Sri Lanka Institute of Information Technology

LifeOmic Web Audit

Bug Bounty Assignment

IE2062 – Web Security

Submitted by –

Student Registration Number	Student Name
IT20627928	Herath H.M.T.D

One drive Link:

https://mysliit-my.sharepoint.com/:f:/g/personal/it20627928_my_sliit_lk/ErCkCCMhfzdEkFCQoernyxYBs-88uupAVvG9ohNo8XnsxQ?e=e6uip0

Date of Submission

2022.06.06

Table of Contents

Acknowledgement

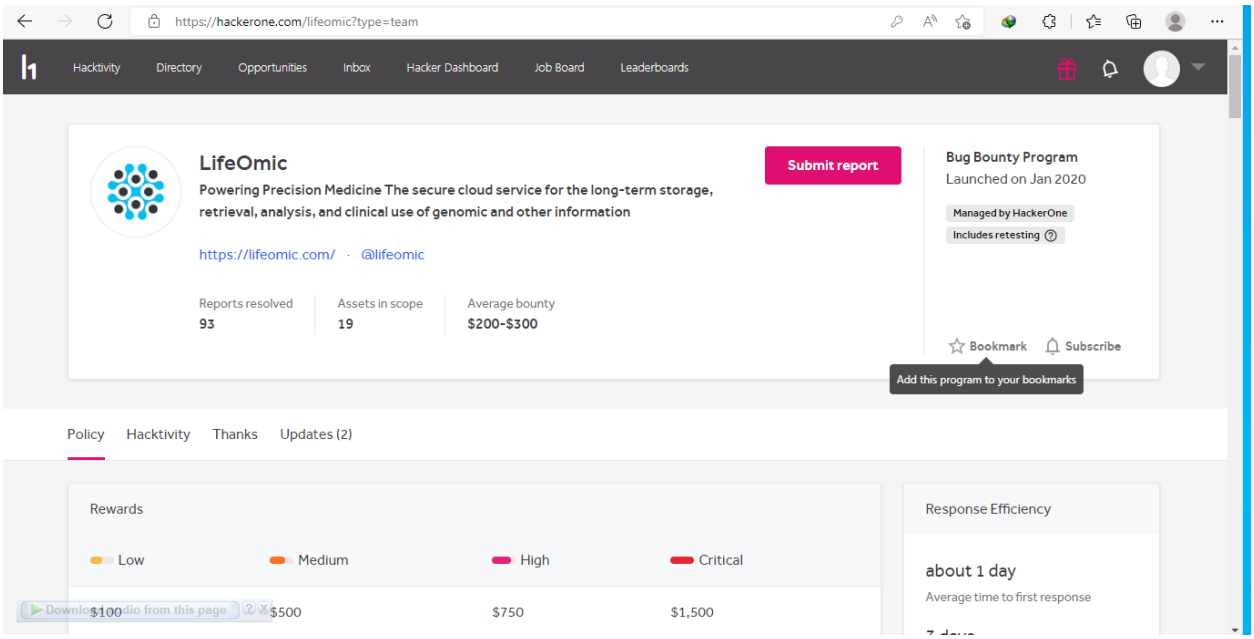
I'd like to thank Dr. Lakmal Rupasinghe, the lecturer in charge of the Web security module, for his essential assistance and advice, which was crucial to the start of our web audit.

I'd like to express my gratitude to Ms. Chethna Lyanapathirana, Ms. Lanisha Rugghahakotuwa, and Ms. Chathu Udagedra for their assistance and direction throughout this Web audit.

Objectives of the Assessment

The https://lifeomic.com security evaluation for the second year second semester Web Security Module. The goal of this assessment is to find vulnerabilities in the target domain and to determine the risk level associated with such vulnerabilities.

Selected domain



LifeOmic is a precision health platform that stores, retrieves, analyzes, and uses patient data such as genomics, clinical, imaging, wearables, and demographic data for clinical application. Consumers, healthcare providers, companies, and health coaches may all benefit from the company's health applications.

LifeOmic is based in Indianapolis, Indiana, and was formed in 2016 by CEO Dr. Don Brown.

Features & Products of LifeOmic

LifeOmic provides a wide range of goods and services for a number of uses and healthcare disciplines, including:

• Oncology

• Cardiology

• Integrative Medicine

• Employee Health and Happiness

• Nutritional Counseling

• Individuals

Policy Analyzing

They told us about the policies and other details about HackerOne. So, before we begin looking at technological viewpoints, we must first examine their terms and circumstances. We must acquire information about the website and thoroughly research their policies since if we do something unlawful, they may pursue legal action against us.

Scope

Every bug bounty program has its own scope, and as a hunter, we must understand what is in-scope and what is out-of-scope. This section discusses how to report a problem and describes the program's disclosure policy, among other things. Because inappropriate disclosure (for example, publicly reporting a flaw without authority when authorization is required) might have unfavorable implications for both you and the client, it's vital that you understand the system's policy statement..

Out of scope

*.us.lifeomic.com

https://lifeapps.io

info.lifeomic.com

lifeomic.com

fed.*.lifeomic.com

DMARC, SPF, DKIM

In-scope domains

https://apps.wellness.dev.lifeomic.com

https://lifeology.dev.lifeomic.com

https://lifeology.dev.lifeomic.com

apps.dev.skillspring.com

marketplace.dev.lifeomic.com

api.dev.lifeomic.com

Information Gathering

Information collection is the process of acquiring various forms of data about the target victim or system.

For information collecting and vulnerability evaluation, I utilized certain inbuilt kalilinux utilities as well as some tools from the github repository.

- **Subdomain Enumeration**

Subdomain enumeration is a strategy for obtaining data. It may be used to define all of a company's internet-accessible sites. It is fairly usual in large enterprises to have some forgotten websites with vulnerabilities or sensitive data. As a result, subdomain enumeration is crucial for bug bounty programs..

Subdomain enumeration tools

1. Subfinder
2. Subdomainizer
3. Bug bounty hunting tool by nahamsec
4. Crt.sh

1. Subfinder

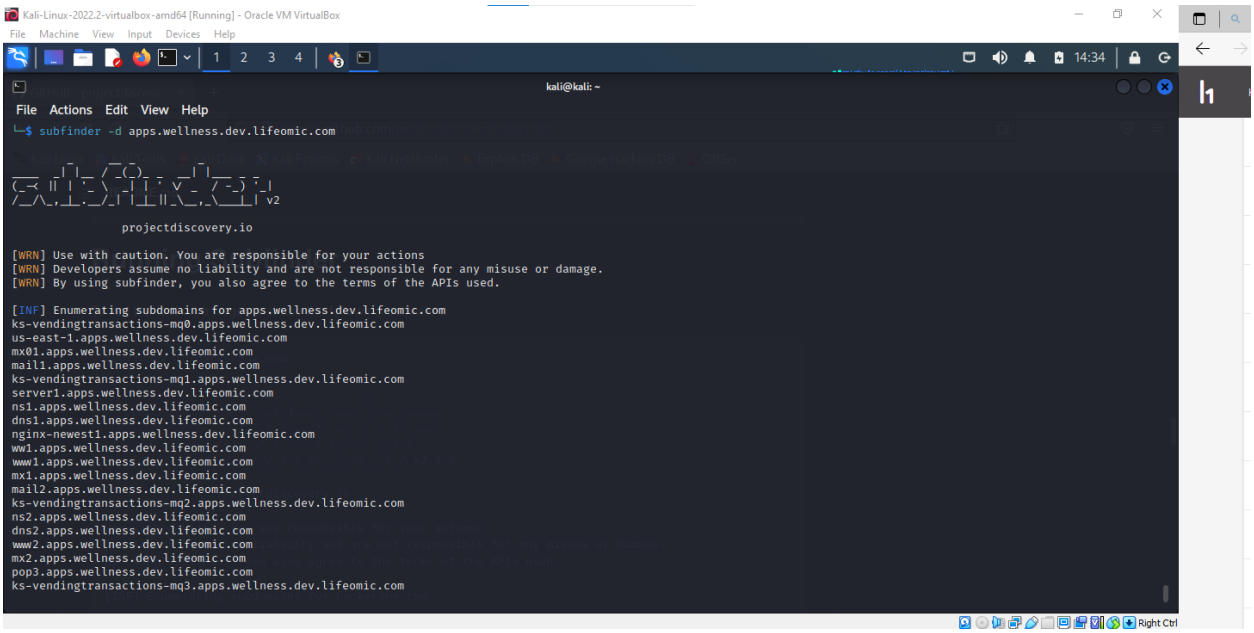
   subfinder is a subdomain discovery tool that uses passive online sources to locate acceptable subdomains for websites. It features a straightforward modular design that is intended for speed. Subfinder was designed to accomplish one thing and one thing well: passive subdomain enumeration.

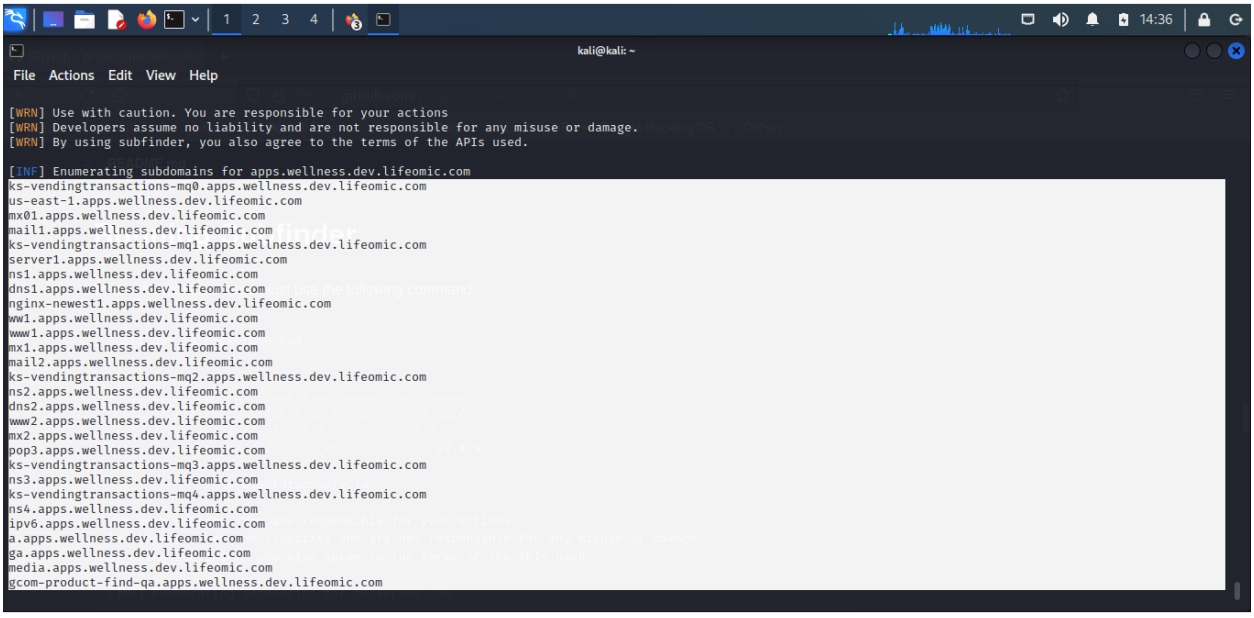
- For the installation go to the following GitHub page and clone to the machine

  Github link - GitHub - projectdiscovery/subfinder

- Target domain - apps.wellness.dev.lifeomic.com
- To run the tool on a target, just use the following command.

  subfinder –d <target domain>


Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
14:34
kali@kali: ~
File Actions Edit View Help
└─$ subfinder -d apps.wellness.dev.lifeomic.com
projectdiscovery.io
[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using subfinder, you also agree to the terms of the APIs used.
[INF] Enumerating subdomains for apps.wellness.dev.lifeomic.com
ks-vendingtransactions-mq0.apps.wellness.dev.lifeomic.com
us-east-1.apps.wellness.dev.lifeomic.com
mx01.apps.wellness.dev.lifeomic.com
mail1.apps.wellness.dev.lifeomic.com
ks-vendingtransactions-mq1.apps.wellness.dev.lifeomic.com
server1.apps.wellness.dev.lifeomic.com
ns1.apps.wellness.dev.lifeomic.com
dns1.apps.wellness.dev.lifeomic.com
nginx-newest1.apps.wellness.dev.lifeomic.com
ww1.apps.wellness.dev.lifeomic.com
www1.apps.wellness.dev.lifeomic.com
mx1.apps.wellness.dev.lifeomic.com
mail2.apps.wellness.dev.lifeomic.com
ks-vendingtransactions-mq2.apps.wellness.dev.lifeomic.com
ns2.apps.wellness.dev.lifeomic.com
dns2.apps.wellness.dev.lifeomic.com
www2.apps.wellness.dev.lifeomic.com
mx2.apps.wellness.dev.lifeomic.com
pop3.apps.wellness.dev.lifeomic.com
ks-vendingtransactions-mq3.apps.wellness.dev.lifeomic.com
Right Ctrl


14:36
kali@kali: ~
File Actions Edit View Help
[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using subfinder, you also agree to the terms of the APIs used.
[INF] Enumerating subdomains for apps.wellness.dev.lifeomic.com
ks-vendingtransactions-mq0.apps.wellness.dev.lifeomic.com
us-east-1.apps.wellness.dev.lifeomic.com
mx01.apps.wellness.dev.lifeomic.com
mail1.apps.wellness.dev.lifeomic.com
ks-vendingtransactions-mq1.apps.wellness.dev.lifeomic.com
server1.apps.wellness.dev.lifeomic.com
ns1.apps.wellness.dev.lifeomic.com
dns1.apps.wellness.dev.lifeomic.com
nginx-newest1.apps.wellness.dev.lifeomic.com
ww1.apps.wellness.dev.lifeomic.com
www1.apps.wellness.dev.lifeomic.com
mx1.apps.wellness.dev.lifeomic.com
mail2.apps.wellness.dev.lifeomic.com
ks-vendingtransactions-mq2.apps.wellness.dev.lifeomic.com
ns2.apps.wellness.dev.lifeomic.com
dns2.apps.wellness.dev.lifeomic.com
www2.apps.wellness.dev.lifeomic.com
mx2.apps.wellness.dev.lifeomic.com
pop3.apps.wellness.dev.lifeomic.com
ks-vendingtransactions-mq3.apps.wellness.dev.lifeomic.com
ns3.apps.wellness.dev.lifeomic.com
ks-vendingtransactions-mq4.apps.wellness.dev.lifeomic.com
ns4.apps.wellness.dev.lifeomic.com
ipv6.apps.wellness.dev.lifeomic.com
a.apps.wellness.dev.lifeomic.com
ga.apps.wellness.dev.lifeomic.com
media.apps.wellness.dev.lifeomic.com
gcom-product-find-qa.apps.wellness.dev.lifeomic.com

```
gcom-product-find-qa.apps.wellness.dev.lifeomic.com
cim-api-qa.apps.wellness.dev.lifeomic.com
searchportal-qa.apps.wellness.dev.lifeomic.com
gws-qa.apps.wellness.dev.lifeomic.com
cim-data-quality-qa.apps.wellness.dev.lifeomic.com
beta.apps.wellness.dev.lifeomic.com
okta.apps.wellness.dev.lifeomic.com
owa.apps.wellness.dev.lifeomic.com
b.apps.wellness.dev.lifeomic.com
collab.apps.wellness.dev.lifeomic.com
gitlab.apps.wellness.dev.lifeomic.com
db.apps.wellness.dev.lifeomic.com
mongodb.apps.wellness.dev.lifeomic.com
web.apps.wellness.dev.lifeomic.com
job.apps.wellness.dev.lifeomic.com
c.apps.wellness.dev.lifeomic.com
dc.apps.wellness.dev.lifeomic.com
basic.apps.wellness.dev.lifeomic.com
static.apps.wellness.dev.lifeomic.com
elastic.apps.wellness.dev.lifeomic.com
_dmarc.apps.wellness.dev.lifeomic.com
download.apps.wellness.dev.lifeomic.com
upload.apps.wellness.dev.lifeomic.com
old.apps.wellness.dev.lifeomic.com
inbound.apps.wellness.dev.lifeomic.com
pre-prod.apps.wellness.dev.lifeomic.com
non-prod.apps.wellness.dev.lifeomic.com
gac-rds-external-readonly-preprod.apps.wellness.dev.lifeomic.com
awsdashboard.apps.wellness.dev.lifeomic.com
cloud.apps.wellness.dev.lifeomic.com
office.apps.wellness.dev.lifeomic.com
voice.apps.wellness.dev.lifeomic.com
wfm-service.apps.wellness.dev.lifeomic.com
de.apps.wellness.dev.lifeomic.com
```

kali@kali: ~

File Actions Edit View Help

```
de.apps.wellness.dev.lifeomic.com
code.apps.wellness.dev.lifeomic.com
stage.apps.wellness.dev.lifeomic.com
edge.apps.wellness.dev.lifeomic.com
_collab-edge.apps.wellness.dev.lifeomic.com
exchange.apps.wellness.dev.lifeomic.com
mobile.apps.wellness.dev.lifeomic.com
cname.apps.wellness.dev.lifeomic.com
home.apps.wellness.dev.lifeomic.com
sitecore.apps.wellness.dev.lifeomic.com
store.apps.wellness.dev.lifeomic.com
pre.apps.wellness.dev.lifeomic.com
secure.apps.wellness.dev.lifeomic.com
certificate.apps.wellness.dev.lifeomic.com
liveupdate.apps.wellness.dev.lifeomic.com
remote.apps.wellness.dev.lifeomic.com
spf.apps.wellness.dev.lifeomic.com
autoconfig.apps.wellness.dev.lifeomic.com
img.apps.wellness.dev.lifeomic.com
staging.apps.wellness.dev.lifeomic.com
publishing-catalog.apps.wellness.dev.lifeomic.com
blog.apps.wellness.dev.lifeomic.com
auth.apps.wellness.dev.lifeomic.com
akamai.apps.wellness.dev.lifeomic.com
wiki.apps.wellness.dev.lifeomic.com
api.apps.wellness.dev.lifeomic.com
ks-invoice-api.apps.wellness.dev.lifeomic.com
ks-program-api.apps.wellness.dev.lifeomic.com
cim-api.apps.wellness.dev.lifeomic.com
cdq-api.apps.wellness.dev.lifeomic.com
ks-order-api.apps.wellness.dev.lifeomic.com
vendor-api.apps.wellness.dev.lifeomic.com
ks-limits-api.apps.wellness.dev.lifeomic.com
ks-inventory-api.apps.wellness.dev.lifeomic.com
```

kali@kali: ~

File Actions Edit View Help

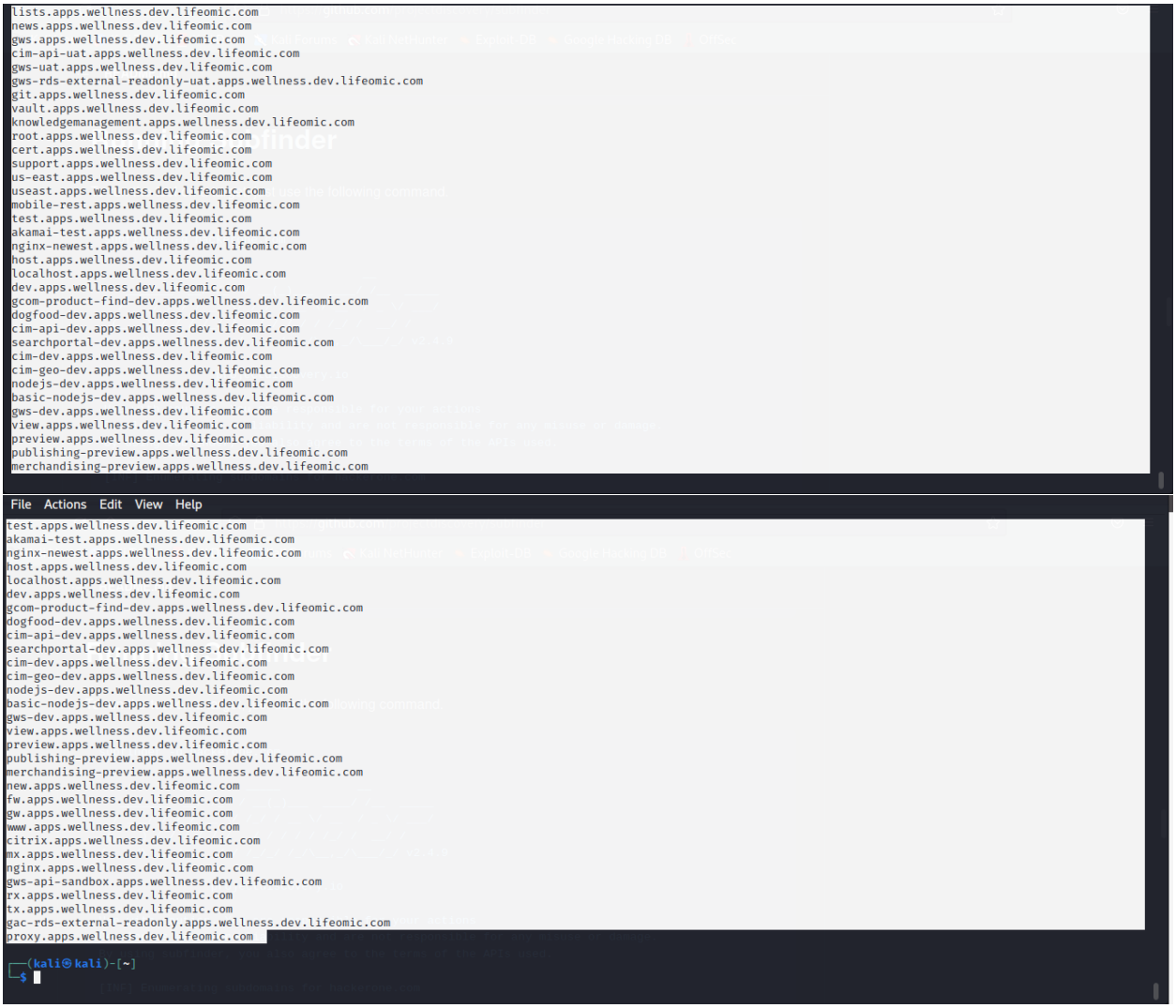
```
ks-inventory-api.apps.wellness.dev.lifeomic.com
acapi.apps.wellness.dev.lifeomic.com
cveapi.apps.wellness.dev.lifeomic.com
gui.apps.wellness.dev.lifeomic.com
check.apps.wellness.dev.lifeomic.com
click.apps.wellness.dev.lifeomic.com
storybook.apps.wellness.dev.lifeomic.com
webhook.apps.wellness.dev.lifeomic.com
outlook.apps.wellness.dev.lifeomic.com
webdisk.apps.wellness.dev.lifeomic.com
uk.apps.wellness.dev.lifeomic.com
portal.apps.wellness.dev.lifeomic.com
searchportal.apps.wellness.dev.lifeomic.com
cpanel.apps.wellness.dev.lifeomic.com
mail.apps.wellness.dev.lifeomic.com
webmail.apps.wellness.dev.lifeomic.com
email.apps.wellness.dev.lifeomic.com
retail.apps.wellness.dev.lifeomic.com
ml.apps.wellness.dev.lifeomic.com
sql.apps.wellness.dev.lifeomic.com
mssql.apps.wellness.dev.lifeomic.com
mysql.apps.wellness.dev.lifeomic.com
ssl.apps.wellness.dev.lifeomic.com
_etcd-server-ssl.apps.wellness.dev.lifeomic.com
consul.apps.wellness.dev.lifeomic.com
m.apps.wellness.dev.lifeomic.com
iam.apps.wellness.dev.lifeomic.com
mdm.apps.wellness.dev.lifeomic.com
whm.apps.wellness.dev.lifeomic.com
dnm.apps.wellness.dev.lifeomic.com
crm.apps.wellness.dev.lifeomic.com
forum.apps.wellness.dev.lifeomic.com
cdn.apps.wellness.dev.lifeomic.com
en.apps.wellness.dev.lifeomic.com
```

