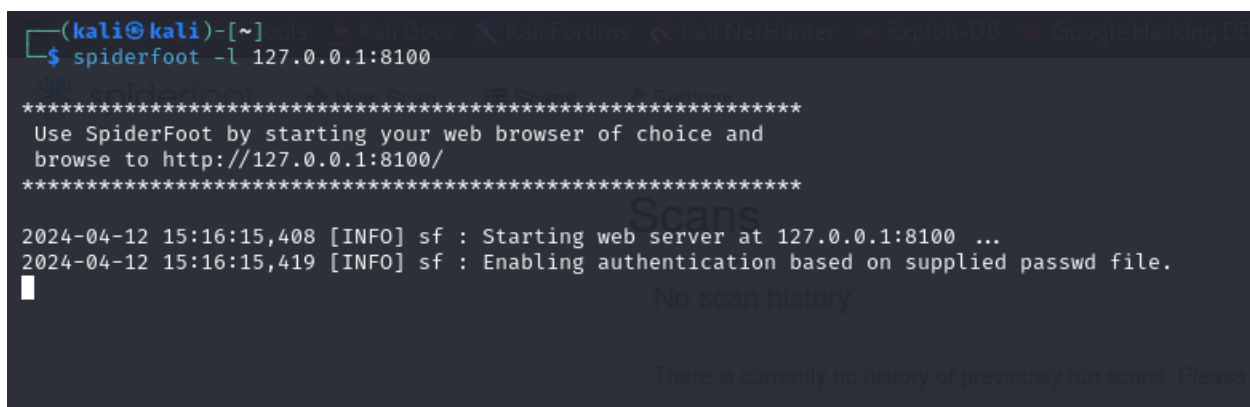
## Spiderfoot

SpiderFoot is an open-source intelligence (OSINT) automation tool that is designed to simplify the process of gathering and analyzing data. It integrates with a wide range of data sources and provides an intuitive web-based interface or a command-line option. SpiderFoot is equipped with over 200 modules for various data analysis tasks, including host/sub-domain/TLD enumeration/extraction, email address, phone number and human name extraction, and much more. It also offers export options in CSV, JSON, and GEXF formats, and integrates with the TOR network for dark web searches. SpiderFoot is a powerful tool for both offensive and defensive reconnaissance, making it an asset in the field of cybersecurity.

### Using spiderfoot

It must be setup, before using this tool.

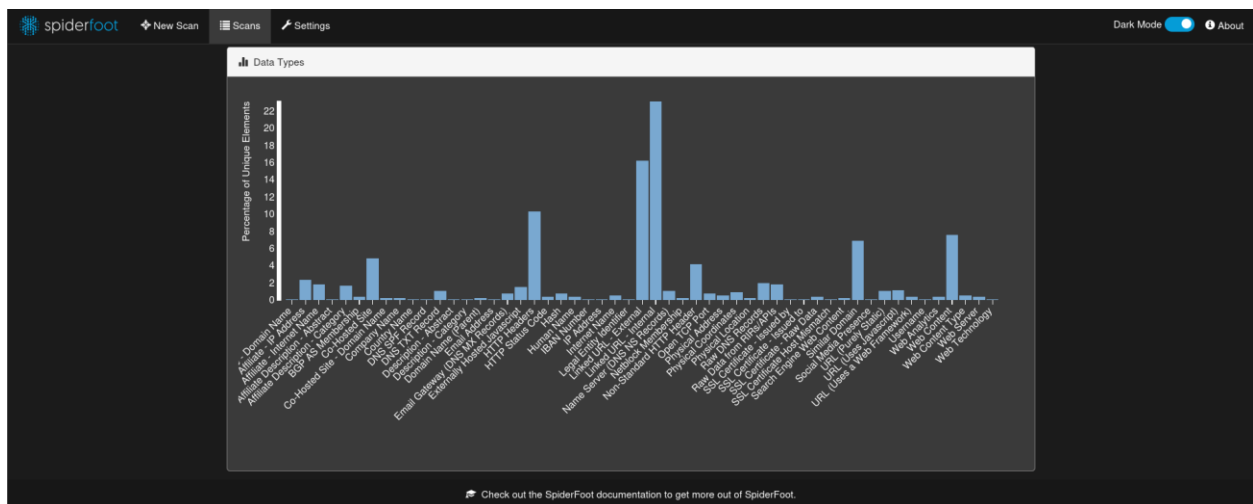
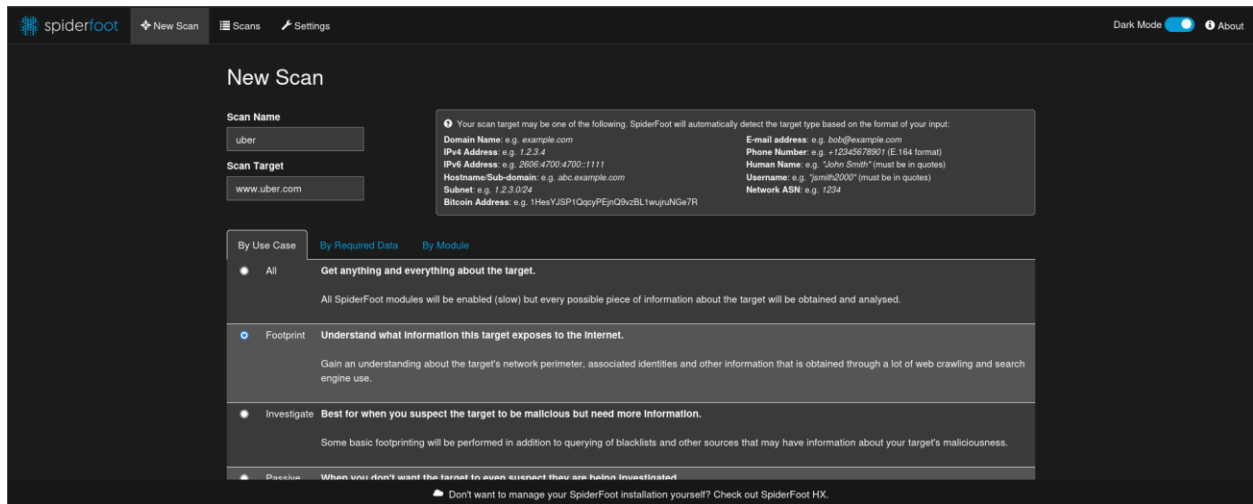
Spiderfoot -l 127.0.0.1:8100

