



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

Objectives of the Assessment

Selected domain

Policy Analyzing

Scope

Out of scope

In scope domains

Information Gathering

Subdomain Enumeration

Tools

Checking alive sub domains

Gathering achieved details

DNS Enumeration

Find the target domain has firewall protection

Vulnerability Assessment

Tools

Vulnerabilities

Conclusion

References

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 Ruggahakotuwa, 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

The screenshot shows the HackerOne website at <https://hackerone.com/lifeomic?type=team>. The page displays information about the LifeOmic team, including its logo, a brief description of the company's mission, and various metrics. A prominent pink 'Submit report' button is visible. To the right, there is a 'Bug Bounty Program' section with details like 'Launched on Jan 2020' and 'Managed by HackerOne'. Below the main content, there are sections for 'Rewards' and 'Response Efficiency'.

Policy Hacktivity Thanks Updates (2)

Rewards

Low	Medium	High	Critical
\$100	\$500	\$750	\$1,500

Response Efficiency

about 1 day
Average time to first response

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
File Actions Edit View Help
kali@kali: ~
└$ subfinder -d apps.wellness.dev.lifeomic.com
[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.

[INFO] 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
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
www1.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
pops.apps.wellness.dev.lifeomic.com
ks-vendingtransactions-mq3.apps.wellness.dev.lifeomic.com
```

```
[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.

[INFO] Enumerating subdomains for apps.wellness.dev.lifeomic.com
ks-vendingtransactions-mq0.apps.wellness.dev.lifeomic.com
xs-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
www1.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
use the following command.
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
```

```
File Actions Edit View Help
kali㉿kali: ~
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
```

```
File Actions Edit View Help
kali㉿kali: ~
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
cpnapi.apps.wellness.dev.lifeomic.com
use the following command.
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
_etc-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
```

```
en.apps.wellness.dev.lifeomic.com
httpbin.apps.wellness.dev.lifeomic.com
akamai-test-origin.apps.wellness.dev.lifeomic.com  Kali NetHunter → Exploit-DB → Google Hacking DB → OffSec
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
ssvpn.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  Use the following command
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  Use the following command
signup.apps.wellness.dev.lifeomic.com  Please note that we are not responsible for any misuse or damage
wp.apps.wellness.dev.lifeomic.com  Please agree to the terms of the API's use
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  Use the following command
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  Use the following command
assets.apps.wellness.dev.lifeomic.com  Please note that we are not responsible for any misuse or damage
mta-sts.apps.wellness.dev.lifeomic.com  Please agree to the terms of the API's use
_mta-sts.apps.wellness.dev.lifeomic.com
lists.apps.wellness.dev.lifeomic.com
```

```
lists.apps.wellness.dev.lifeomic.com
news.apps.wellness.dev.lifeomic.com
gws.apps.wellness.dev.lifeomic.com
cim-api-uat.apps.wellness.dev.lifeomic.com
gws-ut.apps.wellness.dev.lifeomic.com
gws-rds-external-readonly-uat.apps.wellness.dev.lifeomic.com
git.apps.wellness.dev.lifeomic.com
vault.apps.wellness.dev.lifeomic.com
knowledgedemanagement.apps.wellness.dev.lifeomic.com
root.apps.wellness.dev.lifeomic.com
cert.apps.wellness.dev.lifeomic.com
support.apps.wellness.dev.lifeomic.com
useast.apps.wellness.dev.lifeomic.com
useast-rest.apps.wellness.dev.lifeomic.com
test.apps.wellness.dev.lifeomic.com
akamai-test.apps.wellness.dev.lifeomic.com
nginx-newest.apps.wellness.dev.lifeomic.com
host.apps.wellness.dev.lifeomic.com
localhost.apps.wellness.dev.lifeomic.com
dev.apps.wellness.dev.lifeomic.com
gcom-product-find-dev.apps.wellness.dev.lifeomic.com
dogfood-dev.apps.wellness.dev.lifeomic.com
cim-api-dev.apps.wellness.dev.lifeomic.com
searchportal-dev.apps.wellness.dev.lifeomic.com
cim-dev.apps.wellness.dev.lifeomic.com
cim-geo-dev.apps.wellness.dev.lifeomic.com
nodejs-dev.apps.wellness.dev.lifeomic.com
basic-nodejs-dev.apps.wellness.dev.lifeomic.com
gws-dev.apps.wellness.dev.lifeomic.com
view.apps.wellness.dev.lifeomic.com
preview.apps.wellness.dev.lifeomic.com
publishing-preview.apps.wellness.dev.lifeomic.com
merchandising-preview.apps.wellness.dev.lifeomic.com