Right Ctrl

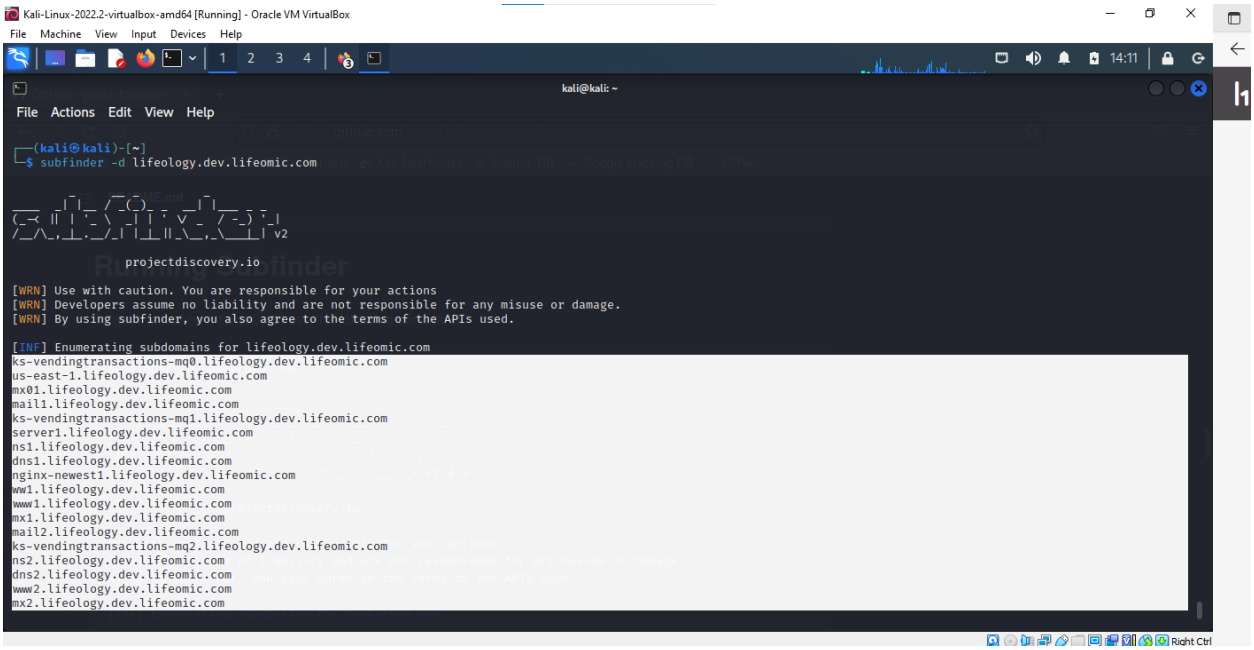
```
en.apps.wellness.dev.lifeomic.com
httpbin.apps.wellness.dev.lifeomic.com
akamai-test-origin.apps.wellness.dev.lifeomic.com
login.apps.wellness.dev.lifeomic.com
_cuplogin.apps.wellness.dev.lifeomic.com
admin.apps.wellness.dev.lifeomic.com
signin.apps.wellness.dev.lifeomic.com
vpn.apps.wellness.dev.lifeomic.com
sslvpn.apps.wellness.dev.lifeomic.com
dyn.apps.wellness.dev.lifeomic.com
video.apps.wellness.dev.lifeomic.com
info.apps.wellness.dev.lifeomic.com
go.apps.wellness.dev.lifeomic.com
mongo.apps.wellness.dev.lifeomic.com
demo.apps.wellness.dev.lifeomic.com
sso.apps.wellness.dev.lifeomic.com
imap.apps.wellness.dev.lifeomic.com
wap.apps.wellness.dev.lifeomic.com
cp.apps.wellness.dev.lifeomic.com
_cuplogin._tcp.apps.wellness.dev.lifeomic.com
_cisco-uds._tcp.apps.wellness.dev.lifeomic.com
ip.apps.wellness.dev.lifeomic.com
sip.apps.wellness.dev.lifeomic.com
help.apps.wellness.dev.lifeomic.com
shop.apps.wellness.dev.lifeomic.com
pop.apps.wellness.dev.lifeomic.com
app.apps.wellness.dev.lifeomic.com
danieapp.apps.wellness.dev.lifeomic.com
ftp.apps.wellness.dev.lifeomic.com
smtp.apps.wellness.dev.lifeomic.com
signup.apps.wellness.dev.lifeomic.com
wp.apps.wellness.dev.lifeomic.com
builder.apps.wellness.dev.lifeomic.com
docker.apps.wellness.dev.lifeomic.com
```

File Actions Edit View Help

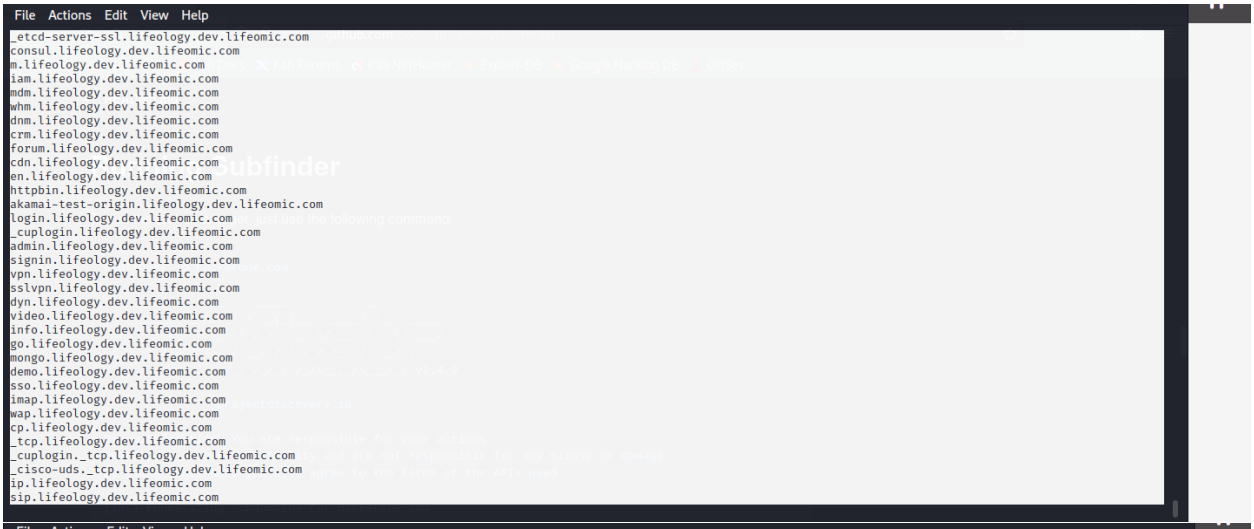
```
docker.apps.wellness.dev.lifeomic.com
hostmaster.apps.wellness.dev.lifeomic.com
postmaster.apps.wellness.dev.lifeomic.com
autodiscover.apps.wellness.dev.lifeomic.com
server.apps.wellness.dev.lifeomic.com
mailserver.apps.wellness.dev.lifeomic.com
vendor.apps.wellness.dev.lifeomic.com
k8s.apps.wellness.dev.lifeomic.com
bbs.apps.wellness.dev.lifeomic.com
jobs.apps.wellness.dev.lifeomic.com
metrics.apps.wellness.dev.lifeomic.com
_cisco-uds.apps.wellness.dev.lifeomic.com
images.apps.wellness.dev.lifeomic.com
kubernetes.apps.wellness.dev.lifeomic.com
blogs.apps.wellness.dev.lifeomic.com
whois.apps.wellness.dev.lifeomic.com
nodejs.apps.wellness.dev.lifeomic.com
tools.apps.wellness.dev.lifeomic.com
tls.apps.wellness.dev.lifeomic.com
_collab-edge._tls.apps.wellness.dev.lifeomic.com
forums.apps.wellness.dev.lifeomic.com
ns.apps.wellness.dev.lifeomic.com
dns.apps.wellness.dev.lifeomic.com
videos.apps.wellness.dev.lifeomic.com
orders.apps.wellness.dev.lifeomic.com
careers.apps.wellness.dev.lifeomic.com
servers.apps.wellness.dev.lifeomic.com
vendors.apps.wellness.dev.lifeomic.com
wordpress.apps.wellness.dev.lifeomic.com
stats.apps.wellness.dev.lifeomic.com
assets.apps.wellness.dev.lifeomic.com
mta-sts.apps.wellness.dev.lifeomic.com
_mta-sts.apps.wellness.dev.lifeomic.com
lists.apps.wellness.dev.lifeomic.com
```

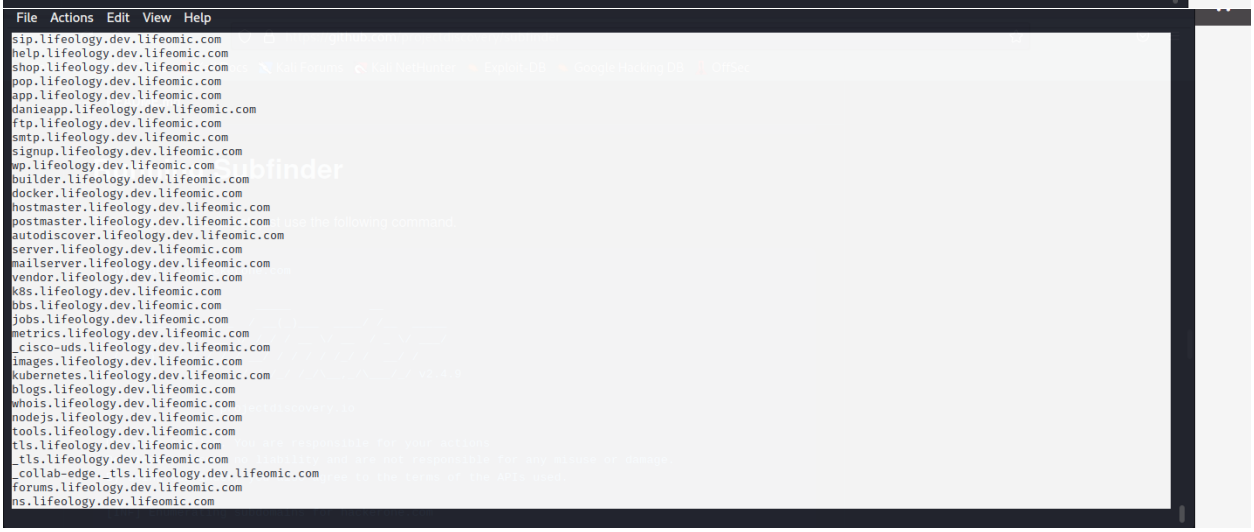


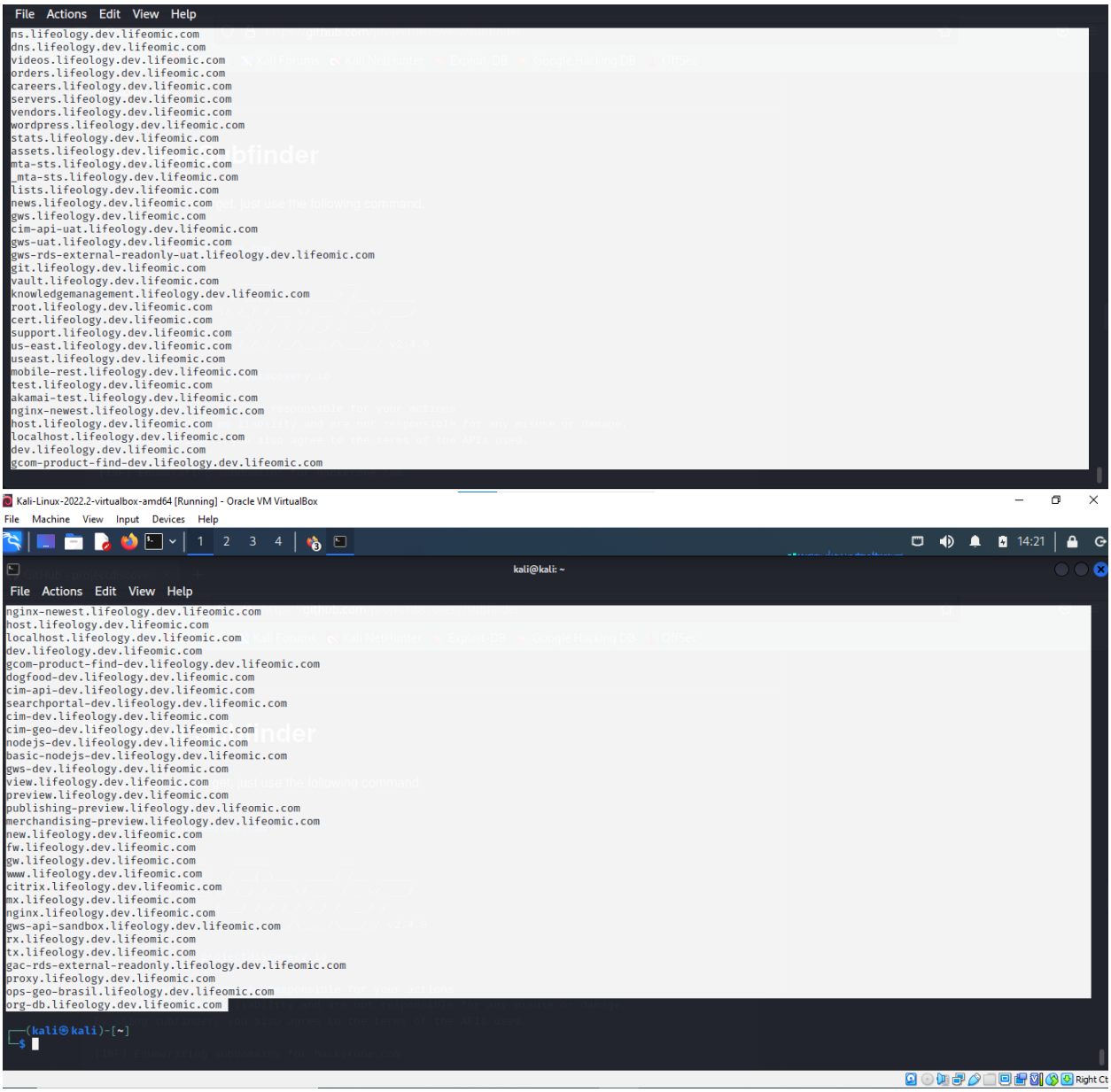
Target domain -**_lifeology.dev.lifeomic.com**


Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
14:11
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ subfinder -d lifeology.dev.lifeomic.com
projectdiscovery.io
[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using subfinder, you also agree to the terms of the APIs used.
[INF] Enumerating subdomains for lifeology.dev.lifeomic.com
ks-vendingtransactions-mq0.lifeology.dev.lifeomic.com
us-east-1.lifeology.dev.lifeomic.com
mx01.lifeology.dev.lifeomic.com
mail1.lifeology.dev.lifeomic.com
ks-vendingtransactions-mq1.lifeology.dev.lifeomic.com
server1.lifeology.dev.lifeomic.com
ns1.lifeology.dev.lifeomic.com
dns1.lifeology.dev.lifeomic.com
nginx-newest1.lifeology.dev.lifeomic.com
ww1.lifeology.dev.lifeomic.com
www1.lifeology.dev.lifeomic.com
mx1.lifeology.dev.lifeomic.com
mail2.lifeology.dev.lifeomic.com
ks-vendingtransactions-mq2.lifeology.dev.lifeomic.com
ns2.lifeology.dev.lifeomic.com
dns2.lifeology.dev.lifeomic.com
www2.lifeology.dev.lifeomic.com
mx2.lifeology.dev.lifeomic.com
Right Ctrl


kali@kali: ~
File Actions Edit View Help
mx2.lifeology.dev.lifeomic.com
pop3.lifeology.dev.lifeomic.com
ks-vendingtransactions-mq3.lifeology.dev.lifeomic.com
ns3.lifeology.dev.lifeomic.com
ks-vendingtransactions-mq4.lifeology.dev.lifeomic.com
ns4.lifeology.dev.lifeomic.com
ipv6.lifeology.dev.lifeomic.com
a.lifeology.dev.lifeomic.com
ga.lifeology.dev.lifeomic.com
media.lifeology.dev.lifeomic.com
gcom-product-find-qa.lifeology.dev.lifeomic.com
cim-api-qa.lifeology.dev.lifeomic.com
searchportal-qa.lifeology.dev.lifeomic.com
gws-qa.lifeology.dev.lifeomic.com
cim-data-quality-qa.lifeology.dev.lifeomic.com
beta.lifeology.dev.lifeomic.com
okta.lifeology.dev.lifeomic.com
owa.lifeology.dev.lifeomic.com
b.lifeology.dev.lifeomic.com
collab.lifeology.dev.lifeomic.com
gitlab.lifeology.dev.lifeomic.com
db.lifeology.dev.lifeomic.com
mongodb.lifeology.dev.lifeomic.com
web.lifeology.dev.lifeomic.com
job.lifeology.dev.lifeomic.com
c.lifeology.dev.lifeomic.com
dc.lifeology.dev.lifeomic.com
basic.lifeology.dev.lifeomic.com
static.lifeology.dev.lifeomic.com
elastic.lifeology.dev.lifeomic.com
_dmarc.lifeology.dev.lifeomic.com
download.lifeology.dev.lifeomic.com
upload.lifeology.dev.lifeomic.com
old.lifeology.dev.lifeomic.com
kali@kali: ~
File Actions Edit View Help
old.lifeology.dev.lifeomic.com
inbound.lifeology.dev.lifeomic.com
pre-prod.lifeology.dev.lifeomic.com
non-prod.lifeology.dev.lifeomic.com
gac-rds-external-readonly-preprod.lifeology.dev.lifeomic.com
awsdashboard.lifeology.dev.lifeomic.com
cloud.lifeology.dev.lifeomic.com
office.lifeology.dev.lifeomic.com
voice.lifeology.dev.lifeomic.com
wfm-service.lifeology.dev.lifeomic.com
de.lifeology.dev.lifeomic.com
code.lifeology.dev.lifeomic.com
stage.lifeology.dev.lifeomic.com
edge.lifeology.dev.lifeomic.com
_collab-edge.lifeology.dev.lifeomic.com
exchange.lifeology.dev.lifeomic.com
mobile.lifeology.dev.lifeomic.com
cname.lifeology.dev.lifeomic.com
home.lifeology.dev.lifeomic.com
sitecore.lifeology.dev.lifeomic.com
store.lifeology.dev.lifeomic.com
pre.lifeology.dev.lifeomic.com
secure.lifeology.dev.lifeomic.com
certificate.lifeology.dev.lifeomic.com
liveupdate.lifeology.dev.lifeomic.com
remote.lifeology.dev.lifeomic.com
spf.lifeology.dev.lifeomic.com
autoconfig.lifeology.dev.lifeomic.com
img.lifeology.dev.lifeomic.com
staging.lifeology.dev.lifeomic.com
publishing-catalog.lifeology.dev.lifeomic.com
blog.lifeology.dev.lifeomic.com
auth.lifeology.dev.lifeomic.com
akamai.lifeology.dev.lifeomic.com
File Actions Edit View Help
akamai.lifeology.dev.lifeomic.com
wiki.lifeology.dev.lifeomic.com
api.lifeology.dev.lifeomic.com
ks-invoice-api.lifeology.dev.lifeomic.com
ks-program-api.lifeology.dev.lifeomic.com
cim-api.lifeology.dev.lifeomic.com
cdq-api.lifeology.dev.lifeomic.com
ks-order-api.lifeology.dev.lifeomic.com
vendor-api.lifeology.dev.lifeomic.com
ks-limits-api.lifeology.dev.lifeomic.com
ks-inventory-api.lifeology.dev.lifeomic.com
acapi.lifeology.dev.lifeomic.com
cveapi.lifeology.dev.lifeomic.com
gui.lifeology.dev.lifeomic.com
check.lifeology.dev.lifeomic.com
click.lifeology.dev.lifeomic.com
storybook.lifeology.dev.lifeomic.com
webhook.lifeology.dev.lifeomic.com
outlook.lifeology.dev.lifeomic.com
webdisk.lifeology.dev.lifeomic.com
uk.lifeology.dev.lifeomic.com
portal.lifeology.dev.lifeomic.com
searchportal.lifeology.dev.lifeomic.com
cpanel.lifeology.dev.lifeomic.com
mail.lifeology.dev.lifeomic.com
webmail.lifeology.dev.lifeomic.com
email.lifeology.dev.lifeomic.com
retail.lifeology.dev.lifeomic.com
ml.lifeology.dev.lifeomic.com
sql.lifeology.dev.lifeomic.com
mssql.lifeology.dev.lifeomic.com
mysql.lifeology.dev.lifeomic.com
ssl.lifeology.dev.lifeomic.com
_etcd-server-ssl.lifeology.dev.lifeomic.com


File Actions Edit View Help
_etcd-server-ssl.lifeology.dev.lifeomic.com
consul.lifeology.dev.lifeomic.com
m.lifeology.dev.lifeomic.com
iam.lifeology.dev.lifeomic.com
mdm.lifeology.dev.lifeomic.com
whm.lifeology.dev.lifeomic.com
dnm.lifeology.dev.lifeomic.com
crm.lifeology.dev.lifeomic.com
forum.lifeology.dev.lifeomic.com
cdn.lifeology.dev.lifeomic.com
en.lifeology.dev.lifeomic.com
httpbin.lifeology.dev.lifeomic.com
akamai-test-origin.lifeology.dev.lifeomic.com
login.lifeology.dev.lifeomic.com
_cuplogin.lifeology.dev.lifeomic.com
admin.lifeology.dev.lifeomic.com
signin.lifeology.dev.lifeomic.com
vpn.lifeology.dev.lifeomic.com
sslvpn.lifeology.dev.lifeomic.com
dyn.lifeology.dev.lifeomic.com
video.lifeology.dev.lifeomic.com
info.lifeology.dev.lifeomic.com
go.lifeology.dev.lifeomic.com
mongo.lifeology.dev.lifeomic.com
demo.lifeology.dev.lifeomic.com
sso.lifeology.dev.lifeomic.com
imap.lifeology.dev.lifeomic.com
wap.lifeology.dev.lifeomic.com
cp.lifeology.dev.lifeomic.com
_tcp.lifeology.dev.lifeomic.com
_cuplogin._tcp.lifeology.dev.lifeomic.com
_cisco-uds._tcp.lifeology.dev.lifeomic.com
ip.lifeology.dev.lifeomic.com
sip.lifeology.dev.lifeomic.com


File Actions Edit View Help
sip.lifeology.dev.lifeomic.com
help.lifeology.dev.lifeomic.com
shop.lifeology.dev.lifeomic.com
pop.lifeology.dev.lifeomic.com
app.lifeology.dev.lifeomic.com
danieapp.lifeology.dev.lifeomic.com
ftp.lifeology.dev.lifeomic.com
smtp.lifeology.dev.lifeomic.com
signup.lifeology.dev.lifeomic.com
wp.lifeology.dev.lifeomic.com
builder.lifeology.dev.lifeomic.com
docker.lifeology.dev.lifeomic.com
hostmaster.lifeology.dev.lifeomic.com
postmaster.lifeology.dev.lifeomic.com
autodiscover.lifeology.dev.lifeomic.com
server.lifeology.dev.lifeomic.com
mailserver.lifeology.dev.lifeomic.com
vendor.lifeology.dev.lifeomic.com
k8s.lifeology.dev.lifeomic.com
bbs.lifeology.dev.lifeomic.com
jobs.lifeology.dev.lifeomic.com
metrics.lifeology.dev.lifeomic.com
_cisco-uds.lifeology.dev.lifeomic.com
images.lifeology.dev.lifeomic.com
kubernetes.lifeology.dev.lifeomic.com
blogs.lifeology.dev.lifeomic.com
whois.lifeology.dev.lifeomic.com
nodejs.lifeology.dev.lifeomic.com
tools.lifeology.dev.lifeomic.com
tls.lifeology.dev.lifeomic.com
_tls.lifeology.dev.lifeomic.com
_collab-edge._tls.lifeology.dev.lifeomic.com
forums.lifeology.dev.lifeomic.com
ns.lifeology.dev.lifeomic.com



2 . SubDomainizer

SubDomainizer is a tool that searches for hidden subdomains and secrets in webpages, Github repositories, and external javascripts at a given URL. This program also extracts S3 buckets, cloudfront URLs, and other information from those JS files that may be useful, such as if an S3 bucket is open to read/write, or whether a subdomain has been taken over, and so on. It also examines the contents of a given folder containing your files.