A terminal window on a Kali Linux system. The prompt is (kali@kali)-[~]. The command \$ spiderfoot -l 127.0.0.1:8100 has been entered. The output shows a series of asterisks, followed by instructions to use SpiderFoot via a web browser at http://127.0.0.1:8100/. Another series of asterisks follows. Then, two log entries are shown: '2024-04-12 15:16:15,408 [INFO] sf : Starting web server at 127.0.0.1:8100 ...' and '2024-04-12 15:16:15,419 [INFO] sf : Enabling authentication based on supplied passwd file.' A cursor is visible on the line following the second log entry. In the background, a faint 'Scans' window is visible with the text 'No scan history' and 'There is currently no history of previously run scans. Please'.

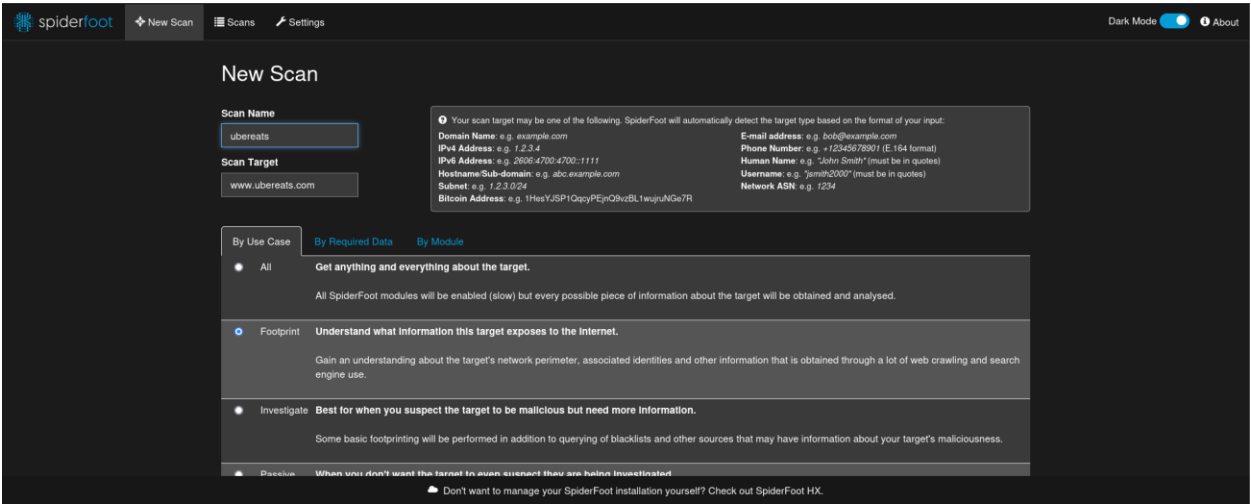
To utilize the Spiderfoot tool, which is hosted on localhost (127.0.0.1) at port 8100, just launch a web browser and enter `http://127.0.0.1:8100` in the address bar.

After the scanner loads, proceed to "New scan" and tailor your scan type according to the scope of your investigation. There are various modules at your disposal that can be activated or deactivated based on your permissions. Since you're engaging in a passive information gathering phase, opt for the 'footprint' option to crawl and collect information about the website.