Installation Steps

- Clone SubDomainzer from git:

git clone https://github.com/nsonaniya2010/SubDomainizer.git

- Change the directory:

cd SubDomainizer

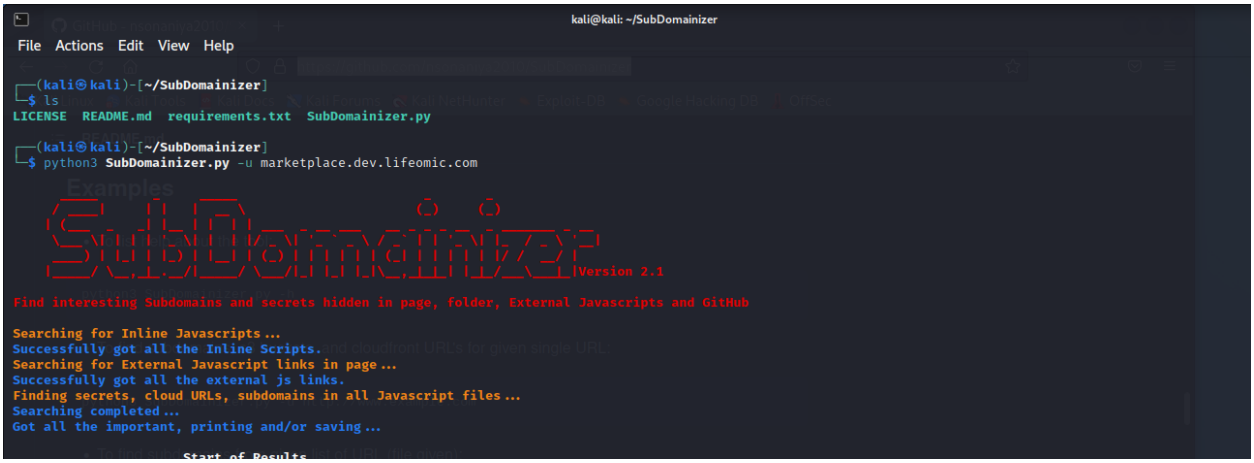
- Install the requirements:

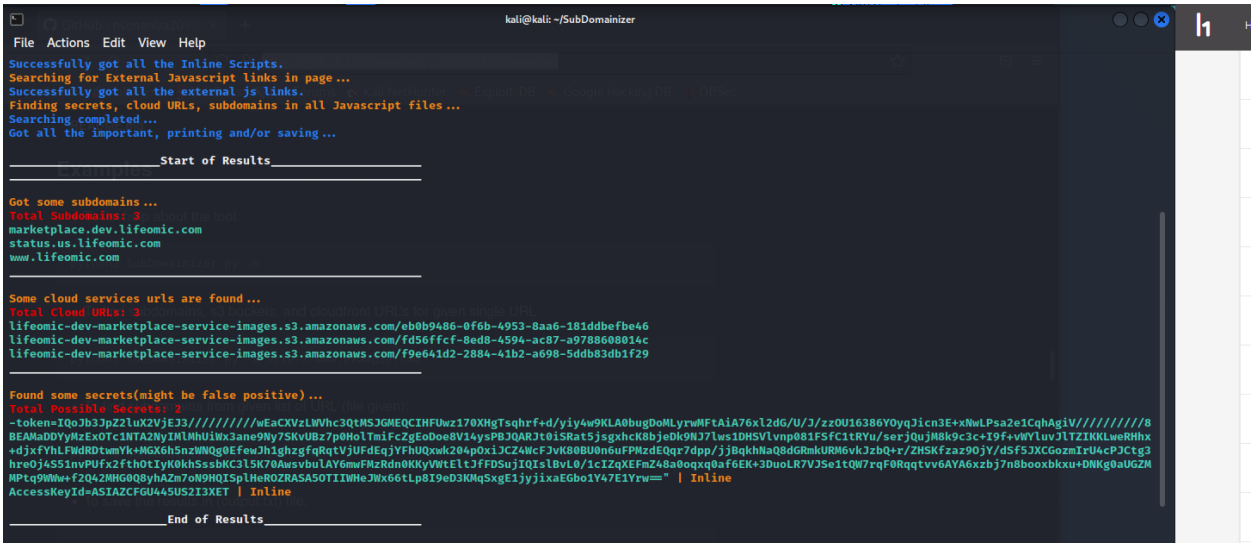
pip3 install -r requirements.txt

- Enjoy the Tool.

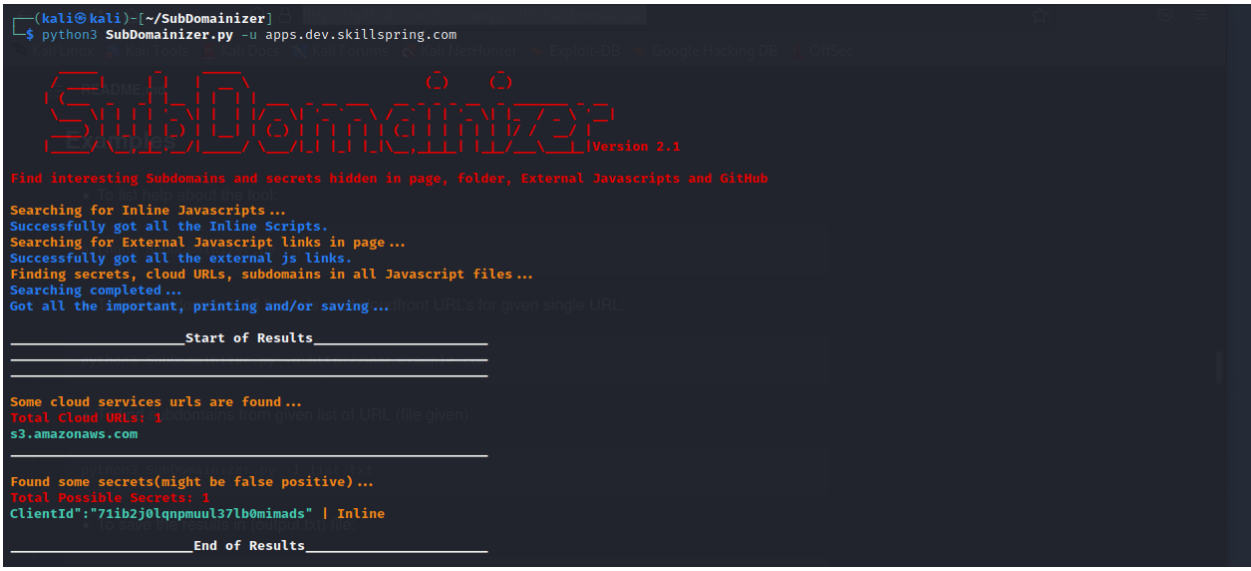
- Target Domain - marketplace.dev.lifeomic.com
- To run the tool on a target, just use the following command

    python3 SubDomainizer.py -u <Target domain>





- Target Domain - **apps.dev.skillspring.com**



3 . Bug Bounty hunting Tool (BBHT) by Nahamsec

Bug Bounty Hunting Tools is a script that installs the most often used tools for hunting for vulnerabilities in bug bounty programs.
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

installing

- 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

```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/nahamsec/bbht
Cloning into 'bbht'...
remote: Enumerating objects: 126, done.
remote: Total 126 (delta 0), reused 0 (delta 0), pack-reused 126
Receiving objects: 100% (126/126), 36.73 KiB | 376.00 KiB/s, done.
Resolving deltas: 100% (35/35), done.

┌──(kali㉿kali)-[~]
└─$ ls
bbht  Desktop  Documents  Downloads  go  Music  Pictures  Public  SubDomainizer  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cd bbht

┌──(kali㉿kali)-[~/bbht]
└─$ ls
install.sh  README.md

┌──(kali㉿kali)-[~/bbht]
└─$ chmod +x install.sh

┌──(kali㉿kali)-[~/bbht]
└─$ ./install.sh
[sudo] password for kali:
Hit:1 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease
Reading package lists ... Done
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Calculating upgrade ... Done
The following packages were automatically installed and are no longer required:
  gccgo-12 libdav1d5 libdrm-intel1 libgo-12-dev libgo21
Use 'sudo apt autoremove' to remove them.
```

```
installing dirsearch
Cloning into 'dirsearch'...
remote: Enumerating objects: 10714, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 10714 (delta 1), reused 0 (delta 0), pack-reused 10706
Receiving objects: 100% (10714/10714), 21.10 MiB | 3.47 MiB/s, done.
Resolving deltas: 100% (7045/7045), done.
done
installing lazys3
Cloning into 'lazys3'...
remote: Enumerating objects: 22, done.
remote: Total 22 (delta 0), reused 0 (delta 0), pack-reused 22
Receiving objects: 100% (22/22), 4.94 KiB | 1.65 MiB/s, done.
Resolving deltas: 100% (3/3), done.
done
installing virtual host discovery
Cloning into 'virtual-host-discovery'...
remote: Enumerating objects: 54, done.
remote: Total 54 (delta 0), reused 0 (delta 0), pack-reused 54
Receiving objects: 100% (54/54), 7.58 KiB | 1.89 MiB/s, done.
Resolving deltas: 100% (17/17), done.
done
installing sqlmap
Cloning into 'sqlmap-dev'...
remote: Enumerating objects: 717, done.
remote: Counting objects: 100% (717/717), done.
remote: Compressing objects: 100% (480/480), done.
remote: Total 717 (delta 244), reused 413 (delta 225), pack-reused 0
Receiving objects: 100% (717/717), 6.96 MiB | 3.57 MiB/s, done.
Resolving deltas: 100% (244/244), done.
done
installing knock.py
```

kali@kali: ~/bbht

File Actions Edit View Help

```
done



Done! All tools are set up in ~/tools
total 64
drwxr-xr-x 16 kali kali 4096 Jun  5 00:15 .
drwxr-xr-x 21 kali kali 4096 Jun  5 00:12 ..
drwxr-xr-x  4 kali kali 4096 Jun  5 00:15 asnlookup
drwxr-xr-x  5 kali kali 4096 Jun  5 00:15 crtndstry
drwxr-xr-x  7 kali kali 4096 Jun  5 00:14 dirsearch
drwxr-xr-x 10 kali kali 4096 Jun  5 00:11 JSParser
drwxr-xr-x  4 kali kali 4096 Jun  5 00:14 knock
drwxr-xr-x  3 kali kali 4096 Jun  5 00:14 lazyrecon
drwxr-xr-x  3 kali kali 4096 Jun  5 00:14 lazys3
drwxr-xr-x  9 kali kali 4096 Jun  5 00:14 massdns
drwxr-xr-x 14 kali kali 4096 Jun  5 00:21 SecLists
drwxr-xr-x 11 kali kali 4096 Jun  5 00:14 sqlmap-dev
drwxr-xr-x  4 kali kali 4096 Jun  5 00:11 Sublist3r
drwxr-xr-x  3 kali kali 4096 Jun  5 00:11 teh_s3_bucketeers
drwxr-xr-x  3 kali kali 4096 Jun  5 00:14 virtual-host-discovery
drwxr-xr-x  9 kali kali 4096 Jun  5 00:12 wpscan
One last time: don't forget to set up AWS credentials in ~/.aws/!

┌──(kali㉿kali)-[~/bbht]
└─$
```

4 . crt.sh

crt.sh is an online interface to the Certificate Transparency Logs, a distributed database.

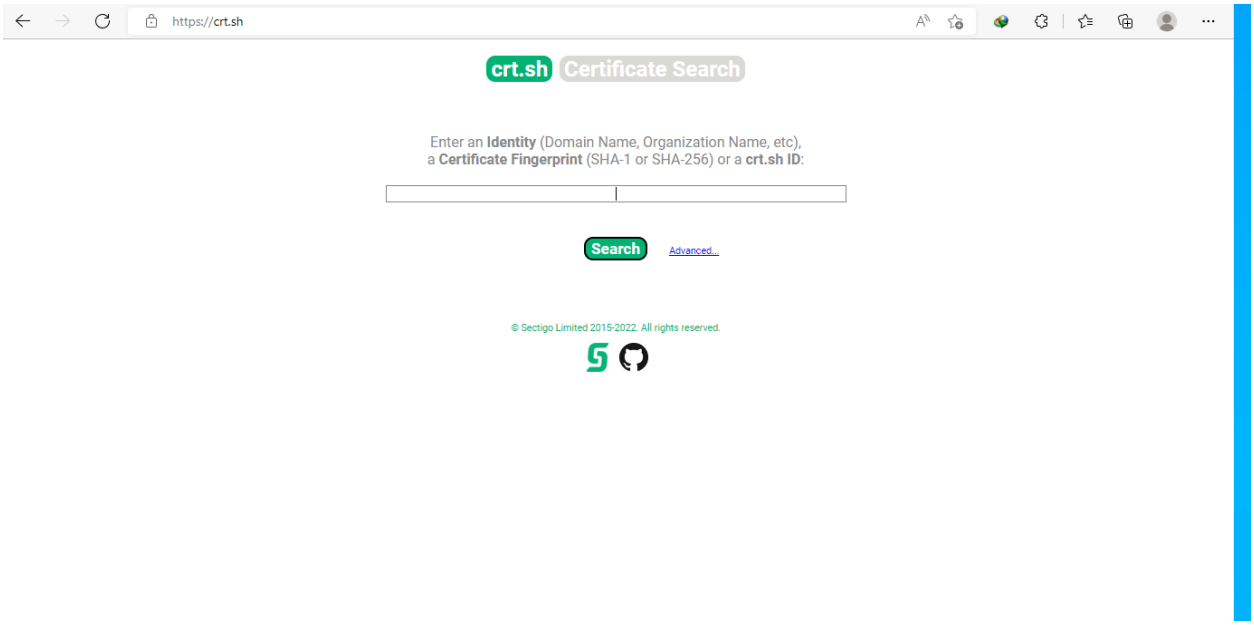
Crt.sh is a website where you can find all of the SSL or TLS certificates for a specific domain. In addition, the site's certificate monitoring is open-source.

The site is in a GUI style, making it very simple to obtain information, and the goal of the site is to maintain certificate records as clear as possible.

The certificate algorithms might also be found in ciphertext format. "Certificates.Saint Helena" is abbreviated as crt.sh.

Website link: https://crt.sh

I also used crt.sh for finding subdomains.



Target Domain - marketplace.dev.lifeomic.com

Criteria	Type: Identity Match: ILIKE Search: 'marketplace.dev.lifeomic.com'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
5408831467	2021-10-13	2021-10-04	2022-11-01	marketplace.dev.lifeomic.com	*.marketplace.dev.lifeomic.com marketplace.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5340404423	2021-10-04	2021-10-04	2022-11-01	marketplace.dev.lifeomic.com	*.marketplace.dev.lifeomic.com marketplace.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3843990024	2020-12-29	2020-11-03	2021-12-02	marketplace.dev.lifeomic.com	*.marketplace.dev.lifeomic.com marketplace.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3598980834	2020-11-03	2020-11-03	2021-12-02	marketplace.dev.lifeomic.com	*.marketplace.dev.lifeomic.com marketplace.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3598769278	2020-11-03	2020-11-03	2021-12-02	marketplace.dev.lifeomic.com	*.marketplace.dev.lifeomic.com marketplace.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon

Target Domain - lifeology.dev.lifeomic.com

Criteria	Type: Identity Match: ILIKE Search: 'lifeology.dev.lifeomic.com'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
5635141403	2021-11-18	2021-10-16	2022-11-13	lifeology.dev.lifeomic.com	*.lifeology.dev.lifeomic.com lifeology.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5423190384	2021-10-16	2021-10-16	2022-11-13	lifeology.dev.lifeomic.com	*.lifeology.dev.lifeomic.com lifeology.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3697828732	2020-11-26	2020-11-15	2021-12-14	lifeology.dev.lifeomic.com	*.lifeology.dev.lifeomic.com lifeology.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3648838887	2020-11-15	2020-11-15	2021-12-14	lifeology.dev.lifeomic.com	*.lifeology.dev.lifeomic.com lifeology.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
2621553401	2020-03-24	2019-12-13	2021-01-13	lifeology.dev.lifeomic.com	*.lifeology.dev.lifeomic.com lifeology.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
2187102073	2019-12-13	2019-12-13	2021-01-13	lifeology.dev.lifeomic.com	lifeology.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
2187101860	2019-12-13	2019-12-13	2021-01-13	lifeology.dev.lifeomic.com	*.lifeology.dev.lifeomic.com lifeology.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
2177669782	2019-12-11	2019-12-11	2021-01-11	lifeology.dev.lifeomic.com	*.lifeology.dev.lifeomic.com lifeology.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
2149789804	2019-11-26	2019-11-26	2020-12-26	lifeology.dev.lifeomic.com	*.lifeology.dev.lifeomic.com lifeology.dev.lifeomic.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon

Target Domain - apps.dev.skillspring.com

Criteria	Type: Identity Match: ILIKE Search: 'apps.dev.skillspring.com'

Certificates

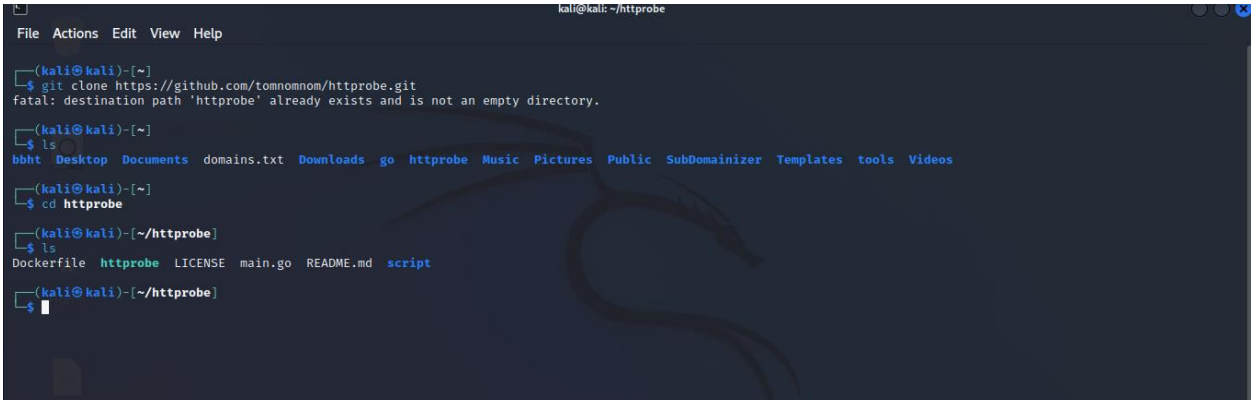
crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
6049939862	2022-01-26	2022-01-20	2023-02-18	apps.dev.lifeomic.com	*.apps.dev.skillspring.com apps.dev.skillspring.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
6013338484	2022-01-20	2022-01-20	2023-02-18	apps.dev.lifeomic.com	*.apps.dev.skillspring.com apps.dev.skillspring.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
4147666926	2021-03-01	2021-02-19	2022-03-20	apps.dev.lifeomic.com	*.apps.dev.skillspring.com apps.dev.skillspring.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
4101049492	2021-02-19	2021-02-19	2022-03-20	apps.dev.lifeomic.com	*.apps.dev.skillspring.com apps.dev.skillspring.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
4099630825	2021-02-18	2021-02-18	2022-03-19	apps.dev.lifeomic.com	*.apps.dev.skillspring.com apps.dev.skillspring.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon

- **Checking alive sub domains**

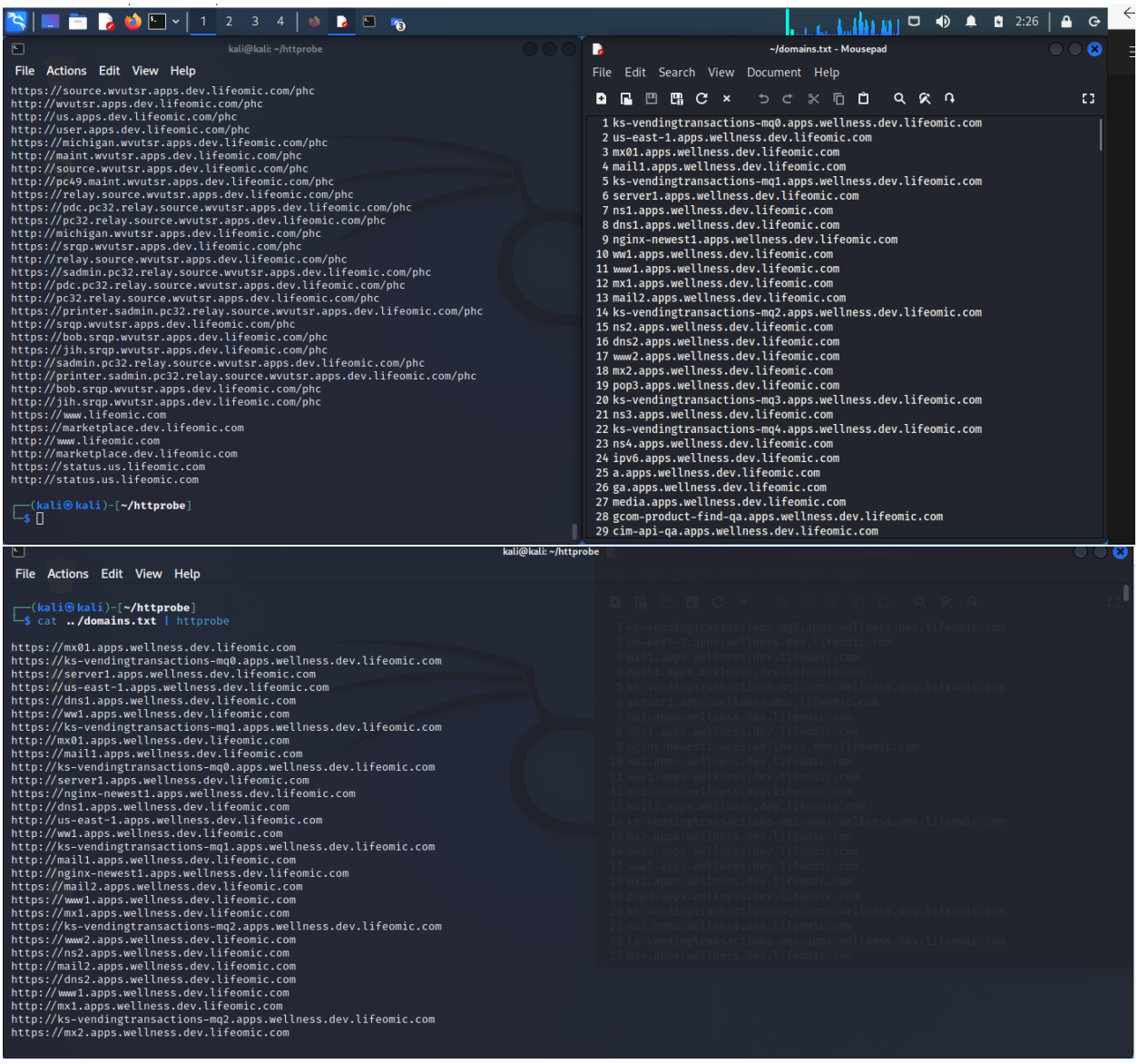
1 . Httprobe

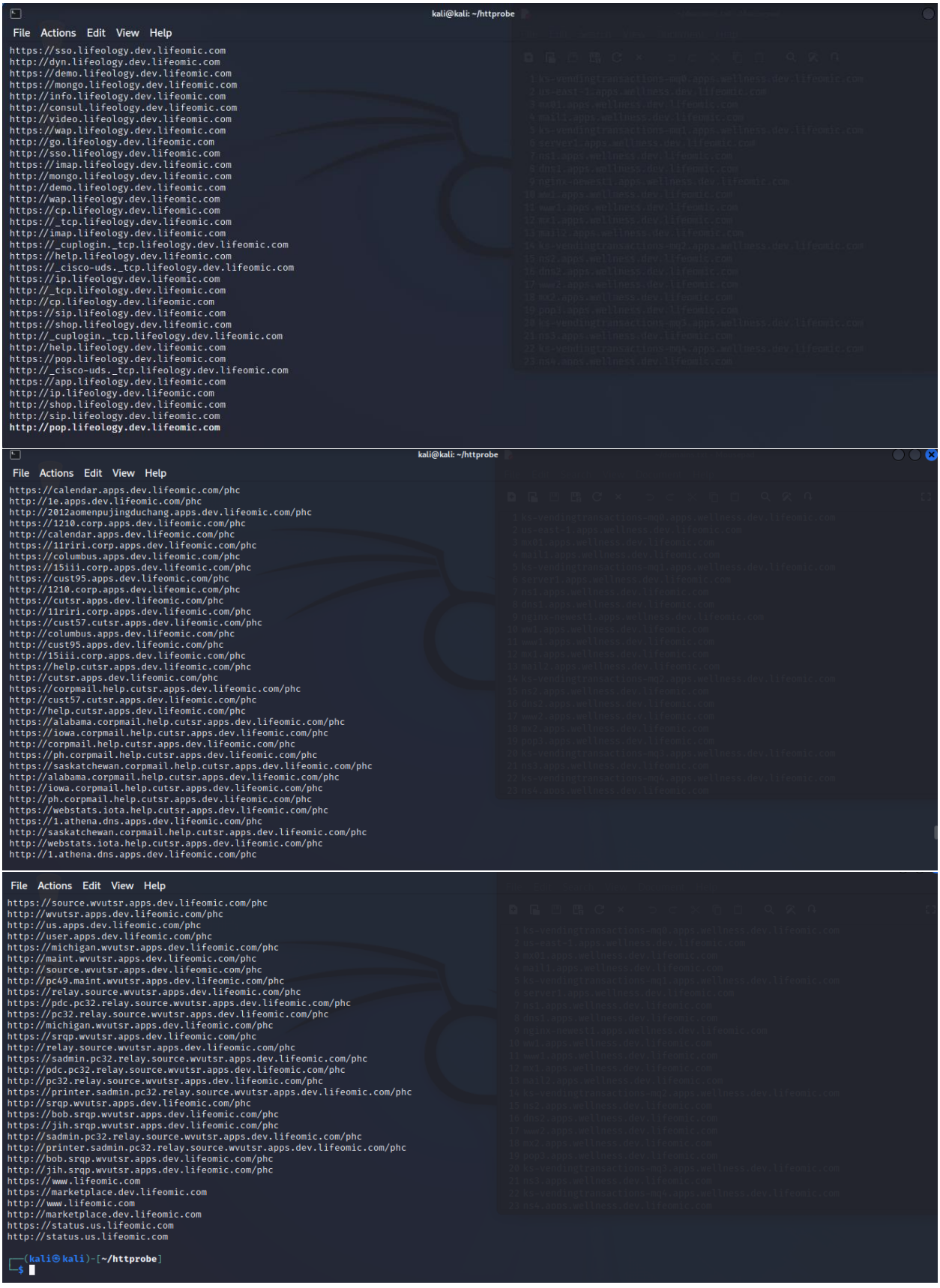
a tool for fast detecting active http and https servers. If you have a list of subdomains, you can use this tool to quickly see which ones are active. Tom Hudson developed Httprobe, which is accessible on Github.

Github link - GitHub - tomnomnom/httprobe



I saved all the sub-domains that I found to the text file called domains.
Then I run the tool to check live subdomains.




kali@kali: ~/httpprobe
File Actions Edit View Help
https://sso.lifeology.dev.lifeomic.com
http://dyn.lifeology.dev.lifeomic.com
https://demo.lifeology.dev.lifeomic.com
https://mongo.lifeology.dev.lifeomic.com
http://info.lifeology.dev.lifeomic.com
http://consul.lifeology.dev.lifeomic.com
http://video.lifeology.dev.lifeomic.com
https://wap.lifeology.dev.lifeomic.com
http://go.lifeology.dev.lifeomic.com
http://sso.lifeology.dev.lifeomic.com
https://imap.lifeology.dev.lifeomic.com
http://mongo.lifeology.dev.lifeomic.com
http://demo.lifeology.dev.lifeomic.com
http://wap.lifeology.dev.lifeomic.com
https://cp.lifeology.dev.lifeomic.com
https://_tcp.lifeology.dev.lifeomic.com
http://imap.lifeology.dev.lifeomic.com
https://_cuplogin._tcp.lifeology.dev.lifeomic.com
https://help.lifeology.dev.lifeomic.com
https://_cisco-uds._tcp.lifeology.dev.lifeomic.com
https://ip.lifeology.dev.lifeomic.com
http://_tcp.lifeology.dev.lifeomic.com
http://cp.lifeology.dev.lifeomic.com
https://sip.lifeology.dev.lifeomic.com
https://shop.lifeology.dev.lifeomic.com
http://_cuplogin._tcp.lifeology.dev.lifeomic.com
http://help.lifeology.dev.lifeomic.com
https://pop.lifeology.dev.lifeomic.com
http://_cisco-uds._tcp.lifeology.dev.lifeomic.com
https://app.lifeology.dev.lifeomic.com
http://ip.lifeology.dev.lifeomic.com
http://shop.lifeology.dev.lifeomic.com
http://sip.lifeology.dev.lifeomic.com
http://pop.lifeology.dev.lifeomic.com
kali@kali: ~/httpprobe
File Actions Edit View Help
https://calendar.apps.dev.lifeomic.com/phc
http://1e.apps.dev.lifeomic.com/phc
http://2012aomenpujingduchang.apps.dev.lifeomic.com/phc
https://1210.corp.apps.dev.lifeomic.com/phc
http://calendar.apps.dev.lifeomic.com/phc
https://11riri.corp.apps.dev.lifeomic.com/phc
https://columbus.apps.dev.lifeomic.com/phc
https://15iii.corp.apps.dev.lifeomic.com/phc
https://cust95.apps.dev.lifeomic.com/phc
http://1210.corp.apps.dev.lifeomic.com/phc
https://cutsr.apps.dev.lifeomic.com/phc
http://11riri.corp.apps.dev.lifeomic.com/phc
https://cust57.cutsr.apps.dev.lifeomic.com/phc
http://columbus.apps.dev.lifeomic.com/phc
http://cust95.apps.dev.lifeomic.com/phc
http://15iii.corp.apps.dev.lifeomic.com/phc
https://help.cutsr.apps.dev.lifeomic.com/phc
http://cutsr.apps.dev.lifeomic.com/phc
https://corpmail.help.cutsr.apps.dev.lifeomic.com/phc
http://cust57.cutsr.apps.dev.lifeomic.com/phc
http://help.cutsr.apps.dev.lifeomic.com/phc
https://alabama.corpmail.help.cutsr.apps.dev.lifeomic.com/phc
https://iowa.corpmail.help.cutsr.apps.dev.lifeomic.com/phc
http://corpmail.help.cutsr.apps.dev.lifeomic.com/phc
https://ph.corpmail.help.cutsr.apps.dev.lifeomic.com/phc
https://saskatchewan.corpmail.help.cutsr.apps.dev.lifeomic.com/phc
http://alabama.corpmail.help.cutsr.apps.dev.lifeomic.com/phc
http://iowa.corpmail.help.cutsr.apps.dev.lifeomic.com/phc
http://ph.corpmail.help.cutsr.apps.dev.lifeomic.com/phc
https://webstats.iota.help.cutsr.apps.dev.lifeomic.com/phc
https://1.athena.dns.apps.dev.lifeomic.com/phc
http://saskatchewan.corpmail.help.cutsr.apps.dev.lifeomic.com/phc
http://webstats.iota.help.cutsr.apps.dev.lifeomic.com/phc
http://1.athena.dns.apps.dev.lifeomic.com/phc
File Actions Edit View Help
https://source.wvutsr.apps.dev.lifeomic.com/phc
http://wvutsr.apps.dev.lifeomic.com/phc
http://us.apps.dev.lifeomic.com/phc
http://user.apps.dev.lifeomic.com/phc
https://michigan.wvutsr.apps.dev.lifeomic.com/phc
http://maint.wvutsr.apps.dev.lifeomic.com/phc
http://source.wvutsr.apps.dev.lifeomic.com/phc
http://pc49.maint.wvutsr.apps.dev.lifeomic.com/phc
https://relay.source.wvutsr.apps.dev.lifeomic.com/phc
https://pdc.pc32.relay.source.wvutsr.apps.dev.lifeomic.com/phc
https://pc32.relay.source.wvutsr.apps.dev.lifeomic.com/phc
http://michigan.wvutsr.apps.dev.lifeomic.com/phc
https://srqp.wvutsr.apps.dev.lifeomic.com/phc
http://relay.source.wvutsr.apps.dev.lifeomic.com/phc
https://sadmin.pc32.relay.source.wvutsr.apps.dev.lifeomic.com/phc
http://pdc.pc32.relay.source.wvutsr.apps.dev.lifeomic.com/phc
http://pc32.relay.source.wvutsr.apps.dev.lifeomic.com/phc
https://printer.sadmin.pc32.relay.source.wvutsr.apps.dev.lifeomic.com/phc
http://srqp.wvutsr.apps.dev.lifeomic.com/phc
https://bob.srqp.wvutsr.apps.dev.lifeomic.com/phc
https://jih.srqp.wvutsr.apps.dev.lifeomic.com/phc
http://sadmin.pc32.relay.source.wvutsr.apps.dev.lifeomic.com/phc
http://printer.sadmin.pc32.relay.source.wvutsr.apps.dev.lifeomic.com/phc
http://bob.srqp.wvutsr.apps.dev.lifeomic.com/phc
http://jih.srqp.wvutsr.apps.dev.lifeomic.com/phc
https://www.lifeomic.com
https://marketplace.dev.lifeomic.com
http://www.lifeomic.com
http://marketplace.dev.lifeomic.com
https://status.us.lifeomic.com
http://status.us.lifeomic.com
(kali㉿kali)-[~/httpprobe]
$

- **Gathering Achieved details**

1 . wayback machine

See Wayback Machine (Peabody's Improbable History) for the time machine from Peabody's Improbable History. The Internet Archive, a nonprofit library located in San Francisco, created the Wayback Machine as a digital archive of the World Wide Web. It allows users to "go back in time" to view how websites appeared in the past.

This is quite useful for information collecting since it allows us to discover some intriguing facts.

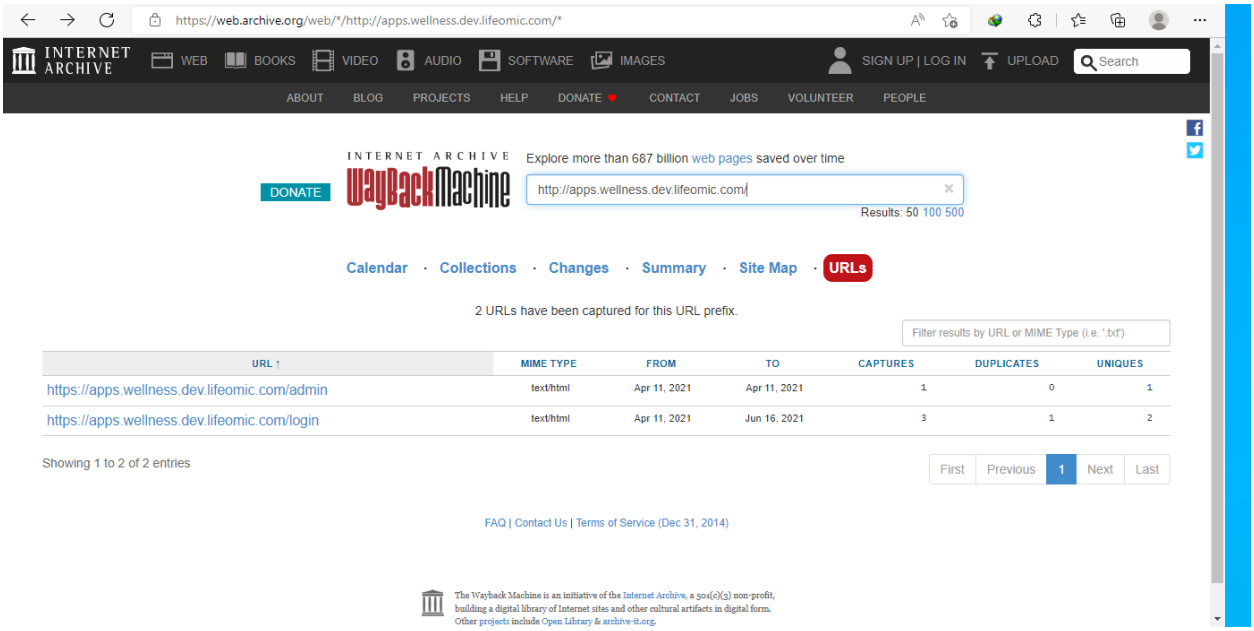
as an example,

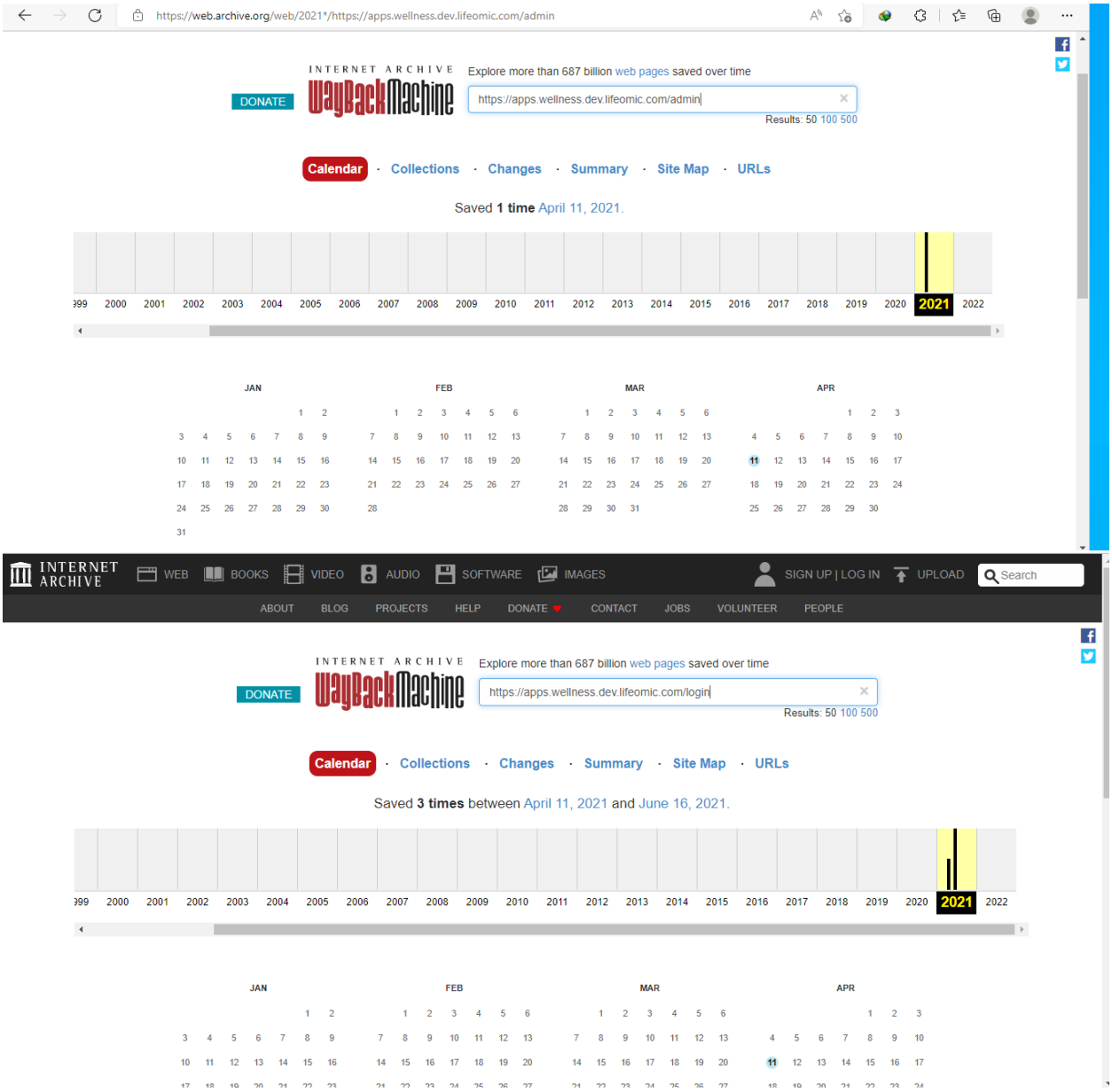
• Endpoints that have been ignored for a long time

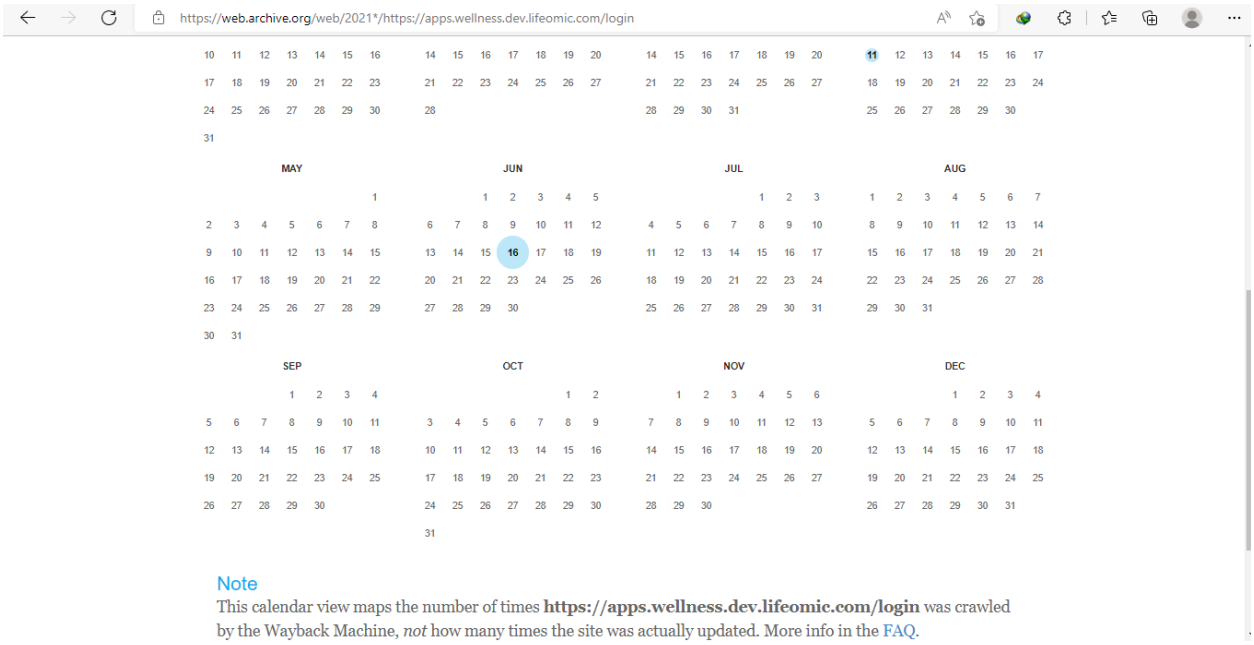
• JS files of interest

• Confidential information

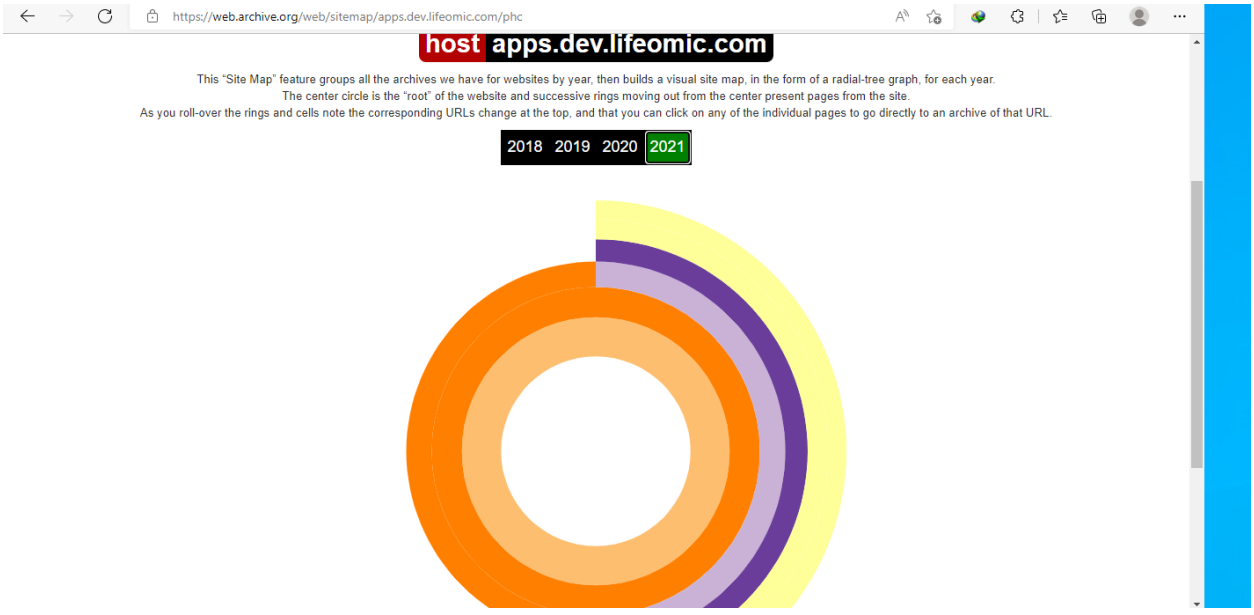
domain - https://apps.wellness.dev.lifeomic.com



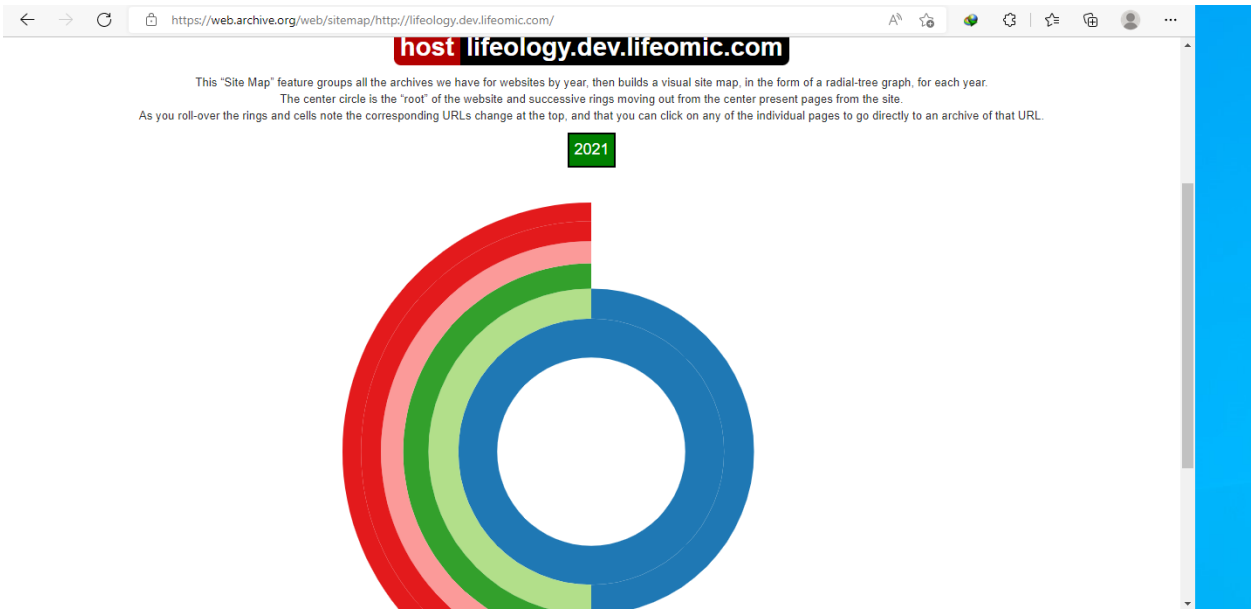

https://web.archive.org/web/2021*/https://apps.wellness.dev.lifeomic.com/admin
INTERNET ARCHIVE
WayBackMachine
DONATE
Explore more than 687 billion web pages saved over time
https://apps.wellness.dev.lifeomic.com/admin
Results: 50 100 500
Calendar · Collections · Changes · Summary · Site Map · URLs
Saved 1 time April 11, 2021.
999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022
JAN
FEB
MAR
APR
INTERNET ARCHIVE
WEB BOOKS VIDEO AUDIO SOFTWARE IMAGES
SIGN UP | LOG IN UPLOAD
Search
ABOUT BLOG PROJECTS HELP DONATE CONTACT JOBS VOLUNTEER PEOPLE
INTERNET ARCHIVE
WayBackMachine
DONATE
Explore more than 687 billion web pages saved over time
https://apps.wellness.dev.lifeomic.com/login
Results: 50 100 500
Calendar · Collections · Changes · Summary · Site Map · URLs
Saved 3 times between April 11, 2021 and June 16, 2021.
999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022
JAN
FEB
MAR
APR



Domain - **apps.dev.lifeomic.com/phc**



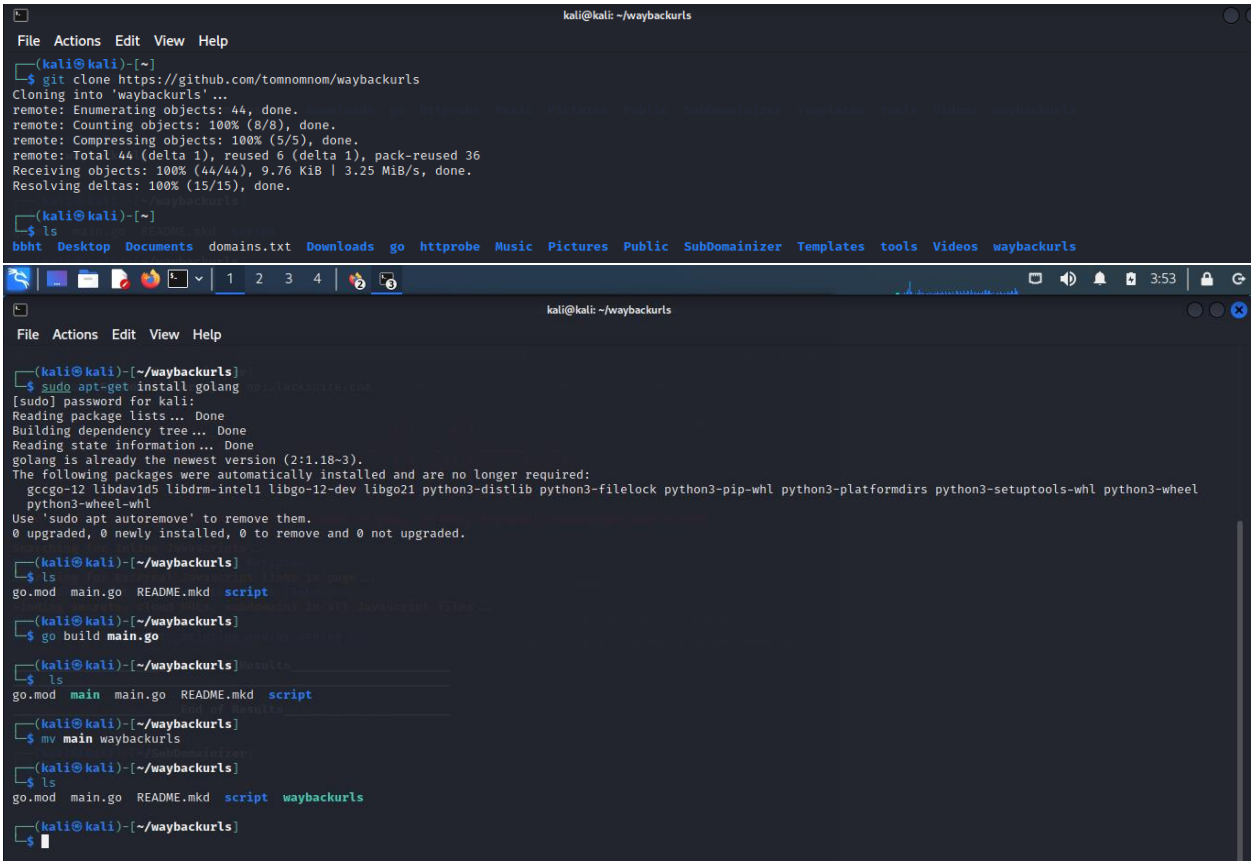
Domain - https://lifeology.dev.lifeomic.com



2 . Wayback URLs

Waybackurls is a Golang-based script or tool that crawls domains on stdin, fetches known URLs from Wayback Machines, also known as Archives, and outputs them to stdout. Note that because Waybackurls is a Golang-based utility, you must have a Golang environment installed on your machine.