## Scanned results for uber.com



Scanned results for uber eats.com

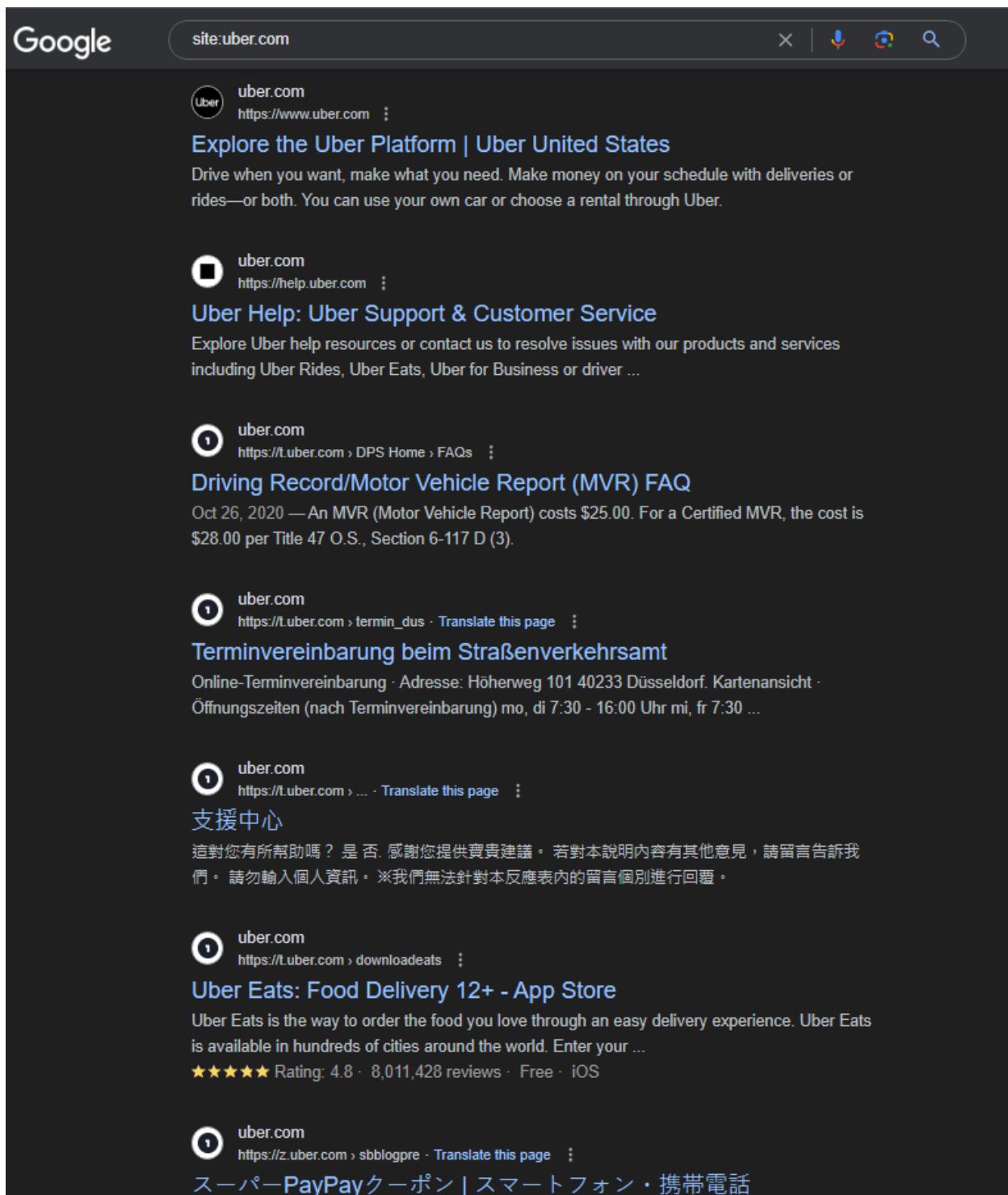


The scan has produced noteworthy findings, such as usernames, SSL certificates, and physical addresses. A significant portion of this data seems to be publicly accessible information and links leading to external websites. However, it's essential to highlight those usernames, especially when coupled with their corresponding email addresses, could potentially become avenues for social engineering or spear phishing attacks. Nevertheless, it's important to acknowledge that addressing such concerns lies beyond the boundaries of this assessment.

## Google Dorks

Google Dorks, also known as Google Hacking or Google Dorking, are specialized search queries that leverage Google's powerful search engine to unearth specific information and vulnerabilities that might not be accessible through standard searches. These are advanced search queries that use special operators to find specific information in Google's databases. They can be used to uncover hidden data or vulnerabilities on websites. By employing these dorks, you can focus on specific search results, unveiling hidden gems that ordinary searches might miss. They are valuable for security research but also pose risks if used maliciously. For example, they can reveal sensitive or private information about websites and the companies, organizations, and individuals that own and operate them. Google Dorks are a powerful tool for information gathering and vulnerability scanning, but they should be used responsibly to avoid unintended consequences.

**site:uber.com** operator searches for websites that has "**uber.com**" in their domains.



Certainly, the appearance of subdomains in search results illustrates a common utilization of Google Dorking. This method facilitates the discovery of different file types and pages that are exposed by a specific website on the internet, whether it's deliberate or unintentional. Through



the refinement of search queries, users can unearth information and potentially pinpoint vulnerabilities or confidential data that might be accessible online.

During a search for various file types exposed on the internet, I came across some intriguing and possibly concerning PDFs within this subdomain.

The screenshot shows a Google search interface with the query 'site:uber.com filetype:pdf' entered in the search bar. The search results are displayed on a dark background. The first result is titled 'Consultation des livreurs' and mentions a consultation nationale for drivers in 2019. The second result is titled 'UBER B.V. SERVICES AGREEMENT Last update' and mentions a legal agreement between Uber and drivers. The third result is titled 'PRIVATE HIRE DRIVERS LICENCE APPLICATION' and mentions a form for applying for a private hire drivers licence. The fourth result is titled 'niniejsze tłumaczenie umowy przygotowano tylko d' and mentions a translation of the Uber agreement. The fifth result is titled 'Application for a licence to drive Private Hire / Hackney ...' and mentions a driving licence check code. The sixth result is titled 'Taxi medical form' and mentions a medical fitness standard for taxi drivers.

Google

site:uber.com filetype:pdf

All Images Shopping Videos News More Tools

About 159 results (0.21 seconds)

1 uber.com  
https://t.uber.com › consultationlivreurs2020 PDF

**Consultation des livreurs**

Au printemps 2019, nous lançons la première édition de la consultation nationale pour donner la parole aux livreurs. À l'issue de 45 tables rondes et grâce ...

1 uber.com  
https://t.uber.com › servicesagreement PDF

**UBER B.V. SERVICES AGREEMENT Last update**

Oct 20, 2015 — UBER B.V.. SERVICES AGREEMENT. Last update: October 20, 2015. This Services Agreement ("Agreement") constitutes a legal agreement between an ...

1 uber.com  
https://t.uber.com › lds\_application PDF

**PRIVATE HIRE DRIVERS LICENCE APPLICATION**

PLEASE USE THIS FORM IF YOU WOULD LIKE TO APPLY FOR A PRIVATE HIRE DRIVERS. LICENCE. • BEFORE COMPLETING THIS FORM, APPLICANTS ARE ADVISED TO...

1 uber.com  
https://t.uber.com › umowa PDF

**niniejsze tłumaczenie umowy przygotowano tylko d**

Nov 24, 2015 — Niniejsza Umowa o świadczenie usług (zwana dalej „Umową”) stanowi prawnie wiążącą umowę pomiędzy Państwem, osobą fizyczną (zwana dalej ...

1 uber.com  
https://t.uber.com › WGN\_app PDF

**Application for a licence to drive Private Hire / Hackney ...**

17 The Licensing Section will carry out an online check via GOV.UK to confirm your driving licence details. This will require a driving licence check code ...

1 uber.com  
https://t.uber.com › new\_medical PDF

**Taxi medical form**

The medical fitness standard adopted by the Licensing Authority for such licence holders reflects the fitness standard for Group 2 DVLA drivers

The management of information and files within this subdomain appears to be efficient, as no additional significant files were uncovered apart from the previously mentioned PDFs.

## Directory and services enumeration

### Dirbuster

DirBuster, a web content scanner developed by OWASP, utilizes brute force methods to uncover different directories within a target website. By scrutinizing HTTP responses and their associated response codes, the tool detects concealed or referenced directories. Built in Java, DirBuster supports multi-threading to expedite directory scanning and produce a comprehensive file and folder structure of the target site.

Employing this tool facilitates the identification of directories or files that might be accessible yet not overtly exposed. Furthermore, it offers a glimpse into the server's file and folder arrangement, assisting in comprehending its structure and potential vulnerabilities

Domain: [www.uber.com](http://www.uber.com)

After running the scan for some time, DirBuster encountered errors and ceased functioning. Upon further investigation, it appeared that DirBuster was unable to access the domain.

```
file:///home/kali/Documents/audit/uber/DirBusterReport-www.uber.com-443.xml
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

-<DirBusterResults>
<Result type="Dir" path="/de/" responseCode="301"/>
<Result type="Dir" path="/fr/" responseCode="301"/>
<Result type="Dir" path="/de/4/" responseCode="301"/>
<Result type="Dir" path="/fr/3/" responseCode="301"/>
<Result type="File" path="/fr/13.php" responseCode="301"/>
<Result type="Dir" path="/de/content/" responseCode="301"/>
<Result type="Dir" path="/fr/security/" responseCode="301"/>
<Result type="File" path="/fr/3" responseCode="301"/>
<Result type="File" path="/de/15" responseCode="406"/>
<Result type="File" path="/fr/security" responseCode="301"/>
<Result type="File" path="/fr/category.php" responseCode="301"/>
<Result type="File" path="/de/15.php" responseCode="301"/>
<Result type="File" path="/de/main.php" responseCode="301"/>
<Result type="Dir" path="/de/14/" responseCode="406"/>
<Result type="Dir" path="/fr/13/" responseCode="406"/>
<Result type="File" path="/fr/13" responseCode="406"/>
<Result type="File" path="/fr/4.php" responseCode="301"/>
<Result type="File" path="/de/press.php" responseCode="301"/>
<Result type="Dir" path="/de/main/" responseCode="301"/>
<Result type="Dir" path="/fr/category/" responseCode="301"/>
<Result type="File" path="/fr/category" responseCode="301"/>
<Result type="File" path="/fr/content.php" responseCode="301"/>
<Result type="Dir" path="/de/15/" responseCode="406"/>
<Result type="Dir" path="/fr/4/" responseCode="301"/>
<Result type="File" path="/de/media.php" responseCode="301"/>
<Result type="File" path="/fr/4" responseCode="301"/>
<Result type="File" path="/fr/14.php" responseCode="301"/>
<Result type="File" path="/de/templates.php" responseCode="301"/>
<Result type="Dir" path="/de/press/" responseCode="301"/>
<Result type="File" path="/de/content/serial.php" responseCode="301"/>
<Result type="File" path="/fr/4/privacy.php" responseCode="301"/>
<Result type="File" path="/fr/category/about.php" responseCode="301"/>
<Result type="Dir" path="/fr/4/spacer/" responseCode="301"/>
<Result type="File" path="/de/partners.php" responseCode="301"/>
<Result type="File" path="/de/15/search" responseCode="406"/>
<Result type="File" path="/de/press/logo.php" responseCode="301"/>
```

I checked every result manually and not found that is suspicious or flaws.