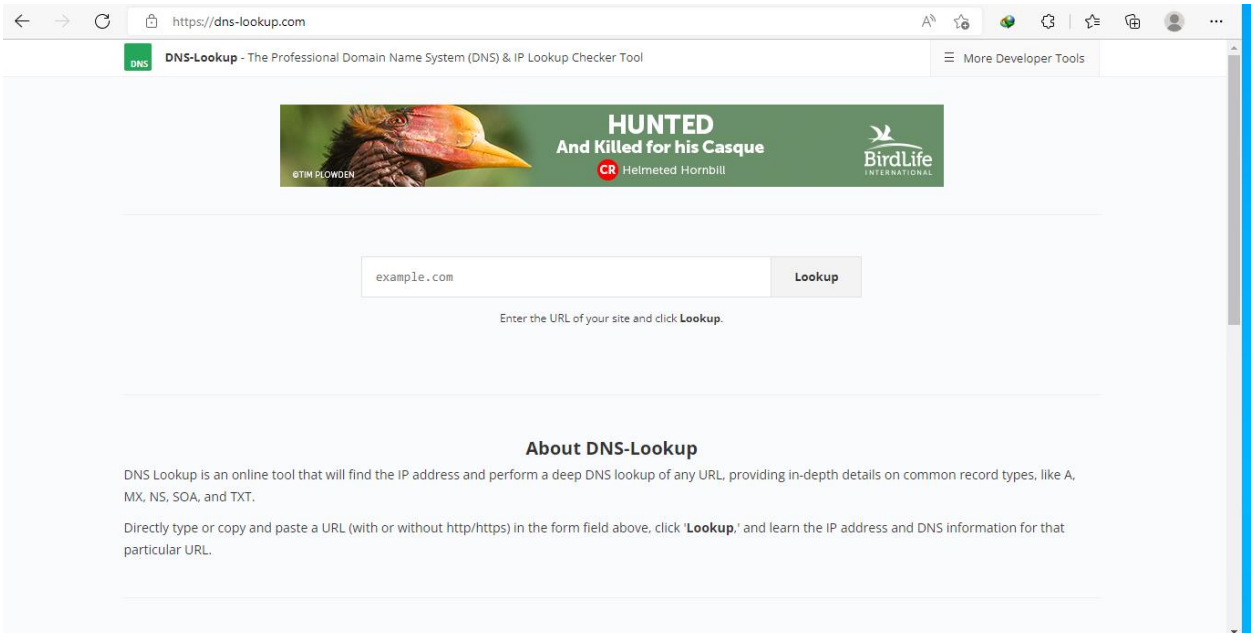
Github link: https://github.com/tomnomnom/waybackurls



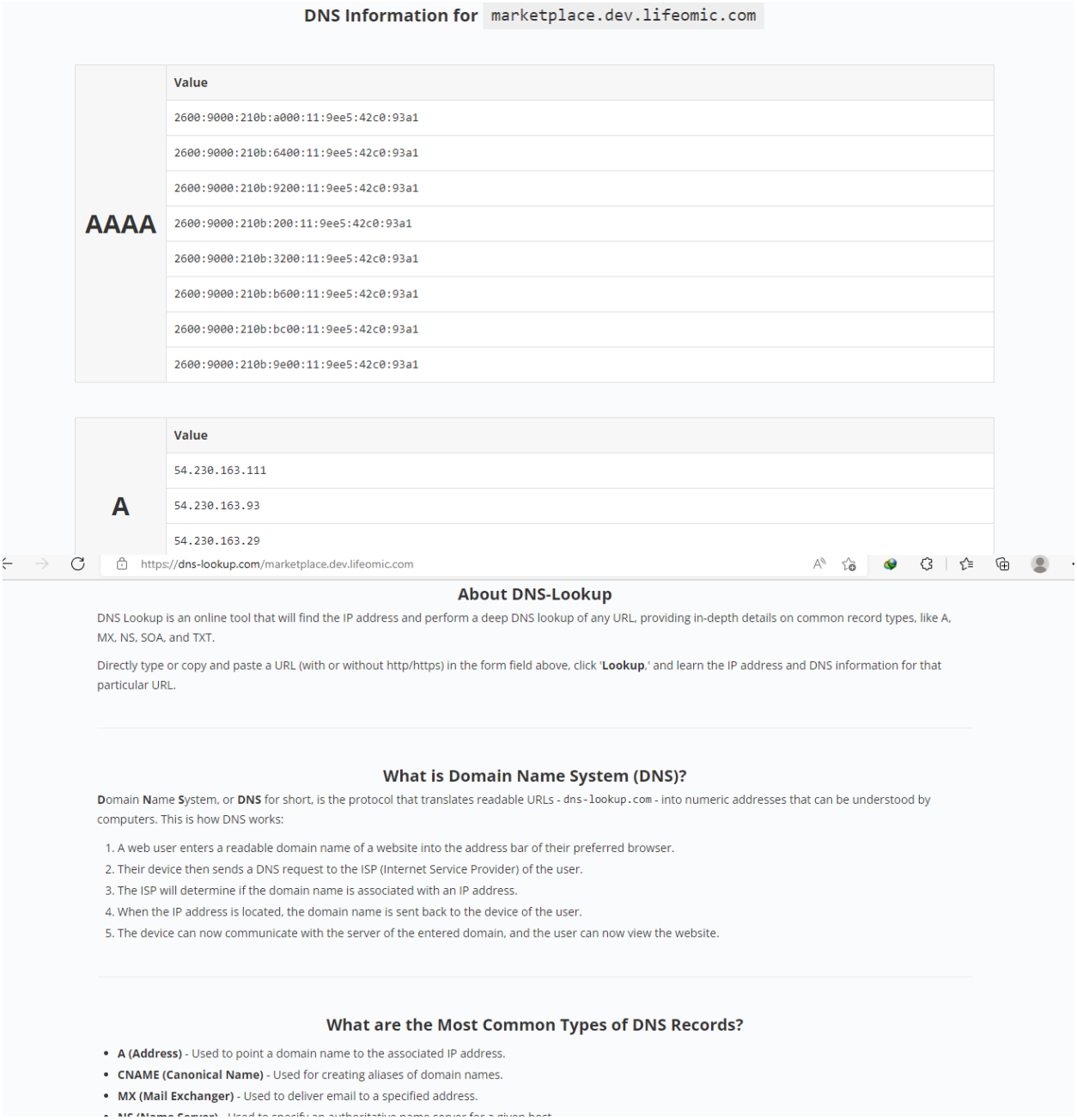
DNS Enumeration

1 . DNS lookup

DNS Lookup is an online application that will locate an IP address and do a deep DNS lookup on any URL, offering detailed information on popular record types such as A, MX, NS, SOA, and TXT.



Domain – marketplace.dev.lifeomic.com



DNS Information for `marketplace.dev.lifeomic.com`

	Value
AAAA	2600:9000:210b:a000:11:9ee5:42c0:93a1
	2600:9000:210b:6400:11:9ee5:42c0:93a1
	2600:9000:210b:9200:11:9ee5:42c0:93a1
	2600:9000:210b:200:11:9ee5:42c0:93a1
	2600:9000:210b:3200:11:9ee5:42c0:93a1
	2600:9000:210b:b600:11:9ee5:42c0:93a1
	2600:9000:210b:bc00:11:9ee5:42c0:93a1
	2600:9000:210b:9e00:11:9ee5:42c0:93a1

	Value
A	54.230.163.111
	54.230.163.93
	54.230.163.29

https://dns-lookup.com/marketplace.dev.lifeomic.com

About DNS-Lookup

DNS Lookup is an online tool that will find the IP address and perform a deep DNS lookup of any URL, providing in-depth details on common record types, like A, MX, NS, SOA, and TXT.

Directly type or copy and paste a URL (with or without http/https) in the form field above, click '**Lookup**,' and learn the IP address and DNS information for that particular URL.

What is Domain Name System (DNS)?

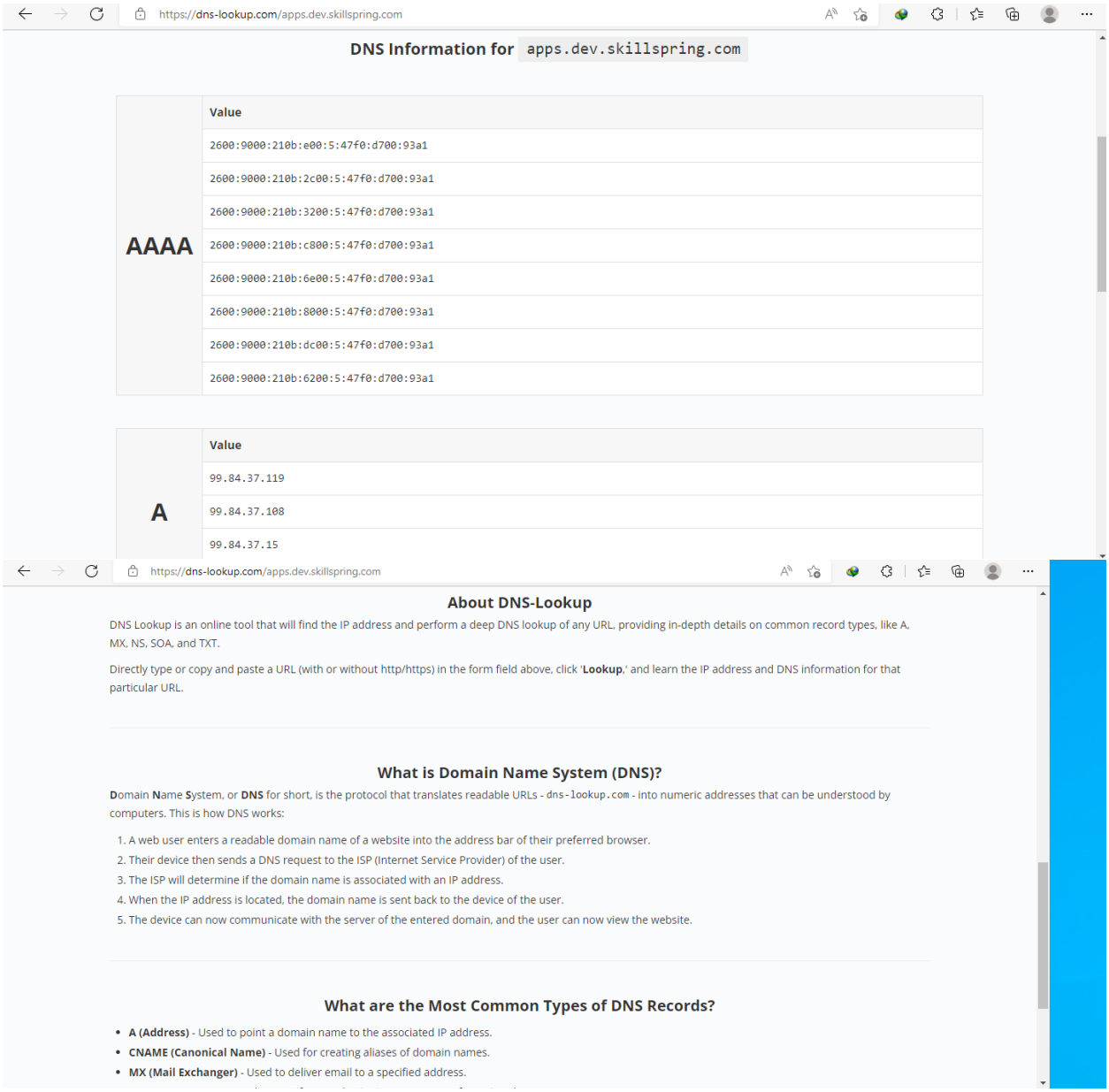
Domain **N**ame **S**ystem, or **DNS** for short, is the protocol that translates readable URLs - `dns-lookup.com` - into numeric addresses that can be understood by computers. This is how DNS works:

1. A web user enters a readable domain name of a website into the address bar of their preferred browser.
2. Their device then sends a DNS request to the ISP (Internet Service Provider) of the user.
3. The ISP will determine if the domain name is associated with an IP address.
4. When the IP address is located, the domain name is sent back to the device of the user.
5. The device can now communicate with the server of the entered domain, and the user can now view the website.

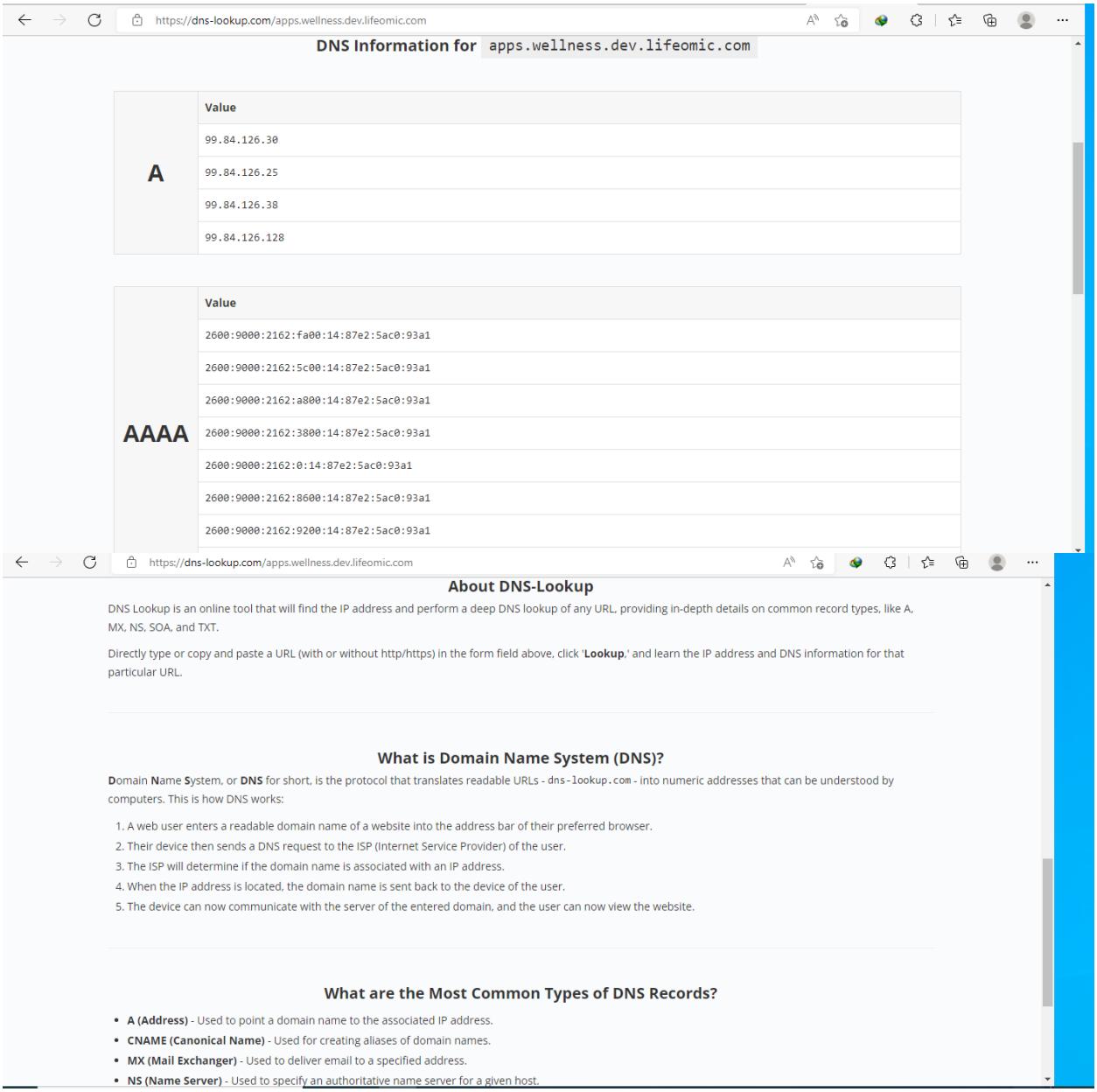
What are the Most Common Types of DNS Records?

- **A (Address)** - Used to point a domain name to the associated IP address.
- **CNAME (Canonical Name)** - Used for creating aliases of domain names.
- **MX (Mail Exchanger)** - Used to deliver email to a specified address.

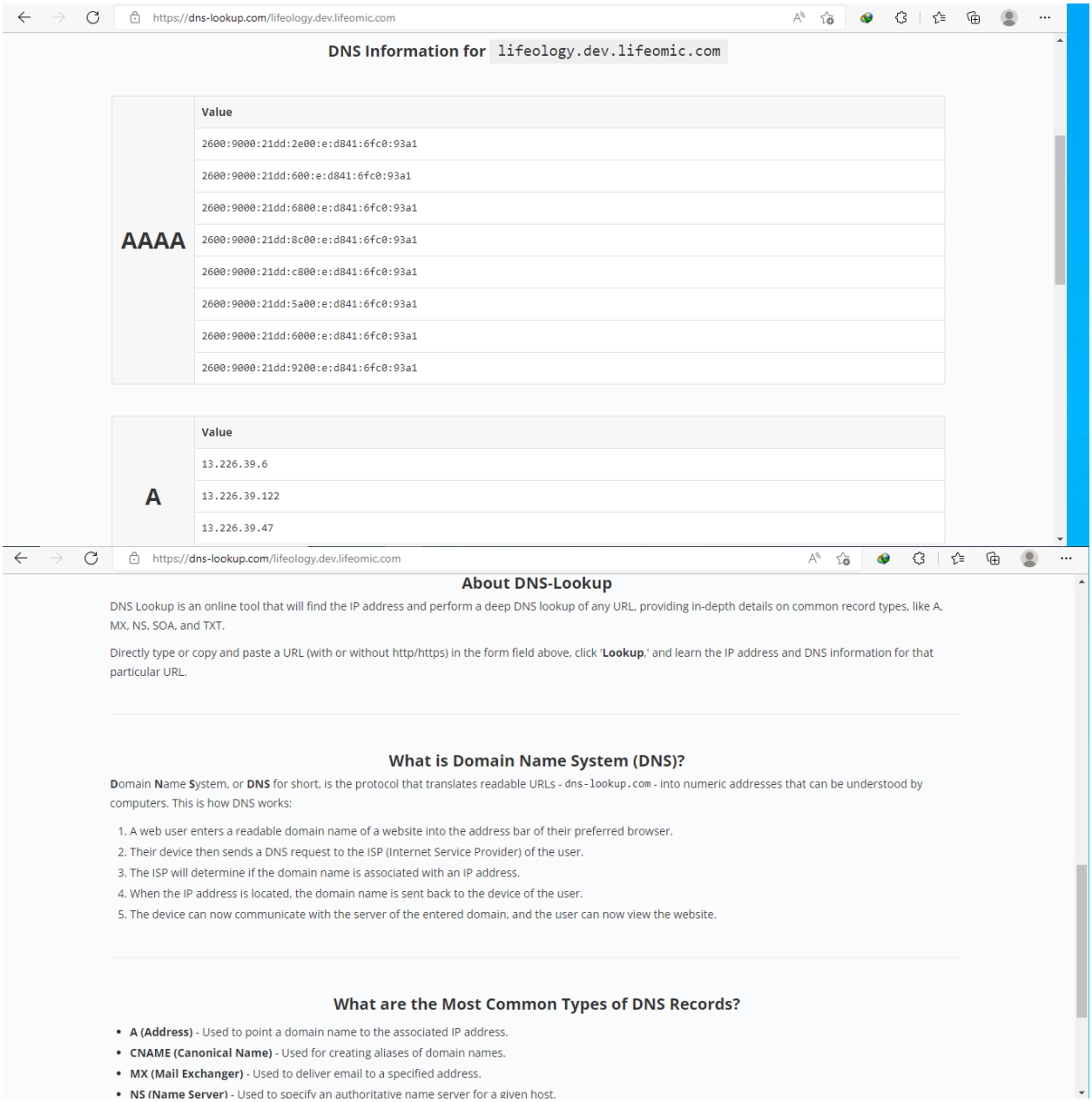
Domain – apps.dev.skillspring.com



Domain – https://apps.wellness.dev.lifeomic.com



Domain – https://lifeology.dev.lifeomic.com



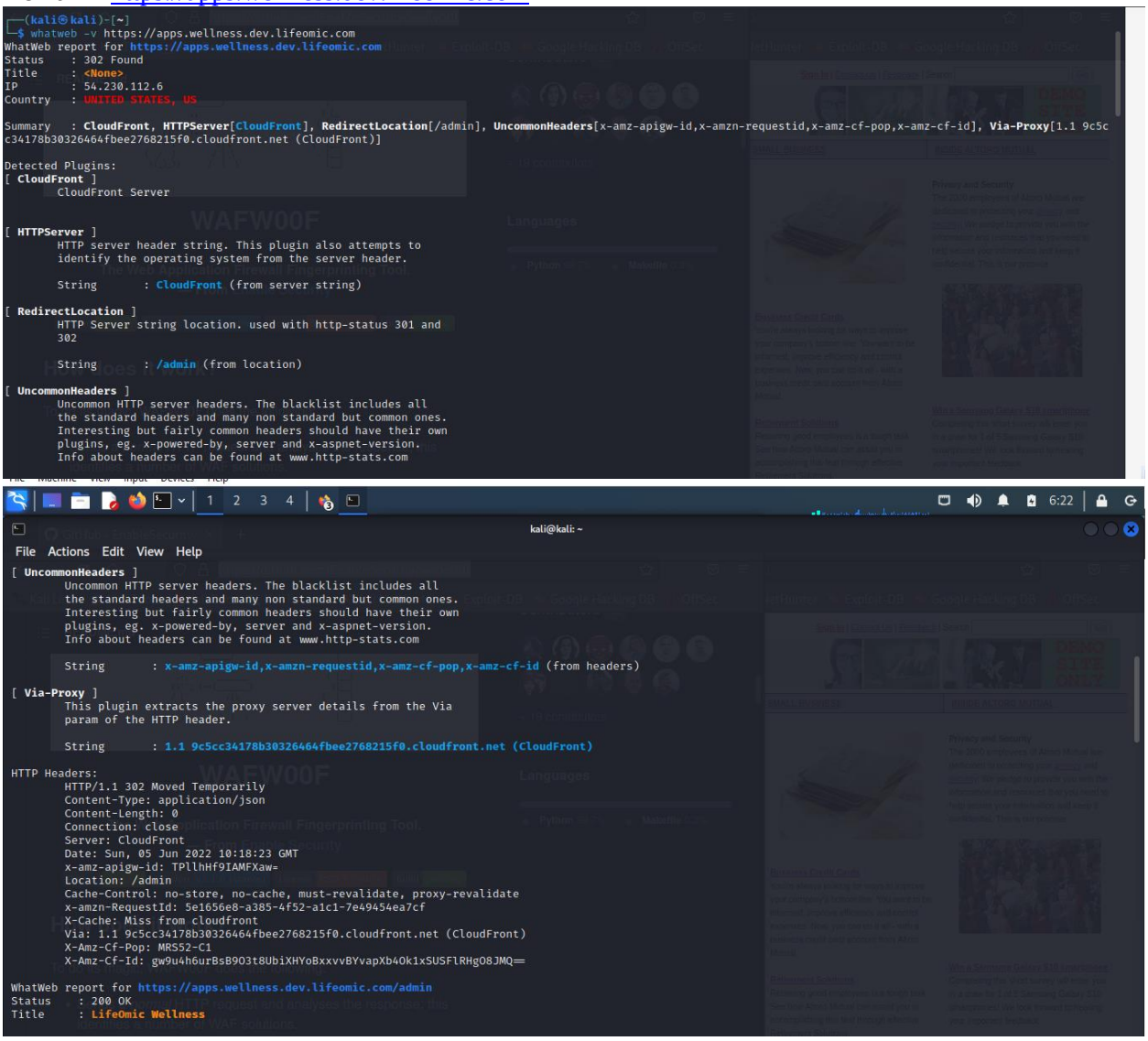
Domain - **apps.dev.lifeomic.com/phc**
No results