Nmap, also known as Network Mapper, is a flexible port scanner engineered to probe hosts and reveal their open ports, associated services, port statuses, running service versions, and the operating system in use, among other details. This open-source tool serves various purposes, offering valuable insights into network configurations and potential vulnerabilities. Additionally, Nmap supports the execution of scripts on target systems to exploit vulnerabilities or gather additional information.

\*Note that some options may require administrator / super user privileges.

```
sudo nmap <host name> -sS -sV -O -oN <filename>
```

-sV: Enables version detection. It tries to detect the version of the service running in that port.

- oN : Outputs the scan results to text file

[illegible]

20 | Page

```
(kali@kali) [~/Desktop/Tools/Sublist3r]
$ sudo nmap uber eats.com -ss -sv -O -oN /home/kali/Documents/audit/uber/nmap_uber eats.txt
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 11:44 EDT
Nmap scan report for uber eats.com (34.98.127.226)
Host is up (0.032s latency).
rDNS record for 34.98.127.226: 226.127.98.34.bc.googleusercontent.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   ufe
443/tcp    open  ssl/https
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====
NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)
SF:Port80-TCP:V=7.94SVNXI=7XD=4/18XTime=66214009P=x86_64-pc-linux-gnuXr(G
SF:etRequest,B1,"HTTP/1.0;x20301x20Movedx20Permanently\r\nlocation:x20
SF:https://34\,98\,127\,226\r\nvary:x20Accept-Encoding\r\nDate:x20Thu,\
SF:x2018x20Aprx202024x2015:45:13x20GMT\r\nserver:x20ufe\r\nContent-Le
SF:ngth:x200\r\nVia:x201\,1x20google\r\n\r\n")Xr(HTTPOptions,B1,"HTTP/1
SF:\,0x20301x20Movedx20Permanently\r\nlocation:x20https://34\,98\,127\
SF:\,226\r\nvary:x20Accept-Encoding\r\nDate:x20Thu,x2018x20Aprx202024
SF:x2015:45:12x20GMT\r\nserver:x20ufe\r\nContent-Length:x200\r\nVia:x
SF:201\,1x20google\r\n\r\n")Xr(RTSRequest,IAD,"HTTP/1\,0x20400x20Badx
SF:20Request\r\nContent-Type:x20text/html;x20charset=UTF-8\r\nReferer-P
SF:olicy:x20no-referrer\r\nContent-Length:x20273\r\nDate:x20Thu,x2018\
SF:x20Aprx202024x2015:45:13x20GMT\r\n\r\n<html><head>\n<meta>x20http
SF:equiv=\ncontent-type=\ncontent-type=\ncontent-type=\ncontent-type=\n
SF:400x20Badx20Request</title>\n</head>\n<body>x20text=\n000000x20bgcolo
SF:r=\nffffff\n<h1>Error:x20Badx20Request</h1>\n<h2>Yourx20clientx20ha
SF:sx20issuedx20a\,x20malformedx20orx20illegalx20request\,</h2>\n<h2>x
SF:h2>\n</body></html>\n")Xr(Four0HFourRequest,D0,"HTTP/1\,0x20301x20Mo
SF:vedx20Permanently\r\nlocation:x20https://34\,98\,127\,226\niceX20port
SF:sX2C/Trinity\,txt\,bak\r\nvary:x20Accept-Encoding\r\nDate:x20Thu,x20
SF:18x20Aprx202024x2015:45:18x20GMT\r\nserver:x20ufe\r\nContent-Lengt
SF:h:x200\r\nVia:x201\,1x20google\r\n\r\n")Xr(DNSVersionBindReqTCP,B3,"
SF:HTTP/1\,0x20400x20Badx20Request\r\nContent-Length:x2054\r\nContent-
SF:Type:x20text/html;x20charset=UTF-8\r\nDate:x20Thu,x2018x20Aprx202
SF:024x2015:45:28x20GMT\r\n\r\n<html><title>Errorx20400x20(Badx20Req
SF:uest)\n1</title></html>\n")Xr(DNSStatusRequestTCP,B3,"HTTP/1\,0x20400x
SF:20Badx20Request\r\nContent-Length:x2054\r\nContent-Type:x20text/html
SF:\r\nContent-Length:x20273\r\nDate:x20Thu,x2018x20Aprx202024x2015:29x2
SF:0GMT\r\n\r\n<html><title>Errorx20400x20(Badx20Request)\n1</title>x
SF:/html>\n")Xr(Help,IAD,"HTTP/1\,0x20400x20Badx20Request\r\nContent-Type
SF::x20text/html;x20charset=UTF-8\r\nReferer-Policy:x20no-referrer\r\n
SF:Content-Length:x20273\r\nDate:x20Thu,x2018x20Aprx202024x2015:45:2
SF:9x20GMT\r\n\r\n<html><head>\n<meta>x20http-equiv=\ncontent-type=\n
SF:0content=\ncontent-type=\ncontent-type=\ncontent-type=\ncontent-type=\n
SF:le>\n</head>\n<body>x20text=\n000000x20bgcolor=\nffffff\n<h1>Error:x2
SF:0Badx20Request</h1>\n<h2>Yourx20clientx20hasx20issuedx20a\,x20malfo
```

Scanned results for <https://www.uberintenal.com/>

```
(kali@kali) [~/Desktop/Tools/Sublist3r]
$ sudo nmap uberintenal.com -ss -sv -O -oN /home/kali/Documents/audit/uber/nmap_uberintenal.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 11:48 EDT
Nmap scan report for uberintenal.com (34.98.127.226)
Host is up (0.03s latency).
rDNS record for 34.98.127.226: 226.127.98.34.bc.googleusercontent.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   ufe
443/tcp    open  ssl/https
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====
NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)
SF:Port80-TCP:V=7.94SVNXI=7XD=4/18XTime=66214029P=x86_64-pc-linux-gnuXr(G
SF:etRequest,B1,"HTTP/1.0;x20301x20Movedx20Permanently\r\nlocation:x20
SF:https://34\,98\,127\,226\r\nvary:x20Accept-Encoding\r\nDate:x20Thu,\
SF:x2018x20Aprx202024x2015:49:06x20GMT\r\nserver:x20ufe\r\nContent-Le
SF:ngth:x200\r\nVia:x201\,1x20google\r\n\r\n")Xr(HTTPOptions,B1,"HTTP/1
SF:\,0x20301x20Movedx20Permanently\r\nlocation:x20https://34\,98\,127\
SF:\,226\r\nvary:x20Accept-Encoding\r\nDate:x20Thu,x2018x20Aprx202024
SF:x2015:49:06x20GMT\r\nserver:x20ufe\r\nContent-Length:x200\r\nVia:x
SF:201\,1x20google\r\n\r\n")Xr(RTSRequest,IAD,"HTTP/1\,0x20400x20Badx
SF:20Request\r\nContent-Type:x20text/html;x20charset=UTF-8\r\nReferer-P
SF:olicy:x20no-referrer\r\nContent-Length:x20273\r\nDate:x20Thu,x2018\
SF:x20Aprx202024x2015:49:06x20GMT\r\n\r\n<html><head>\n<meta>x20http
SF:equiv=\ncontent-type=\ncontent-type=\ncontent-type=\ncontent-type=\n
SF:400x20Badx20Request</title>\n</head>\n<body>x20text=\n000000x20bgcolo
SF:r=\nffffff\n<h1>Error:x20Badx20Request</h1>\n<h2>Yourx20clientx20ha
SF:sx20issuedx20a\,x20malformedx20orx20illegalx20request\,</h2>\n<h2>x
SF:h2>\n</body></html>\n")Xr(Four0HFourRequest,D0,"HTTP/1\,0x20301x20Mo
SF:vedx20Permanently\r\nlocation:x20https://34\,98\,127\,226\niceX20port
SF:sX2C/Trinity\,txt\,bak\r\nvary:x20Accept-Encoding\r\nDate:x20Thu,x20
SF:18x20Aprx202024x2015:49:11x20GMT\r\nserver:x20ufe\r\nContent-Lengt
SF:h:x200\r\nVia:x201\,1x20google\r\n\r\n")Xr(DNSVersionBindReqTCP,B3,"
SF:HTTP/1\,0x20400x20Badx20Request\r\nContent-Length:x2054\r\nContent-
SF:Type:x20text/html;x20charset=UTF-8\r\nDate:x20Thu,x2018x20Aprx202
SF:024x2015:49:22x20GMT\r\n\r\n<html><title>Errorx20400x20(Badx20Req
SF:uest)\n1</title></html>\n")Xr(DNSStatusRequestTCP,B3,"HTTP/1\,0x20400x
SF:20Badx20Request\r\nContent-Length:x2054\r\nContent-Type:x20text/html
SF:\r\nContent-Length:x20273\r\nDate:x20Thu,x2018x20Aprx202024x2015:49:2
SF:2x20GMT\r\n\r\n<html><title>Errorx20400x20(Badx20Request)\n1</title>x
SF:/html>\n")Xr(Help,IAD,"HTTP/1\,0x20400x20Badx20Request\r\nContent-Type
SF::x20text/html;x20charset=UTF-8\r\nReferer-Policy:x20no-referrer\r\n
SF:Content-Length:x20273\r\nDate:x20Thu,x2018x20Aprx202024x2015:49:2
SF:2x20GMT\r\n\r\n<html><head>\n<meta>x20http-equiv=\ncontent-type=\n
SF:0content=\ncontent-type=\ncontent-type=\ncontent-type=\ncontent-type=\n
SF:le>\n</head>\n<body>x20text=\n000000x20bgcolor=\nffffff\n<h1>Error:x2
SF:0Badx20Request</h1>\n<h2>Yourx20clientx20hasx20issuedx20a\,x20malfo
SF:rmedx20orx20illegalx20request\,</h2>\n<h2></h2>\n</body></html>\n");
NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)
```

# Automated Testing

For automated testing, I've selected OWASP ZAP widely used tool within the industry.