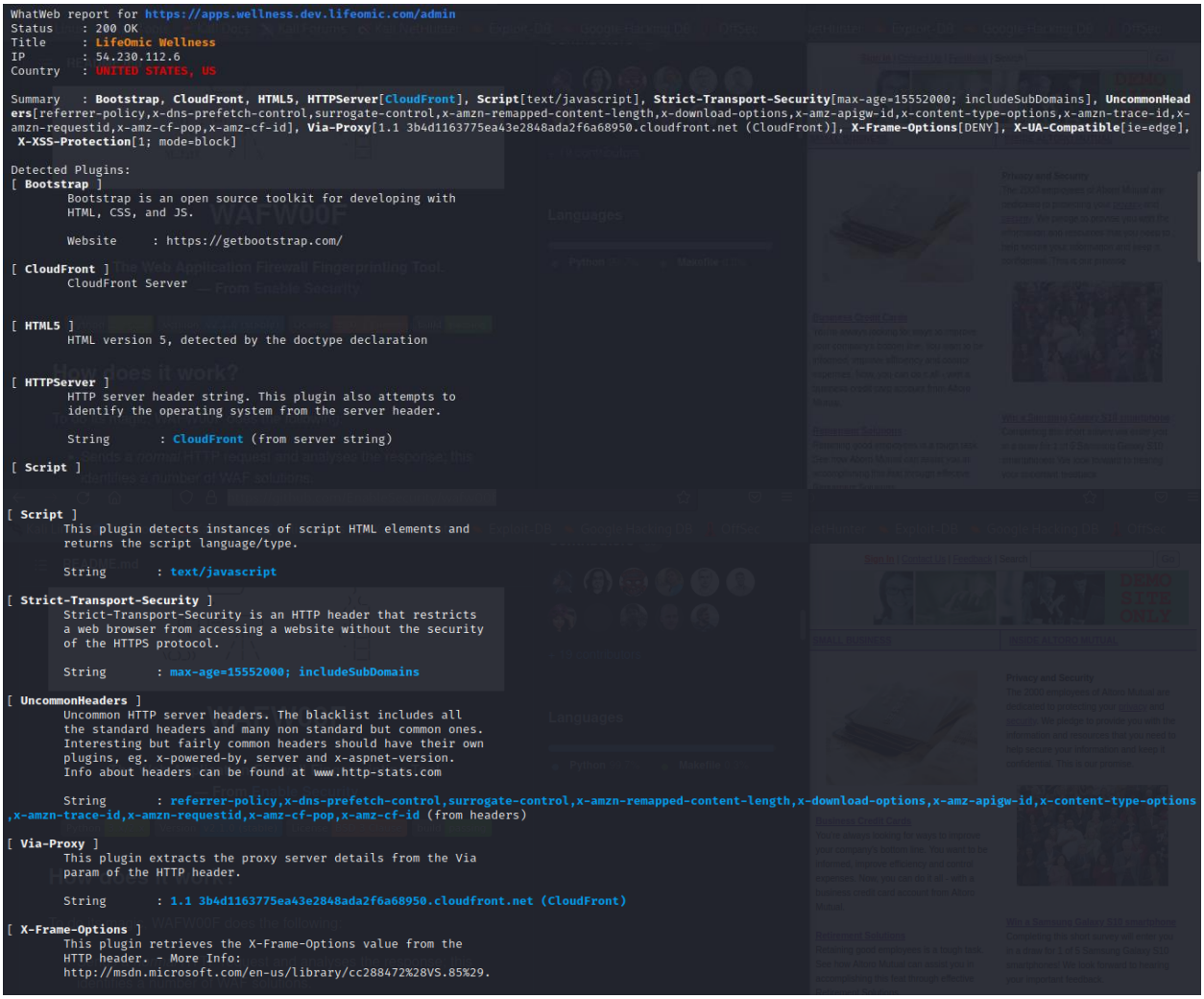
2 . Whatweb

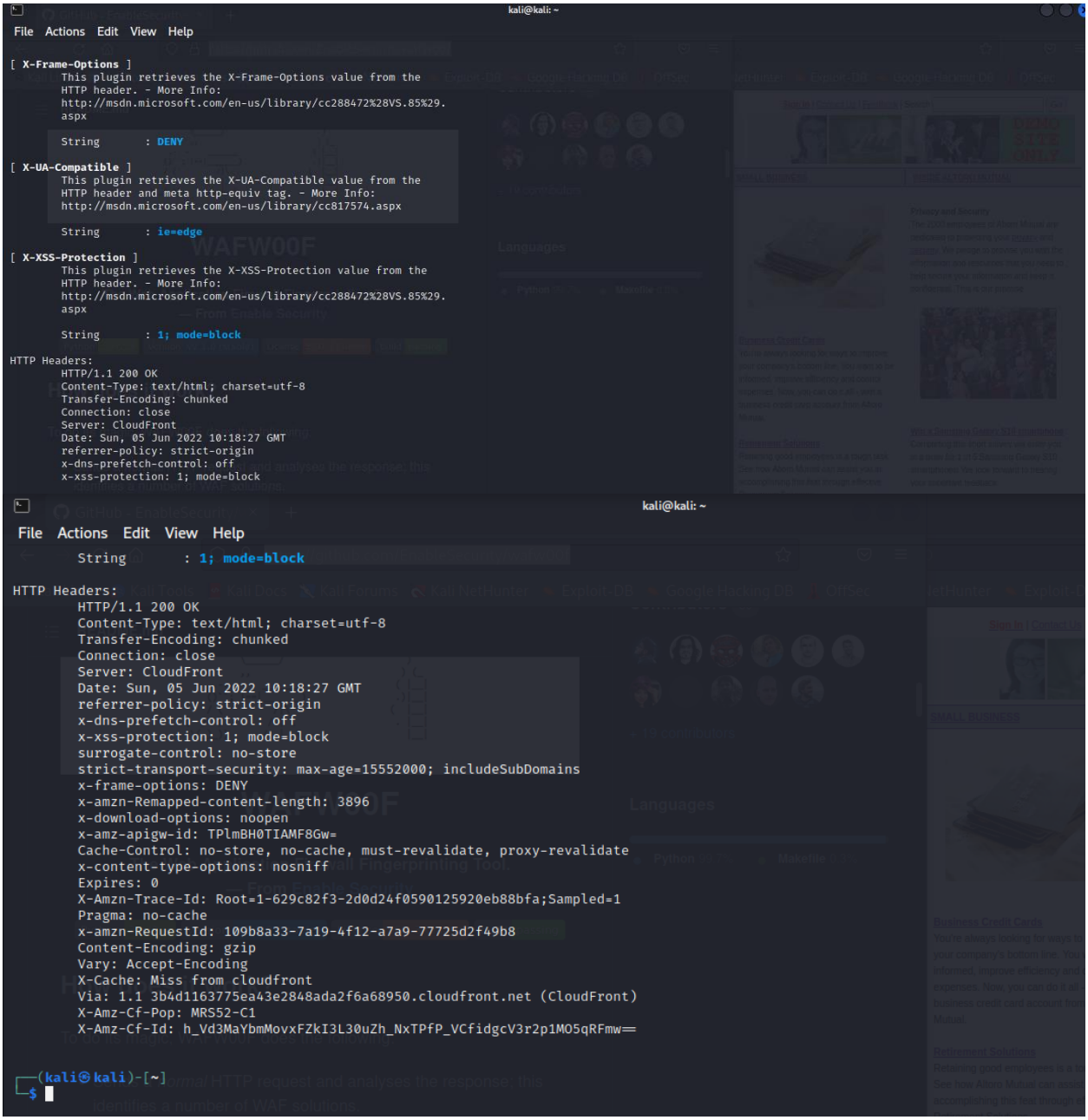
Whatweb is a Ruby-based scanning application. This program can recognize and identify all of the web technologies on the target website. This program can detect technologies such as blogging, content management systems, and any JavaScript libraries used by websites.

Use whatweb –V <domain name> command to perform whatweb aggression for selected domains.

Domain - https://apps.wellness.dev.lifeomic.com




WhatWeb report for https://apps.wellness.dev.lifeomic.com/admin
Status : 200 OK
Title : LifeOmic Wellness
IP : 54.230.112.6
Country : UNITED STATES, US
Summary : Bootstrap, CloudFront, HTML5, HTTPServer[CloudFront], Script[text/javascript], Strict-Transport-Security[max-age=15552000; includeSubDomains], UncommonHeaders[referrer-policy,x-dns-prefetch-control,surrogate-control,x-amzn-remapped-content-length,x-download-options,x-amz-apigw-id,x-content-type-options,x-amzn-trace-id,x-amzn-requestid,x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 3b4d1163775ea43e2848ada2f6a68950.cloudfront.net (CloudFront)], X-Frame-Options[DENY], X-UA-Compatible[ie=edge], X-XSS-Protection[1; mode=block]
Detected Plugins:
[Bootstrap]
Bootstrap is an open source toolkit for developing with HTML, CSS, and JS.
Website : https://getbootstrap.com/
[CloudFront]
CloudFront Server
[HTML5]
HTML version 5, detected by the doctype declaration
[HTTPServer]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.
String : CloudFront (from server string)
[Script]
[Script]
This plugin detects instances of script HTML elements and returns the script language/type.
String : text/javascript
[Strict-Transport-Security]
Strict-Transport-Security is an HTTP header that restricts a web browser from accessing a website without the security of the HTTPS protocol.
String : max-age=15552000; includeSubDomains
[UncommonHeaders]
Uncommon HTTP server headers. The blacklist includes all the standard headers and many non standard but common ones. Interesting but fairly common headers should have their own plugins, eg. x-powered-by, server and x-aspnet-version. Info about headers can be found at www.http-stats.com
String : referrer-policy,x-dns-prefetch-control,surrogate-control,x-amzn-remapped-content-length,x-download-options,x-amz-apigw-id,x-content-type-options,x-amzn-trace-id,x-amzn-requestid,x-amz-cf-pop,x-amz-cf-id (from headers)
[Via-Proxy]
This plugin extracts the proxy server details from the Via param of the HTTP header.
String : 1.1 3b4d1163775ea43e2848ada2f6a68950.cloudfront.net (CloudFront)
[X-Frame-Options]
This plugin retrieves the X-Frame-Options value from the HTTP header. - More Info:
http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.



Find the target domain has firewall protection

1 . Wafw00f

Application fingerprinting, information gathering, penetration testing, reconnaissance, and security assessment are all frequent uses for wafw00f. Pentesters and security professionals are the intended users of this program. Review and comments about the tool.

Git hub link - https://github.com/EnableSecurity/wafw00f.git

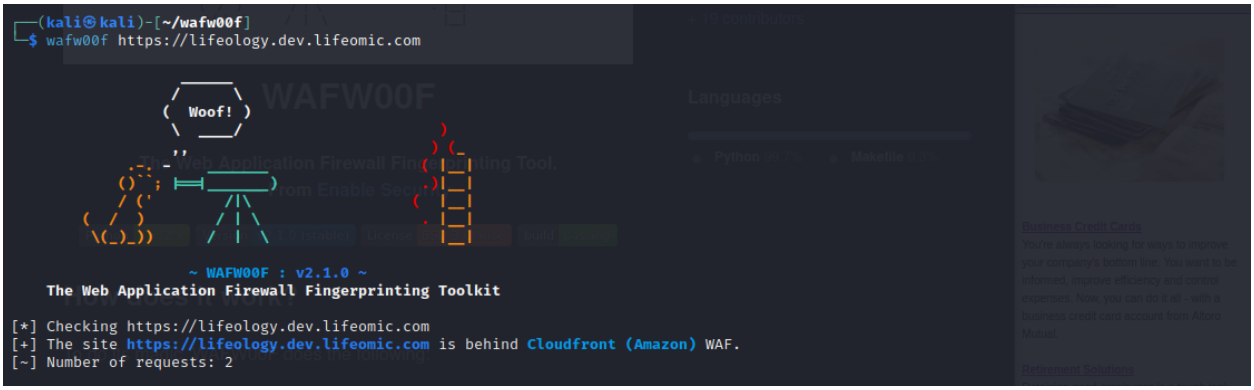
```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/EnableSecurity/wafw00f
Cloning into 'wafw00f'...
remote: Enumerating objects: 4213, done.
remote: Counting objects: 100% (74/74), done.
remote: Compressing objects: 100% (44/44), done.
remote: Total 4213 (delta 43), reused 53 (delta 30), pack-reused 4139
Receiving objects: 100% (4213/4213), 644.91 KiB | 1.26 MiB/s, done.
Resolving deltas: 100% (3064/3064), done.
```

```
┌──(kali㉿kali)-[~/wafw00f]
└─$ wafw00f

                ( W00f! )
                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

Usage: wafw00f url1 [url2 [url3 ... ]]
example: wafw00f http://www.victim.org/
```

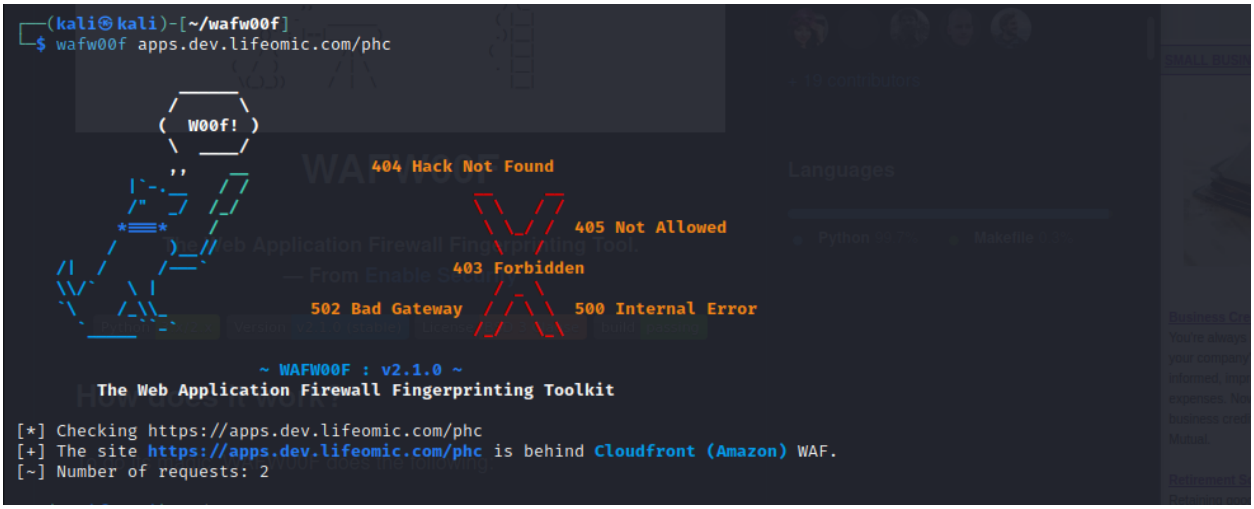
Domain – https://apps.wellness.dev.lifeomic.com

```
┌──(kali㉿kali)-[~/wafw00f]
└─$ wafw00f https://apps.wellness.dev.lifeomic.com

                ( W00f! )
                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://apps.wellness.dev.lifeomic.com
[+] The site https://apps.wellness.dev.lifeomic.com is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2
```

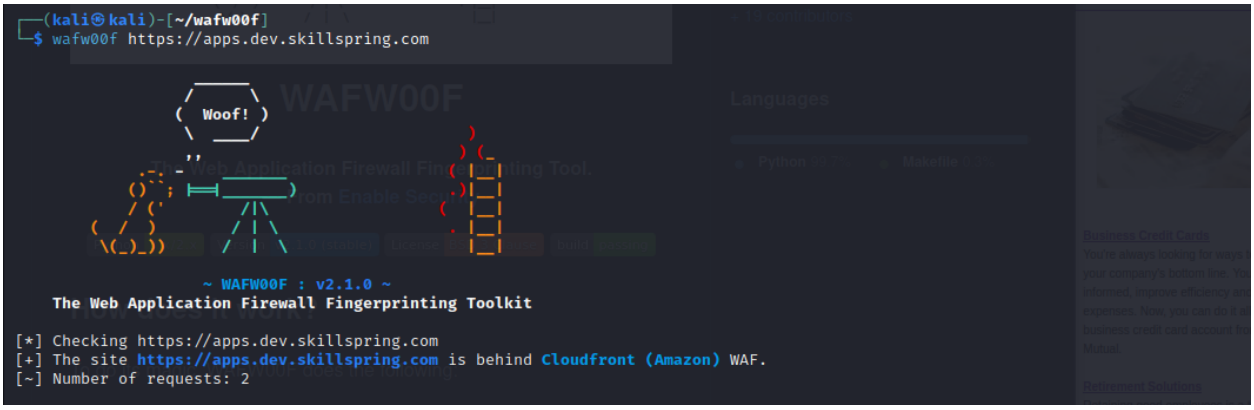
Domain – https://lifeology.dev.lifeomic.com



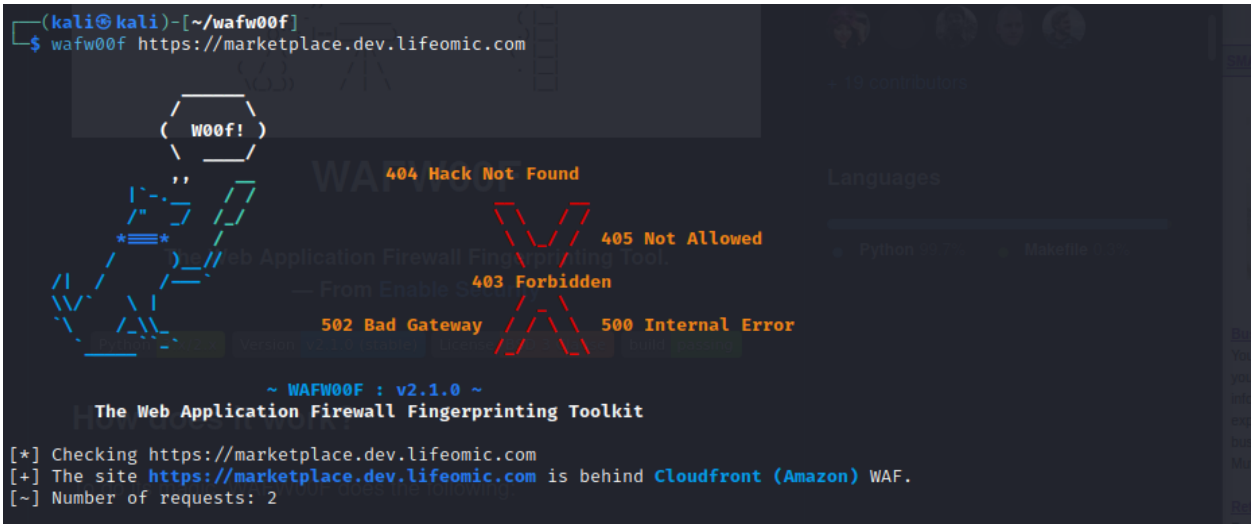
Domain –**_apps.dev.lifeomic.com/phc**



Domain –**_apps.dev.skillspring.com**



Domain –**_marketplace.dev.lifeomic.com**



Vulnerability Assesment

Assessment of Vulnerability It refers to the process of finding, categorizing, and prioritizing computer system, web application, digital asset, and network infrastructure vulnerabilities. It entails a thorough examination of numerous security validations in order to identify problems in pre-existing code.

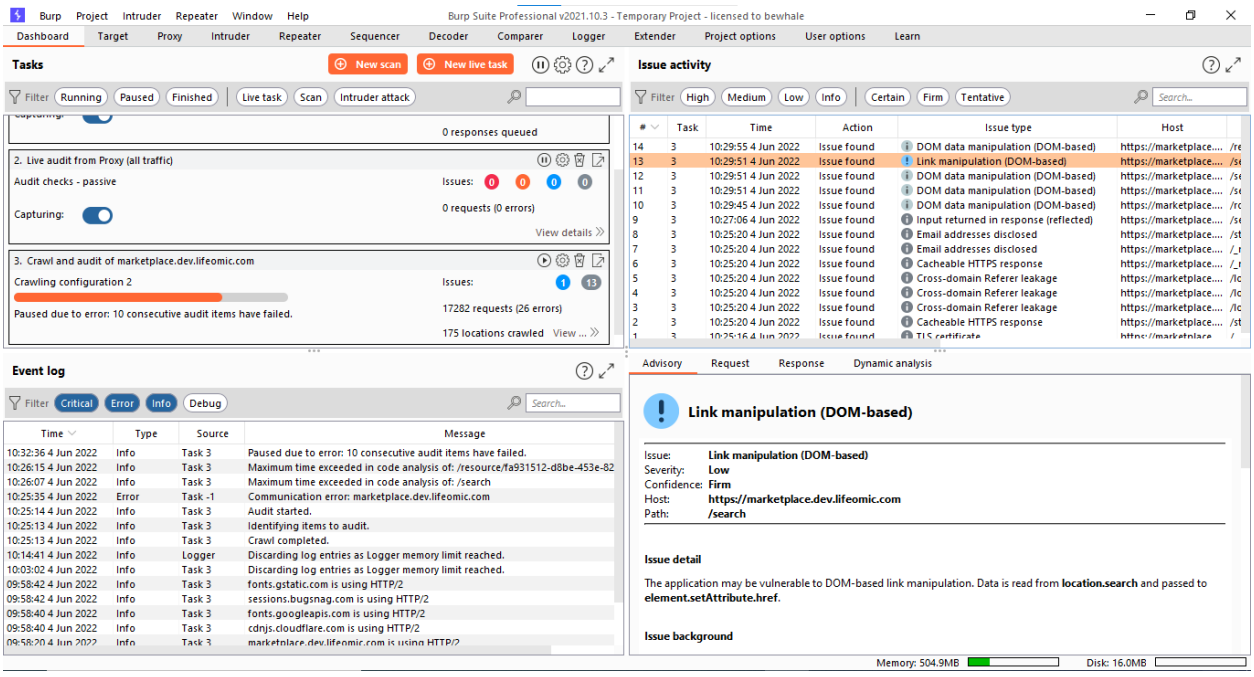
Vulnerability Assessment Tools

- Burp suite
- PWN XSS
- OWASP ZAP
- Netsparker

1 . Burp suite

Burp Suite is a popular Java-based Web Penetration Testing tool. It has become an industry-standard toolbox for information security professionals all across the world. Burp Suite assists in the discovery and verification of online application vulnerabilities and attack vectors.

I scan **marketplace.dev.lifeomic.com** domain in burpsuite.then I got some vulnerabilities in that domain.


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2021.10.3 - Temporary Project - licensed to bewhale
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
0 responses queued
2. Live audit from Proxy (all traffic)
Audit checks - passive
Issues:
Capturing:
0 requests (0 errors)
View details
3. Crawl and audit of marketplace.dev.lifeomic.com
Crawling configuration 2
Issues:
Paused due to error: 10 consecutive audit items have failed.
17282 requests (26 errors)
175 locations crawled View ...
Issue activity
Filter High Medium Low Info Certain Firm Tentative
Search...
Task Time Action Issue type Host
14 3 10:29:55 4 Jun 2022 Issue found DOM data manipulation (DOM-based) https://marketplace.... /re
13 3 10:29:51 4 Jun 2022 Issue found Link manipulation (DOM-based) https://marketplace.... /s
12 3 10:29:51 4 Jun 2022 Issue found DOM data manipulation (DOM-based) https://marketplace.... /s
11 3 10:29:51 4 Jun 2022 Issue found DOM data manipulation (DOM-based) https://marketplace.... /s
10 3 10:29:45 4 Jun 2022 Issue found DOM data manipulation (DOM-based) https://marketplace.... /r
9 3 10:27:06 4 Jun 2022 Issue found Input returned in response (reflected) https://marketplace.... /s
8 3 10:25:20 4 Jun 2022 Issue found Email addresses disclosed https://marketplace.... /st
7 3 10:25:20 4 Jun 2022 Issue found Email addresses disclosed https://marketplace.... /_r
6 3 10:25:20 4 Jun 2022 Issue found Cacheable HTTPS response https://marketplace.... /_r
5 3 10:25:20 4 Jun 2022 Issue found Cross-domain Referer leakage https://marketplace.... /lc
4 3 10:25:20 4 Jun 2022 Issue found Cross-domain Referer leakage https://marketplace.... /lc
3 3 10:25:20 4 Jun 2022 Issue found Cross-domain Referer leakage https://marketplace.... /lc
2 3 10:25:20 4 Jun 2022 Issue found Cacheable HTTPS response https://marketplace.... /st
1 3 10:25:16 4 Jun 2022 Issue found TLS certificate https://marketplace... /
Event log
Filter Critical Error Info Debug
Search...
Time Type Source Message
10:32:36 4 Jun 2022 Info Task 3 Paused due to error: 10 consecutive audit items have failed.
10:26:15 4 Jun 2022 Info Task 3 Maximum time exceeded in code analysis of: /resource/fa931512-d8be-453e-82
10:26:07 4 Jun 2022 Info Task 3 Maximum time exceeded in code analysis of: /search
10:25:35 4 Jun 2022 Error Task -1 Communication error: marketplace.dev.lifeomic.com
10:25:14 4 Jun 2022 Info Task 3 Audit started.
10:25:13 4 Jun 2022 Info Task 3 Identifying items to audit.
10:25:13 4 Jun 2022 Info Task 3 Crawl completed.
10:14:41 4 Jun 2022 Info Logger Discarding log entries as Logger memory limit reached.
10:03:02 4 Jun 2022 Info Task 3 Discarding log entries as Logger memory limit reached.
09:58:42 4 Jun 2022 Info Task 3 fonts.gstatic.com is using HTTP/2
09:58:42 4 Jun 2022 Info Task 3 sessions.bugsnag.com is using HTTP/2
09:58:40 4 Jun 2022 Info Task 3 fonts.googleapis.com is using HTTP/2
09:58:40 4 Jun 2022 Info Task 3 cdnjs.cloudflare.com is using HTTP/2
09:58:20 4 Jun 2022 Info Task 3 marketplace.dev.lifeomic.com is using HTTP/2
Advisory Request Response Dynamic analysis
Link manipulation (DOM-based)
Issue: Link manipulation (DOM-based)
Severity: Low
Confidence: Firm
Host: https://marketplace.dev.lifeomic.com
Path: /search
Issue detail
The application may be vulnerable to DOM-based link manipulation. Data is read from location.search and passed to element.setAttribute.href.
Issue background
Memory: 504.9MB
Disk: 16.0MB

issue: **Link manipulation (DOM-based)**
Severity: **Low**
Confidence: **Firm**
Host: **https://marketplace.dev.lifeomic.com**
Path: **/search**

Type index (hex)

0x00501001

Type index (decimal)

5246977

Issue detail

The application may be vulnerable to DOM-based link manipulation. Data is read from **location.search** and passed to **element.setAttribute.href**.

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based link manipulation arises when a script writes controllable data to a navigation target within the current page, such as a clickable link or the submission URL of a form. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the target of links within the response. An attacker may be able to leverage this to perform various attacks, including:

- Causing the user to redirect to an arbitrary external URL, to facilitate a phishing attack.
- Causing the user to submit sensitive form data to a server controlled by the attacker.
- Causing the user to perform an unintended action within the application, by changing the file or query string associated with a link.
- Bypassing browser anti-XSS defenses by injecting on-site links containing XSS exploits, since browser anti-XSS defenses typically do not operate on on-site links.

Burp Suite automatically identifies this issue using static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based link manipulation vulnerabilities is not to dynamically set the target URLs of links or forms using data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing an arbitrary URL as a link target. In general, this is best achieved by using a whitelist of URLs that are permitted link targets, and strictly validating the target against this list before setting the link target.

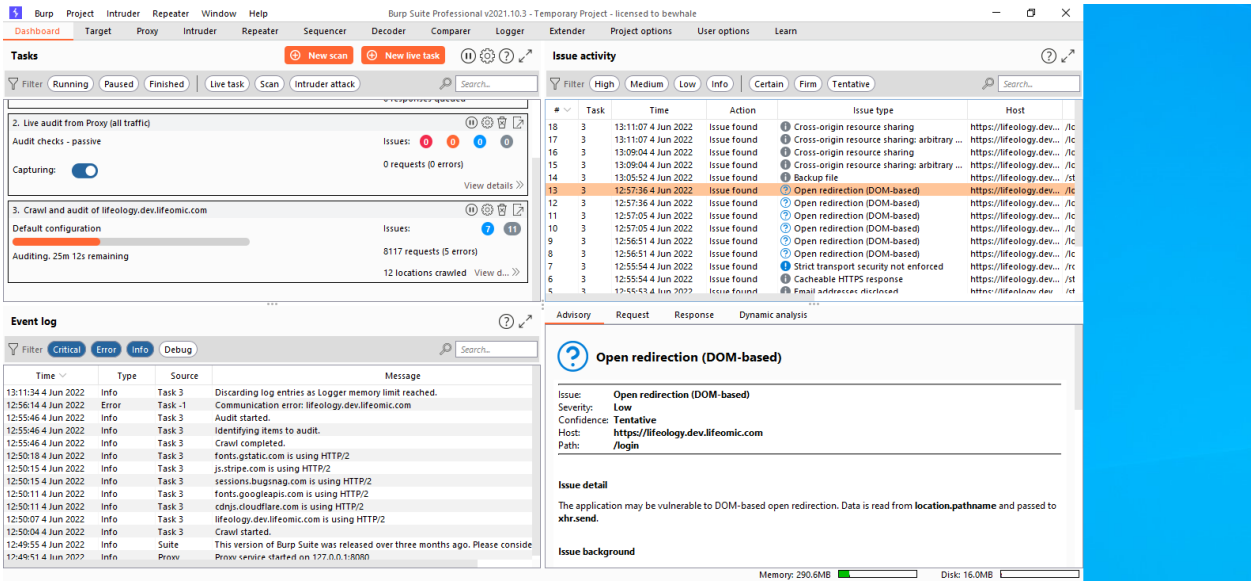
References

- Web Security Academy: Link manipulation (DOM-based)

Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

I scan **https://lifeology.dev.lifeomic.com** domain in burpsuite.then I got some vulnerabilities in that domain.


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2021.10.3 - Temporary Project - licensed to bewhale
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing:
Issues:
0 requests (0 errors)
View details
3. Crawl and audit of lifeology.dev.lifeomic.com
Default configuration
Auditing. 25m 12s remaining
Issues:
8117 requests (5 errors)
12 locations crawled
Issue activity
Filter High Medium Low Info Certain Firm Tentative
Task Time Action Issue type Host
18 3 13:11:07 4 Jun 2022 Issue found Cross-origin resource sharing https://lifeology.dev... /lc
17 3 13:11:07 4 Jun 2022 Issue found Cross-origin resource sharing: arbitrary ... https://lifeology.dev... /lc
16 3 13:09:04 4 Jun 2022 Issue found Cross-origin resource sharing https://lifeology.dev... /lc
15 3 13:09:04 4 Jun 2022 Issue found Cross-origin resource sharing: arbitrary ... https://lifeology.dev... /lc
14 3 13:05:52 4 Jun 2022 Issue found Backup file https://lifeology.dev... /st
13 3 12:57:36 4 Jun 2022 Issue found Open redirection (DOM-based) https://lifeology.dev... /lc
12 3 12:57:36 4 Jun 2022 Issue found Open redirection (DOM-based) https://lifeology.dev... /lc
11 3 12:57:05 4 Jun 2022 Issue found Open redirection (DOM-based) https://lifeology.dev... /lc
10 3 12:57:05 4 Jun 2022 Issue found Open redirection (DOM-based) https://lifeology.dev... /lc
9 3 12:56:51 4 Jun 2022 Issue found Open redirection (DOM-based) https://lifeology.dev... /lc
8 3 12:56:51 4 Jun 2022 Issue found Open redirection (DOM-based) https://lifeology.dev... /lc
7 3 12:55:54 4 Jun 2022 Issue found Strict transport security not enforced https://lifeology.dev... /rc
6 3 12:55:54 4 Jun 2022 Issue found Cacheable HTTPS response https://lifeology.dev... /st
Event log
Filter Critical Error Info Debug
Time Type Source Message
13:11:34 4 Jun 2022 Info Task 3 Discarding log entries as Logger memory limit reached.
12:56:14 4 Jun 2022 Error Task -1 Communication error: lifeology.dev.lifeomic.com
12:55:46 4 Jun 2022 Info Task 3 Audit started.
12:55:46 4 Jun 2022 Info Task 3 Identifying items to audit.
12:55:46 4 Jun 2022 Info Task 3 Crawl completed.
12:50:18 4 Jun 2022 Info Task 3 fonts.gstatic.com is using HTTP/2
12:50:15 4 Jun 2022 Info Task 3 js.stripe.com is using HTTP/2
12:50:15 4 Jun 2022 Info Task 3 sessions.bugsnag.com is using HTTP/2
12:50:11 4 Jun 2022 Info Task 3 fonts.googleapis.com is using HTTP/2
12:50:11 4 Jun 2022 Info Task 3 cdnjs.cloudflare.com is using HTTP/2
12:50:07 4 Jun 2022 Info Task 3 lifeology.dev.lifeomic.com is using HTTP/2
12:50:04 4 Jun 2022 Info Task 3 Crawl started.
12:49:55 4 Jun 2022 Info Suite This version of Burp Suite was released over three months ago. Please conside
Advisory Request Response Dynamic analysis
Open redirection (DOM-based)
Issue: Open redirection (DOM-based)
Severity: Low
Confidence: Tentative
Host: https://lifeology.dev.lifeomic.com
Path: /login
Issue detail
The application may be vulnerable to DOM-based open redirection. Data is read from location.pathname and passed to xhr.send.
Issue background
Memory: 290.6MB
Disk: 16.0MB

Issue:	**Open redirection (DOM-based)**
Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://lifeology.dev.lifeomic.com**
Path:	**/login**

Type index (hex)

0x00500110

Type index (decimal)

5243152

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.send**.

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based open redirection arises when a script writes controllable data into the target of a redirection in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

Note: If an attacker is able to control the start of the string that is passed to the redirection API, then it may be possible to escalate this vulnerability into a JavaScript injection attack, by using a URL with the javascript: pseudo-protocol to execute arbitrary script code when the URL is processed by the browser.

Burp Suite automatically identifies this issue using static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based open redirection vulnerabilities is not to dynamically set redirection targets using data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing an arbitrary URL as a redirection target. In general, this is best achieved by using a whitelist of URLs that are permitted redirection targets, and strictly validating the target against this list before performing the redirection.

References

- Web Security Academy: Open redirection (DOM-based)

Vulnerability classifications

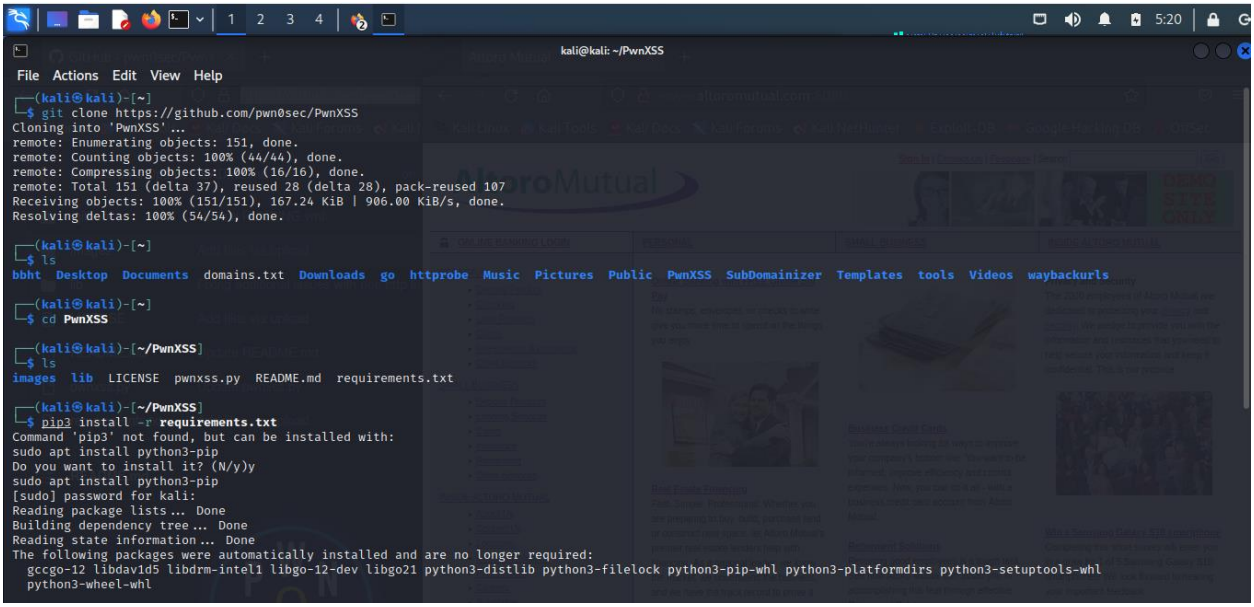
- CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

2 . Pwnxss

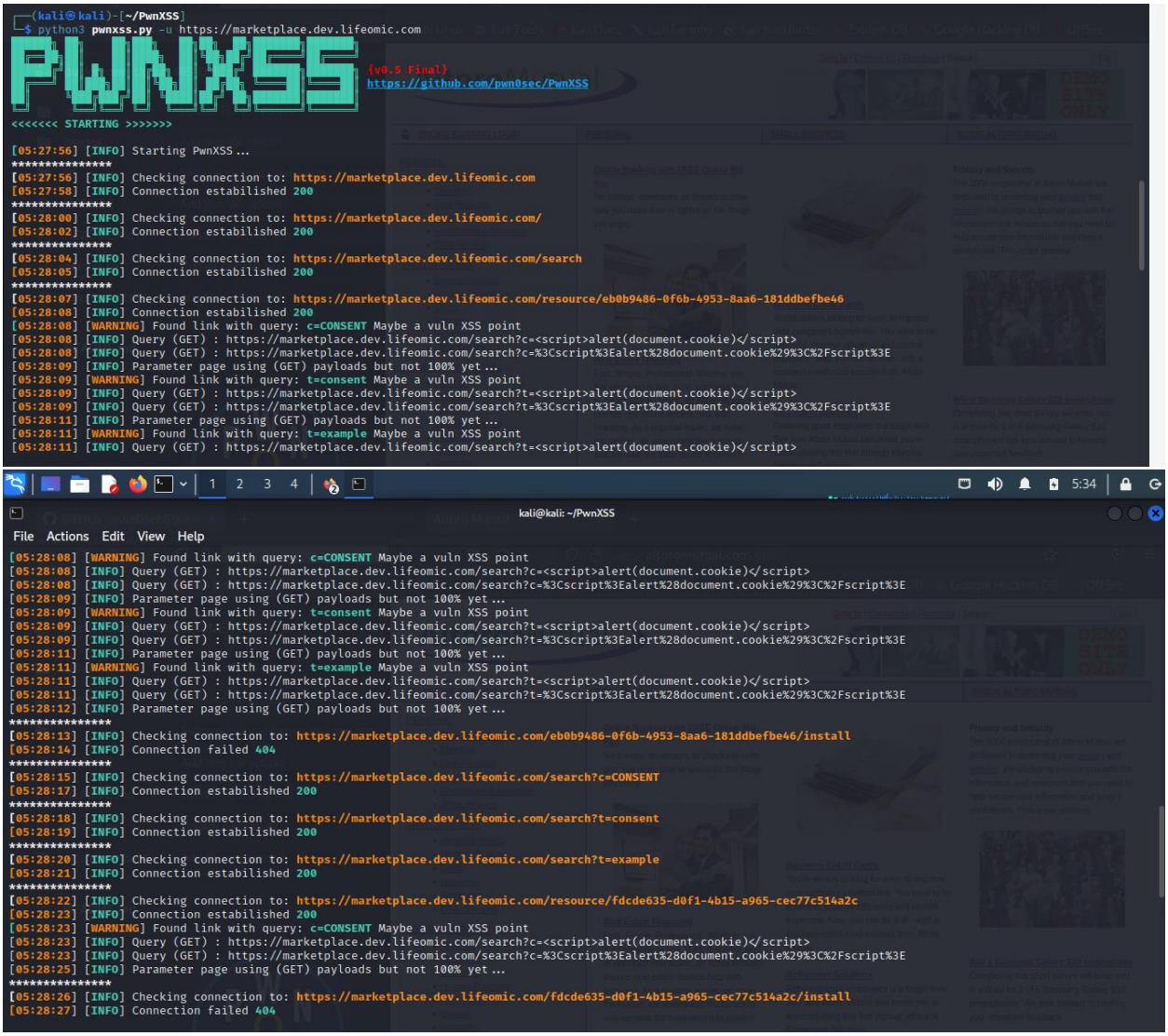
PwnXSS is a tool for multiprocessing support. PwnXSS is a tool that can be tailored to your needs. PwnXSS can handle both POST and GET requests. Error handling is a feature of PwnXSS. It can easily handle any errors that occur during scanning. PwnXSS is a tool that is both free and open source. PwnXSS is written in the Python programming language.

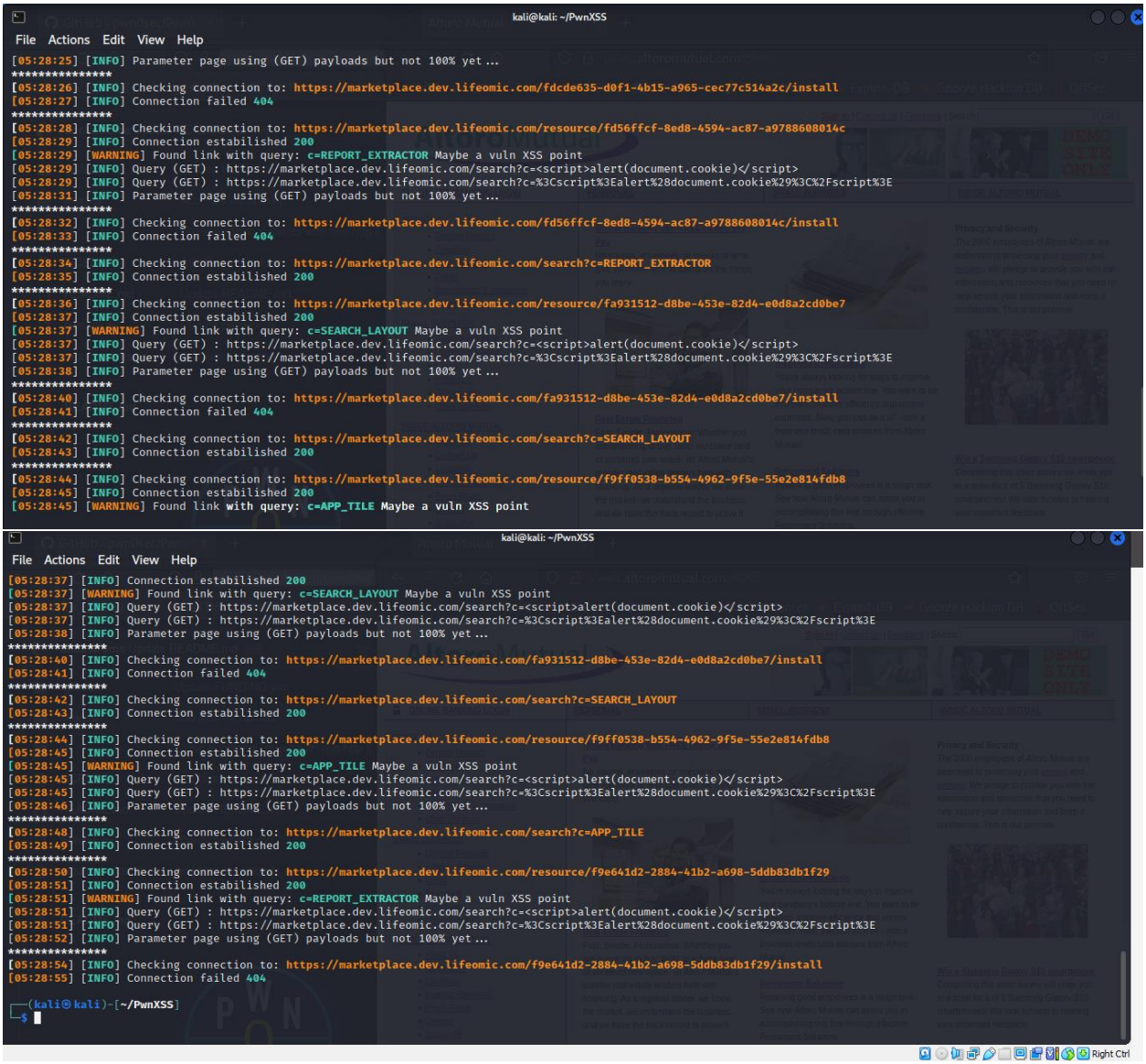
Github link - https://github.com/pwn0sec/PwnXSS.git

Command used to scan website – python3 pwnxss.py –u <domain name>



Target domain –**_marketplace.dev.lifeomic.com**


┌──(kali㉿kali)-[~/PwnXSS]
└─$ python3 pwnxss.py -u https://marketplace.dev.lifeomic.com
PWNXSS
{v0.5 Final}
https://github.com/pwn0sec/PwnXSS
<<<<<<< STARTING >>>>>>>
[05:27:56] [INFO] Starting PwnXSS ...
****
[05:27:56] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com
[05:27:58] [INFO] Connection estabilished 200
****
[05:28:00] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/
[05:28:02] [INFO] Connection estabilished 200
****
[05:28:04] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/search
[05:28:05] [INFO] Connection estabilished 200
****
[05:28:07] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/resource/eb0b9486-0f6b-4953-8aa6-181ddbefbe46
[05:28:08] [INFO] Connection estabilished 200
[05:28:08] [WARNING] Found link with query: c=CONSENT Maybe a vuln XSS point
[05:28:08] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=<script>alert(document.cookie)</script>
[05:28:08] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[05:28:09] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[05:28:09] [WARNING] Found link with query: t=consent Maybe a vuln XSS point
[05:28:09] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?t=<script>alert(document.cookie)</script>
[05:28:09] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?t=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[05:28:11] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[05:28:11] [WARNING] Found link with query: t=example Maybe a vuln XSS point
[05:28:11] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?t=<script>alert(document.cookie)</script>
1 2 3 4
5:34
kali@kali: ~/PwnXSS
File Actions Edit View Help
[05:28:08] [WARNING] Found link with query: c=CONSENT Maybe a vuln XSS point
[05:28:08] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=<script>alert(document.cookie)</script>
[05:28:08] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[05:28:09] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[05:28:09] [WARNING] Found link with query: t=consent Maybe a vuln XSS point
[05:28:09] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?t=<script>alert(document.cookie)</script>
[05:28:09] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?t=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[05:28:11] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[05:28:11] [WARNING] Found link with query: t=example Maybe a vuln XSS point
[05:28:11] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?t=<script>alert(document.cookie)</script>
[05:28:11] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?t=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[05:28:12] [INFO] Parameter page using (GET) payloads but not 100% yet ...
****
[05:28:13] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/eb0b9486-0f6b-4953-8aa6-181ddbefbe46/install
[05:28:14] [INFO] Connection failed 404
****
[05:28:15] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/search?c=CONSENT
[05:28:17] [INFO] Connection estabilished 200
****
[05:28:18] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/search?t=consent
[05:28:19] [INFO] Connection estabilished 200
****
[05:28:20] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/search?t=example
[05:28:21] [INFO] Connection estabilished 200
****
[05:28:22] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/resource/fdcde635-d0f1-4b15-a965-cec77c514a2c
[05:28:23] [INFO] Connection estabilished 200
[05:28:23] [WARNING] Found link with query: c=CONSENT Maybe a vuln XSS point
[05:28:23] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=<script>alert(document.cookie)</script>
[05:28:23] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[05:28:25] [INFO] Parameter page using (GET) payloads but not 100% yet ...
****
[05:28:26] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/fdcde635-d0f1-4b15-a965-cec77c514a2c/install
[05:28:27] [INFO] Connection failed 404



Report shows that"may be a vuln xss point"

I have received a critical level report. This is about internal errors and its SSL certification error.