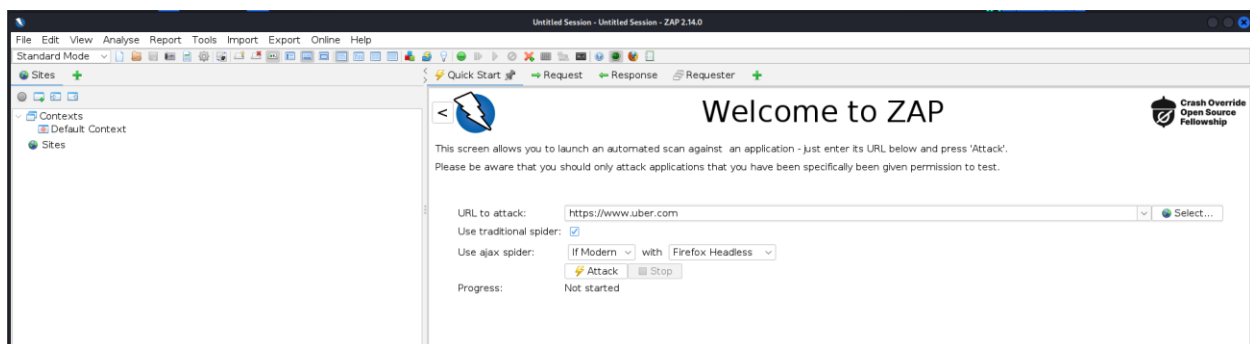
## OWASP ZAP

The Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) is a well-known open-source vulnerability scanner recognized for its ability to operate as a Man-in-the-Middle (MITM) proxy. It evaluates various vulnerabilities by examining responses from the web application or server. OWASP ZAP is notably user-friendly and offers customization options through the installation of modules, allowing for efficient management of results.

Within this proxy, there are primarily two types of scans available:

1. Automated Scan: Users input the target URL and initiate the attack. The behavior can be customized by selecting the ZAP mode, triggering all scripts against the target to detect vulnerabilities and generate reports accordingly.
2. Manual Explore: Users can navigate to the target web application and begin exploration. During manual exploration, ZAP HUD (Hheads Up Display) captures each page, while the ZAP proxy records responses.

For this assessment, I am running ZAP in automated mode.



After specifying the target URL in the designated textbox, simply select "Attack" to initiate the scanning process. Upon completion, a comprehensive report of the findings can be generated by selecting "Report." Below are screenshots showcasing the results obtained after scanning several domains.

### Alert counts by risk and confidence

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

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

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	1 (3.8%)	0 (0.0%)	0 (0.0%)	1 (3.8%)
	Medium	0 (0.0%)	5 (19.2%)	1 (3.8%)	0 (0.0%)	6 (23.1%)
	Low	0 (0.0%)	3 (11.5%)	7 (26.9%)	1 (3.8%)	11 (42.3%)
	Informational	0 (0.0%)	0 (0.0%)	4 (15.4%)	4 (15.4%)	8 (30.8%)
	Total	0 (0.0%)	9 (34.6%)	12 (46.2%)	5 (19.2%)	26 (100%)

### Alert counts by alert type

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

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

Alert type	Risk	Count
<a href="#">PII Disclosure</a>	High	1 (3.8%)
<a href="#">CSP: Wildcard Directive</a>	Medium	271 (1,042.3%)
<a href="#">CSP: script-src unsafe-inline</a>	Medium	180 (692.3%)
<a href="#">CSP: style-src unsafe-inline</a>	Medium	269 (1,034.6%)
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	1 (3.8%)
<a href="#">Cross-Domain Misconfiguration</a>	Medium	98 (376.9%)
<a href="#">Session ID in URL Rewrite</a>	Medium	1 (3.8%)
<a href="#">Application Error Disclosure</a>	Low	1 (3.8%)
<a href="#">CSP: Notices</a>	Low	273 (1,050.0%)
<a href="#">Cookie No HttpOnly Flag</a>	Low	72 (276.9%)
<a href="#">Cookie Without Secure Flag</a>	Low	2 (7.7%)
<a href="#">Cookie without SameSite Attribute</a>	Low	77 (296.2%)
<a href="#">Cross-Domain JavaScript Source File Inclusion</a>	Low	173 (665.4%)
<a href="#">Information Disclosure - Debug Error Messages</a>	Low	1 (3.8%)



<a href="#">Server Leaks Version Information via "Server" HTTP Response Header Field</a>	Low	13 (50.0%)
<a href="#">Strict-Transport-Security Header Not Set</a>	Low	12 (46.2%)
<a href="#">Timestamp Disclosure - Unix</a>	Low	71 (273.1%)
<a href="#">X-Content-Type-Options Header Missing</a>	Low	13 (50.0%)
<a href="#">Charset Mismatch</a>	Informational	22 (84.6%)
<a href="#">Information Disclosure - Sensitive Information in URL</a>	Informational	1 (3.8%)
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	122 (469.2%)
<a href="#">Loosely Scoped Cookie</a>	Informational	67 (257.7%)
<a href="#">Modern Web Application</a>	Informational	87 (334.6%)
<a href="#">Re-examine Cache-control Directives</a>	Informational	31 (119.2%)
<a href="#">Retrieved from Cache</a>	Informational	8 (30.8%)
<a href="#">Session Management Response Identified</a>	Informational	301 (1,157.7%)
Total		26

\*Note that these vulnerabilities are rated according to the OWASP risk rating methodology which can be found in this link. [OWASP Risk Rating Methodology](#).