Then I scanned for other domains but it don’t show any report.

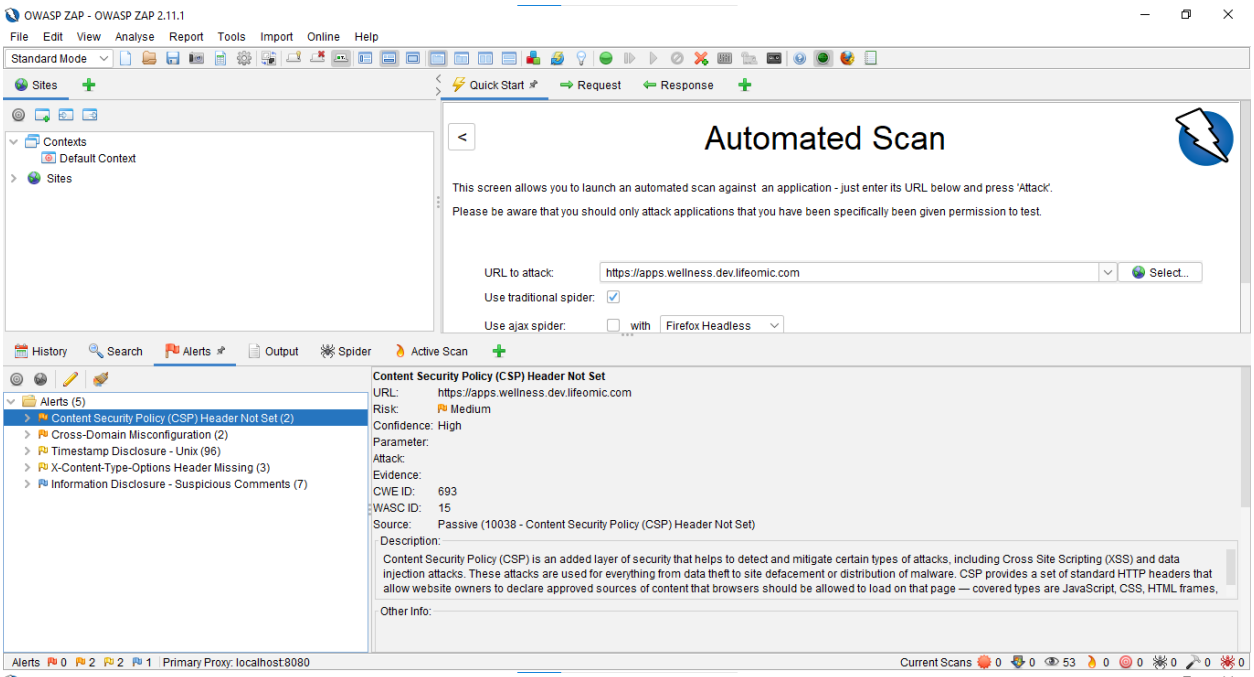
t.

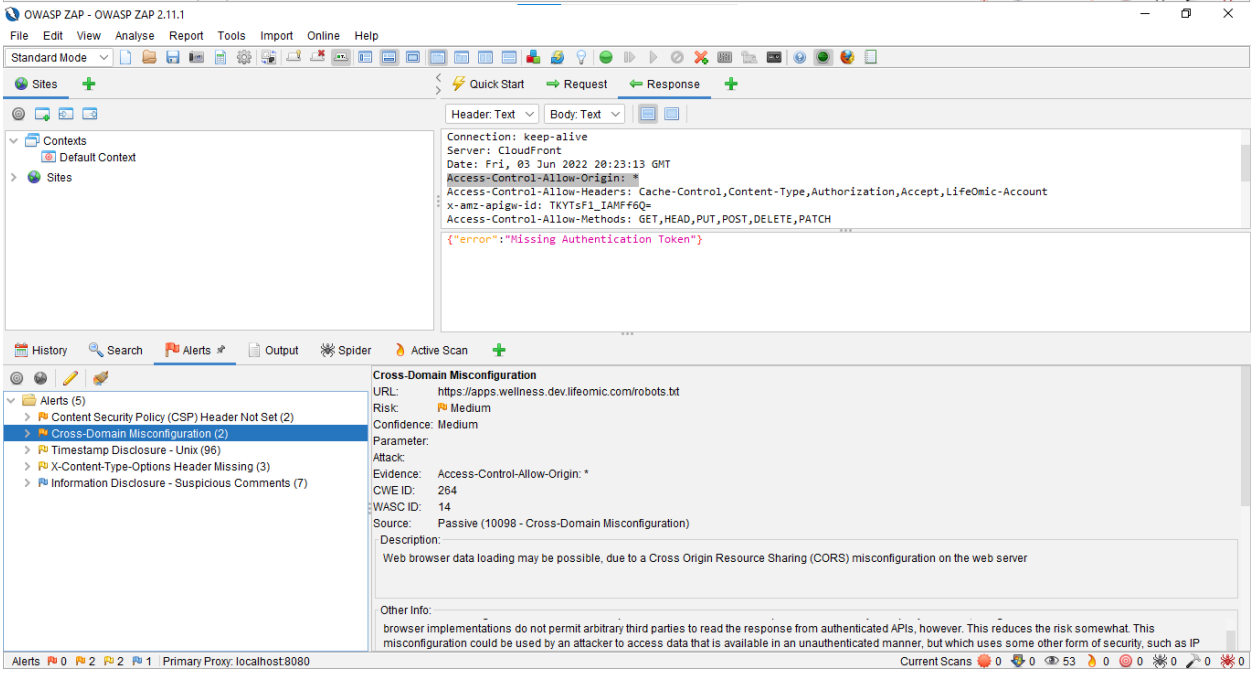
3 . Owasp zap

OWASP ZAP is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers.

Download link - [OWASP ZAP – Download (zaproxy.org)]

I have used this tool and scanned the domain https://apps.wellness.dev.lifeomic.com





Then I found two vulnerabilities in that domain.

That are content security policy(csp) header not set & cross domain misconfiguration.

Cross domain misconfiguration

Cross Domain Misconfiguration

Alert Id - 10098

Alert Type - Passive

Status release

Risk Medium

CWE 264

WASC 14

Tags OWASP_2017_A05

OWASP_2021_A01

to fix “Cross-Domain Misconfiguration”

Make sure the Access-Control-Allow-Origin header is not excessively permissive (doesn't have wildcard * as its value). You may also remove all the CORS headers and rely on the browser's default behaviour (following Same Origin Policy).

Why “Cross-Domain Misconfiguration” can be dangerous

For security reasons browsers by default don’t allow different websites (having different domains) to send any requests between each other. However, there exist scenarios in which that behaviour is desirable. For that reason certain HTTP headers (CORS headers) were introduced to allow you to configure which domains are eligible to get a response from a given url on your website. However,

How to fix “Cross-Domain Misconfiguration”

Make sure the Access-Control-Allow-Origin header is not excessively permissive (doesn’t have wildcard * as its value). You may also remove all the CORS headers and rely on the browser’s default behaviour (following Same Origin Policy).

How does ScanRepeat report “Cross-Domain Misconfiguration”

ScanRepeat reports urls that have excessively permissive CORS headers.

Solution

Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the 'Access-Control-Allow-Origin' HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

Content security policy (csp) header not set

content security policy header not set

Details

Alert Id - 10038

Alert Type - Passive

Status release

Risk - Medium

CWE

WASC

Tags OWASP_2017_A06

OWASP_2021_A05

To fix Content Security Policy (CSP) Header Not Set

you need to configure your web server to return the Content-Security-Policy HTTP Header and giving it values to control what resources the browser is allowed to load for your page.

Why Content Security Policy (CSP) Header Not Set can be dangerous -

Content Security Policy (CSP) adds a layer of security which helps to detect and mitigate certain types of attacks such as Cross Site Scripting (XSS) and data injection attacks. Hackers use XSS attacks to trick trusted websites into delivering malicious content. The browser executes all code from trusted origin and can't differentiate between legitimate and malicious code, so any injected code is executed as well.

How to fix Content Security Policy (CSP) Header Not Set -

To fix Content Security Policy (CSP) Header Not Set you need to configure your web server to return the Content-Security-Policy HTTP Header and giving it values to control what resources the browser is allowed to load for your page.

The syntax is:

Content-Security-Policy: <policy-directive>; <policy-directive>

where:

<policy-directive>consists of: <directive> <value> with no internal punctuation.

Example:

Content-Security-Policy: default-src 'self' http://example.com;

For a full list of possible directives and more examples please check https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy.

How does ScanRepeat report Content Security Policy (CSP) Header Not Set -

ScanRepeat analyzes the value of the "Content-Security-Policy" header of every HTTP response. It reports every potential misconfiguration or weakness and provides origins of these requests.

Summary

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.

Solution

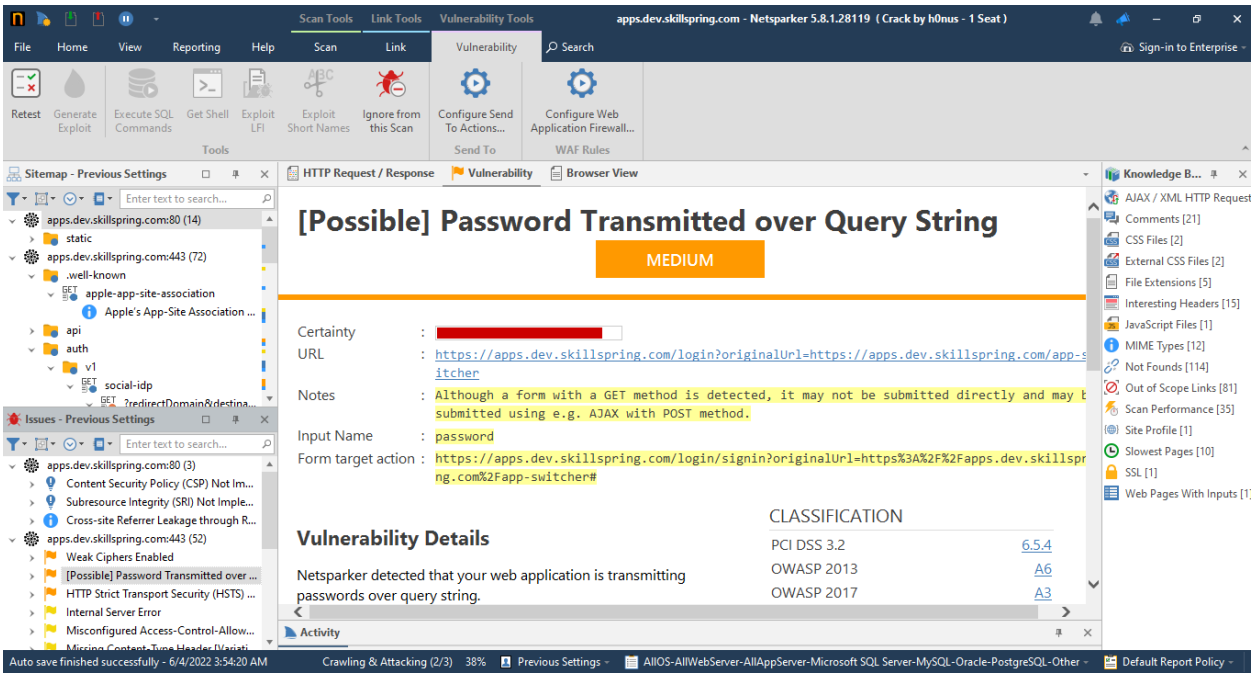
Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: 'Content-Security-Policy' for Chrome 25+, Firefox 23+ and Safari 7+, 'X-Content-Security-Policy' for Firefox 4.0+ and Internet Explorer 10+, and 'X-WebKit-CSP' for Chrome 14+ and Safari 6+.

4. Netsparker

Netsparker is a web application security scanner that automatically detects security flaws in online applications, websites, and web services. It's a user-friendly and accurate program that detects SQL injections, cross-site scripting (XSS), and other major security problems.

I have used this scanner and I have scanned the some lifeomic domains and I got the vulnerability reports.

Domain - **apps.dev.skillspring.com**



(possible) Password transmitted over query string

(possible) Password transmitted over query string

Risk – Medium

CLASSIFICATION

PCI DSS 3.26.5.4

OWASP 2013A6

OWASP 2017A3

CWE598

Vulnerability Details

Netsparker detected that your web application is transmitting passwords over query string

Impact

A password is sensitive data and shouldn't be transmitted over 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.

Query string is generally stored in server logs.

Browsers will cache the query string.

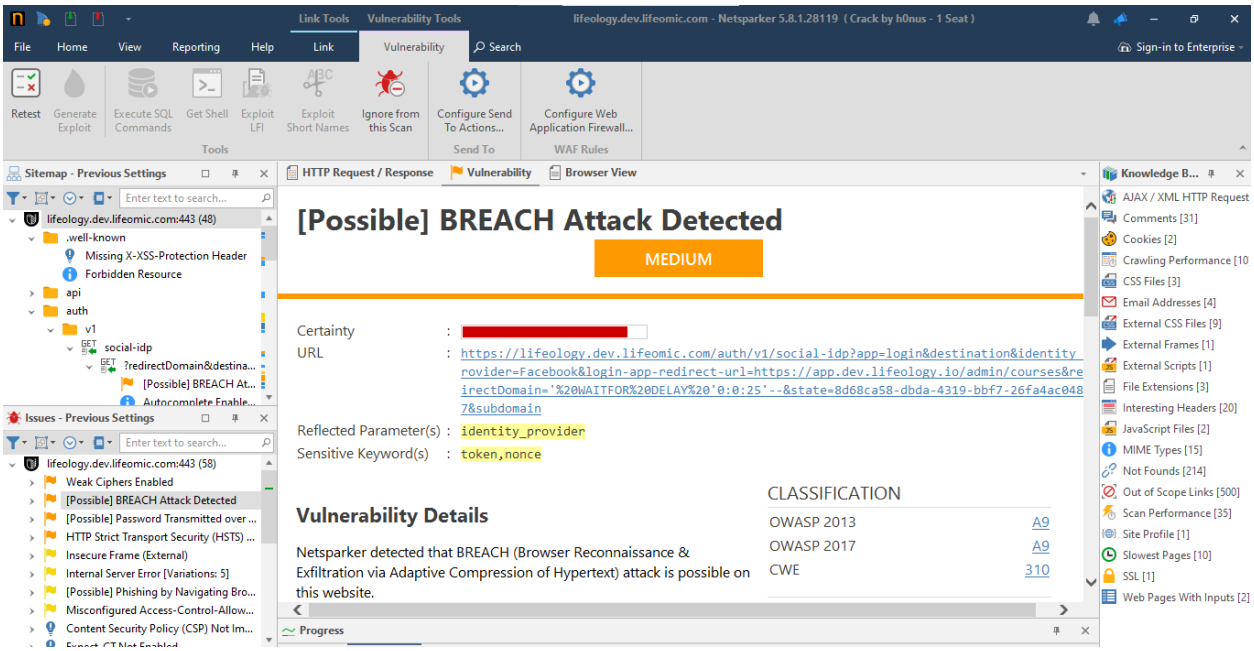
Query string is generally stored in server logs.

Browsers will cache the query string.

Remedy

Do not send any sensitive data through query string.

Domain - https://lifeology.dev.lifeomic.com



(Possible) BREACH Attack Detected

(Possible) BREACH Attack Detected

Risk – Medium

CLASSIFICATION

OWASP 2013A9

OWASP 2017A9

CWE310

Vulnerability Details

Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.

Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.

Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

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

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:

If possible, disable HTTP level compression

Separate sensitive information from user input

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.

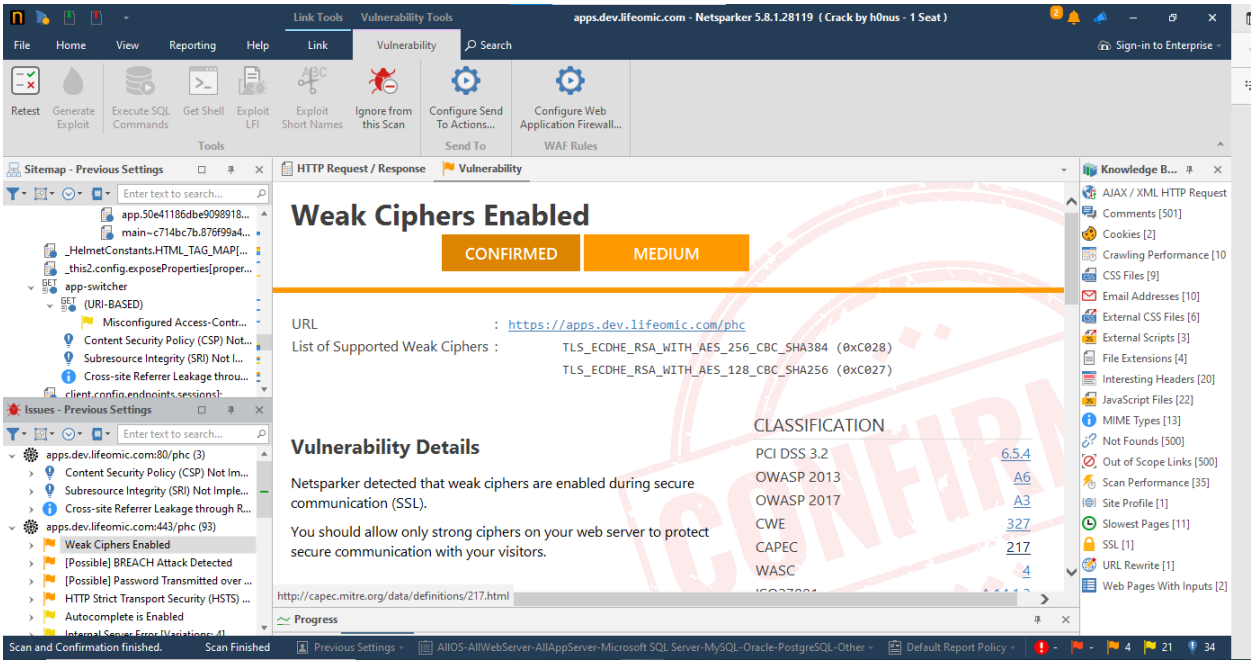
Hide the length of the traffic by adding a random number of bytes to the responses.

Add in a rate limit, so that the page maximum is reached five times per minute.

techniques for mitigating this attack are:

- 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

Domain - **apps.dev.lifeomic.com/phc**



Weak Ciphers Enabled

Weak Ciphers Enabled

MEDIUM CONFIRMED

URL :https://apps.dev.lifeomic.com/phc

CLASSIFICATION

PCI DSS 3.26.5.4

OWASP 2013A6

OWASP 2017A3

CWE327

Vulnerability Details

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

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

Actions to Take

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

SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4

Lighttpd:

ssl.honor-cipher-order = "enable"

ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"

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

a. Click Start, click Run, type regedt32 or type regedit, and then click OK.

b. In Registry Editor, locate the following registry key:
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

c. Set "Enabled" DWORD to "0x0" for the following registry keys:

SCHANNEL\Ciphers\DES 56/56

SCHANNEL\Ciphers\RC4 64/128

SCHANNEL\Ciphers\RC4 40/128

SCHANNEL\Ciphers\RC2 56/128

SCHANNEL\Ciphers\RC2 40/128

SCHANNEL\Ciphers\NULL

SCHANNEL\Hashes\MD5

Remedy

Configure your web server to disallow using weak ciphers.

External References

OWASP - Insecure Configuration Management

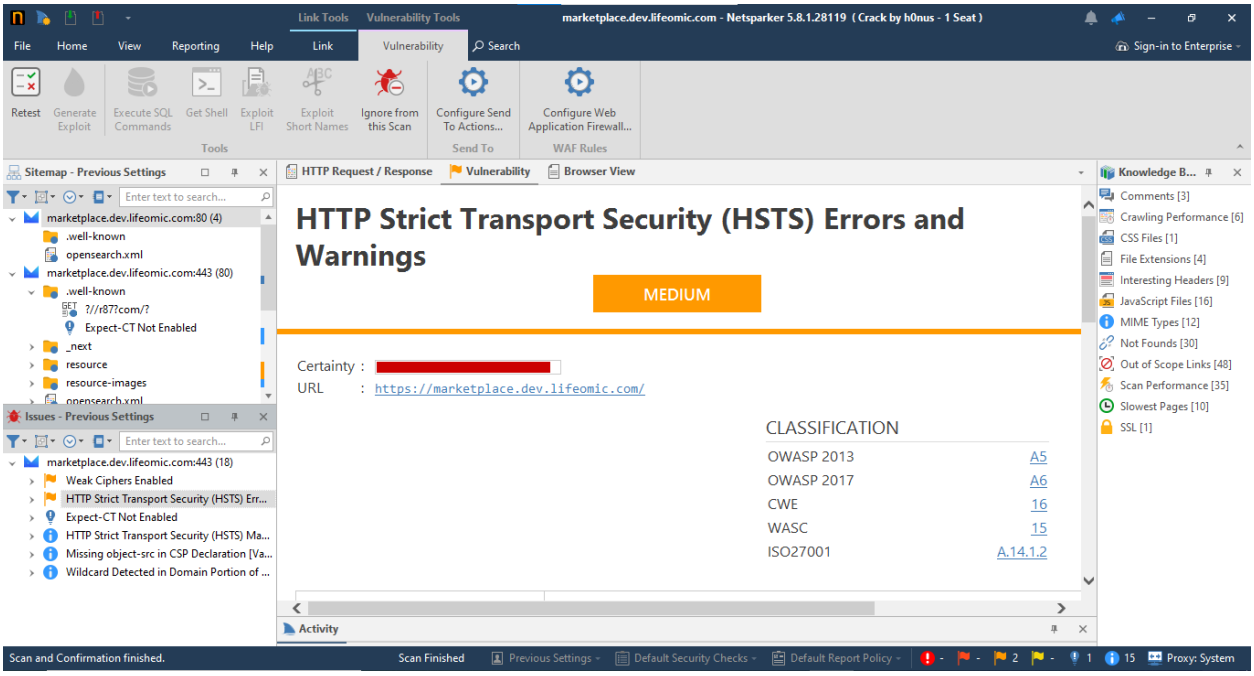
OWASP Top 10-2017 A3-Sensitive Data Exposure

Zombie Poodle - Golden Doodle (CBC)

Mozilla SSL Configuration Generator

Strong Ciphers for Apache, Nginx and Lighttpd

Domain - **marketplace.dev.lifeomic.com**



HTTP Strict Transport Security (HSTS) Errors and Warnings

HTTP Strict Transport Security (HSTS) Errors and Warnings

Severity: Medium

CLASSIFICATION

OWASP 2013A5

OWASP 2017A6

CWE16

WASC15

ISO27001A.14.1.2

Summary

Invicti detected errors during parsing of Strict-Transport-Security header.

Impact

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

Remediation

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:

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)

Classifications

CWE-16; ISO27001-A.14.1.2; WASC-15; OWASP 2013-A5; OWASP 2017-A6

Conclusion

The vulnerabilities and critical suggestions for the https://lifeomic.com domain have been presented in this study. Vulnerabilities are classified as critical, high, medium, low, or informative depending on their severity. In addition, I've detailed what tools I used for each reconnaissance and vulnerability analysis phrase in this security audit.

References

https://owasp.org/www-project-top-ten/

https://github.com/nahamsec

https://github.com/nahamsec/Resources-for-Beginner-Bug-BountyHunters/blob/master/assets/vulns.md

https://thehackerish.com/bug-bounty-tools-from-enumeration-to-reporting