Here are the vulnerabilities detected within this domain, along with their impacts. The insights provided, including screenshots and remedies, are sourced from the report generated by OWASP ZAP and the Netsparker website. [ <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities> ])

## Content Security Policy (CSP) Header Not Set (1)

▼ GET https://www.uber.com/\_events

### Alert tags

- [OWASP\\_2021\\_A05](#)
- [OWASP\\_2017\\_A06](#)

### Alert description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

### Request

- Request line and header section (233 bytes)
- Request body (0 bytes)

### Response

- Status line and header section (456 bytes)
- Response body (552 bytes)

### Solution

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

## Information Disclosure - Debug Error Messages (1)

▼ GET https://www.uber.com/bootstrap.json?referrer=&\_bmd=2024-04-27T15%3A23%3A29.671Z\_16edc7ba-7b10-4a33-b036-81c1b8720a44

### Alert tags

- [OWASP\\_2021\\_A01](#)
- [WSTG-v42-ERRH-01](#)
- [OWASP\\_2017\\_A03](#)

### Alert description

The response appeared to contain common error messages returned by platforms such as ASP.NET, and Web-servers such as IIS and Apache. You can configure the list of common debug messages.

### Request

- Request line and header section (321 bytes)
- Request body (0 bytes)

### Response

- Status line and header section (460 bytes)
- ▼ Response body (21 bytes)

Internal Server Error

### Evidence

Internal Server Error

### Solution

Disable debugging messages before pushing to production.

<https://www.uber.com> (2)

### Modern Web Application (1)

▼ GET <https://www.uber.com/lk/si-lk/>

#### Alert tags

#### Alert description

The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

#### Other Info

Links have been found with a target of '\_self' - this is often used by modern frameworks to force a full page reload.

#### Request

► Request line and header section (726 bytes)

▼ Request body (0 bytes)

#### Response

► Status line and header section (3079 bytes)

► Response body (154019 bytes)

#### Evidence

```
<a data-baseweb="link" href="https://www.uber.com/"
target="_self" aria-label="Go to Uber.com"
class="css-jHDdnW">Uber</a>
```

#### Solution

This is an informational alert and so no changes are required.

### **Charset Mismatch (1)**

▼ GET <https://www.uber.com/sitemap.xml>

#### **Alert tags**

##### **Alert description**

This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set.

An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.

##### **Other Info**

There was a charset mismatch between the HTTP Header and the XML encoding declaration: [utf-8] and [utf8] do not match.

##### **Request**

- Request line and header section (237 bytes)
- Request body (0 bytes)

##### **Response**

- Status line and header section (946 bytes)
- Response body (30602 bytes)

##### **Solution**

Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.

## **Information Disclosure - Suspicious Comments (1)**

▼ GET <https://www.uber.com/lk/si-lk/>

### **Alert tags**

- [OWASP\\_2021\\_A01](#)
- [WSTG-v42-INFO-05](#)
- [OWASP\\_2017\\_A03](#)

### **Alert description**

The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

### **Other info**

The following pattern was used: `\bDEBUG\b` and was detected in the element starting with: `"<script nonce="87abfee0-42e9-47c5-8601-f50048d0600a" integrity="sha384-Wkhg1tNdk1rCHUoJ0lotbHgQ8p34Ft77j2oX5JT1x5V7oU4PHPUx2Tzyx"`, see evidence field for the suspicious comment/snippet.

### **Request**

- Request line and header section (726 bytes)
- Request body (0 bytes)

### **Response**

- Status line and header section (3079 bytes)
- Response body (154019 bytes)

### **Evidence**

debug

### **Solution**

Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

## Conclusion

The web application, along with its associated authorization gateway, showcases a commendable level of upkeep and control, particularly from a cybersecurity standpoint. While there have been occurrences of information exposure, these can be suitably handled, and their corresponding risk quotient is evaluated to be minimal. It's worth noting that all detected security weaknesses fell into the categories of either being Informational or of Low severity. Moreover, the vulnerabilities that were categorized as Low are not readily exploitable, as has been evidenced in the past.

It's also important to highlight that the application's security measures are regularly updated to keep up with the evolving threat landscape. Regular security audits are conducted to identify and rectify any potential vulnerabilities. The application also employs a robust encryption mechanism to protect sensitive data and ensure secure communication. Additionally, the application's user authentication process is designed to prevent unauthorized access, further enhancing its security posture. Despite the presence of some low-level vulnerabilities, the overall security of the web application and its authorization portal is well-maintained and managed. This reflects the commitment to security and the proactive approach taken towards identifying and addressing potential security issues.

## References

[OWASP Top Ten | OWASP Foundation](#)

[WSTG - Stable | OWASP Foundation](#)

[ZAP \(zaproxy.org\)](#)

[GitHub - aboul3la/Sublist3r: Fast subdomains enumeration tool for penetration testers](#)

[GitHub - tomnomnom/httpprobe: Take a list of domains and probe for working HTTP and HTTPS servers](#)

[Kali Tools | Kali Linux Tools](#)

[Netcraft | Leader in Phishing Detection, Cybercrime Disruption and Website Takedown](#)

[Nmap: the Network Mapper - Free Security Scanner](#)