File Actions Edit View Help
test.apps.wellness.dev.lifeomic.com
akamai-test.apps.wellness.dev.lifeomic.com
nginx-newest.apps.wellness.dev.lifeomic.com
host.apps.wellness.dev.lifeomic.com
localhost.apps.wellness.dev.lifeomic.com
dev.apps.wellness.dev.lifeomic.com
gcom-product-find-dev.apps.wellness.dev.lifeomic.com
dogfood-dev.apps.wellness.dev.lifeomic.com
cim-api-dev.apps.wellness.dev.lifeomic.com
searchportal-dev.apps.wellness.dev.lifeomic.com
cim-dev.apps.wellness.dev.lifeomic.com
cim-geo-dev.apps.wellness.dev.lifeomic.com
nodejs-dev.apps.wellness.dev.lifeomic.com
basic-nodejs-dev.apps.wellness.dev.lifeomic.com
gws-dev.apps.wellness.dev.lifeomic.com
view.apps.wellness.dev.lifeomic.com
preview.apps.wellness.dev.lifeomic.com
publishing-preview.apps.wellness.dev.lifeomic.com
merchandising-preview.apps.wellness.dev.lifeomic.com
new.apps.wellness.dev.lifeomic.com
fw.apps.wellness.dev.lifeomic.com
gw.apps.wellness.dev.lifeomic.com
www.apps.wellness.dev.lifeomic.com
citrix.apps.wellness.dev.lifeomic.com
mx.apps.wellness.dev.lifeomic.com
nginxx.apps.wellness.dev.lifeomic.com
gws-api-sandbox.apps.wellness.dev.lifeomic.com
rx.apps.wellness.dev.lifeomic.com
tx.apps.wellness.dev.lifeomic.com
gac-rds-external-readonly.apps.wellness.dev.lifeomic.com
proxy.apps.wellness.dev.lifeomic.com
You are not responsible for any misuse or damage
(kali㉿kali)-[~]
$
```

Target domain - lifeology.dev.lifeomic.com

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~

File Actions Edit View Help

\$ 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.

[INFO] Enumerating subdomains for 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-newest1.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

```
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-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
cppanel.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
_etc-d-server-sst.lifeology.dev.lifeomic.com
```

```
File Actions Edit View Help
Letcd-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
sslypn.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
```

```

File Actions Edit View Help
ns.lifeology.dev.lifeomic.com
dns.lifeology.dev.lifeomic.com
videos.lifeology.dev.lifeomic.com
orders.lifeology.dev.lifeomic.com
careers.lifeology.dev.lifeomic.com
servers.lifeology.dev.lifeomic.com
vendors.lifeology.dev.lifeomic.com
wordpress.lifeology.dev.lifeomic.com
stats.lifeology.dev.lifeomic.com
assets.lifeology.dev.lifeomic.com
mta-sts.lifeology.dev.lifeomic.com
lists.lifeology.dev.lifeomic.com
news.lifeology.dev.lifeomic.com
gws.lifeology.dev.lifeomic.com
cim-api-uat.lifeology.dev.lifeomic.com
gws-uat.lifeology.dev.lifeomic.com
gws-rds-external-readonly-uat.lifeology.dev.lifeomic.com
git.lifeology.dev.lifeomic.com
vault.lifeology.dev.lifeomic.com
knowledgemangement.lifeology.dev.lifeomic.com
root.lifeology.dev.lifeomic.com
cert.lifeology.dev.lifeomic.com
support.lifeology.dev.lifeomic.com
us-east.lifeology.dev.lifeomic.com
useast.lifeology.dev.lifeomic.com
mobile-rest.lifeology.dev.lifeomic.com
test.lifeology.dev.lifeomic.com
akamai-test.lifeology.dev.lifeomic.com
nginx-newest.lifeology.dev.lifeomic.com
host.lifeology.dev.lifeomic.com
localhost.lifeology.dev.lifeomic.com
dev.lifeology.dev.lifeomic.com
gcom-product-find-dev.lifeology.dev.lifeomic.com

```

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@kali: ~

```

File Actions Edit View Help
nginx-newest.lifeology.dev.lifeomic.com
host.lifeology.dev.lifeomic.com
localhost.lifeology.dev.lifeomic.com
dev.lifeology.dev.lifeomic.com
gcom-product-find-dev.lifeology.dev.lifeomic.com
dogfood-dev.lifeology.dev.lifeomic.com
cim-api-dev.lifeology.dev.lifeomic.com
searchportal-dev.lifeology.dev.lifeomic.com
cim-dev.lifeology.dev.lifeomic.com
cim-geo-dev.lifeology.dev.lifeomic.com
nodejs-dev.lifeology.dev.lifeomic.com
basic-nodejs-dev.lifeology.dev.lifeomic.com
gws-lifeology.dev.lifeomic.com
view.lifeology.dev.lifeomic.com
preview.lifeology.dev.lifeomic.com
publishing-preview.lifeology.dev.lifeomic.com
merchandising-preview.lifeology.dev.lifeomic.com
new.lifeology.dev.lifeomic.com
fw.lifeology.dev.lifeomic.com
gw.lifeology.dev.lifeomic.com
www.lifeology.dev.lifeomic.com
citrix.lifeology.dev.lifeomic.com
mx.lifeology.dev.lifeomic.com
nginx.lifeology.dev.lifeomic.com
gws-api-sandbox.lifeology.dev.lifeomic.com
rx.lifeology.dev.lifeomic.com
tx.lifeology.dev.lifeomic.com
gac-rds-external-readonly.lifeology.dev.lifeomic.com
proxy.lifeology.dev.lifeomic.com
ops-geo-brasil.lifeology.dev.lifeomic.com
org-db.lifeology.dev.lifeomic.com

```

[kali@kali] [-]

(100) Enumerating subdomains for backcomics.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 SubDomainizer from git:

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

- Change the directory:

```
cd SubDomainizer
```

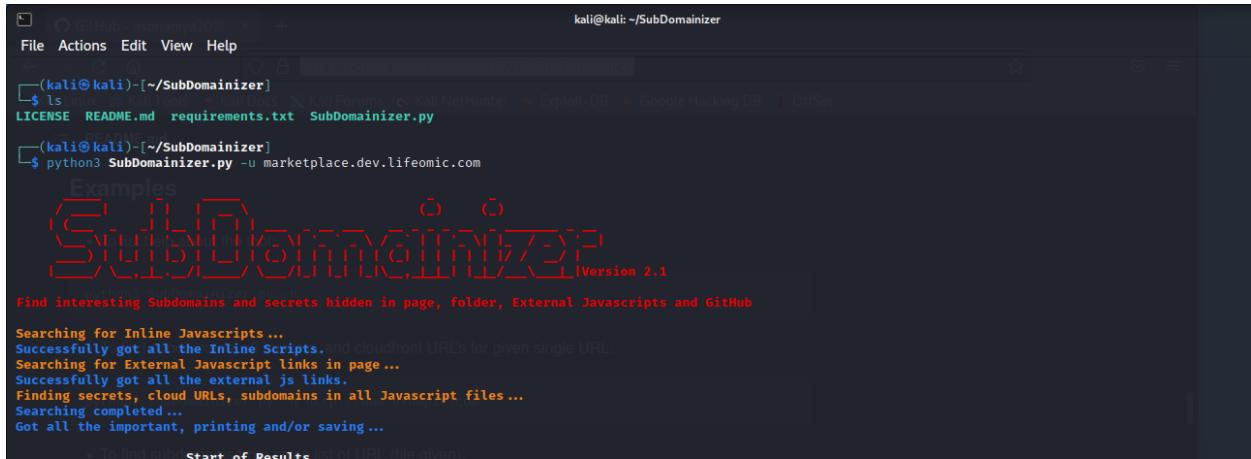
- Install the requirements:

```
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>
```



```
kali㉿kali:~/SubDomainizer
File Actions Edit View Help
(kali㉿kali)-[~/SubDomainizer]
$ ls
LICENSE README.md requirements.txt SubDomainizer.py
(kali㉿kali)-[~/SubDomainizer]
$ python3 SubDomainizer.py -u marketplace.dev.lifeomic.com
Examples
SubDomainizer Version 2.1
Find interesting Subdomains and secrets hidden in page, folder, External Javascripts and GitHub
Searching for Inline Javascripts ...
Successfully got all the Inline Scripts, and cloudfront URLs for given single URL.
Searching for External Javascript links in page ...
Successfully got all the external js links.
Finding secrets, cloud URLs, subdomains in all Javascript files ...
Searching completed ...
Got all the important, printing and/or saving ...
To find more results, use Start of Results button in HTML file output.

```

```

File Actions Edit View Help
Successfully got all the Inline Scripts.
Searching for External Javascript links in page...
Successfully got all the external js links.
Finding secrets, cloud URLs, subdomains in all Javascript files...
Searching completed...
Got all the important, printing and/or saving...
Example _Start of Results_
Got some subdomains...
Total Subdomains: 3
marketplace.dev.lifeomic.com
status.us.lifeomic.com
www.lifeomic.com
Some cloud services urls are found ...
Total Cloud URLs: 3
lifeomic-dev-marketplace-service-images.s3.amazonaws.com/e0bb9486-0f6b-4953-8aa6-181ddbefbe46
lifeomic-dev-marketplace-service-images.s3.amazonaws.com/fd56ffcf-8ed8-4594-ac87-a9788688014c
lifeomic-dev-marketplace-service-images.s3.amazonaws.com/f9e641d2-2884-41b2-a698-5ddb83db1f29
Found some secrets(might be false positive)...
Total Possible Secrets: 2
-token=IQoJb3pz2luX2VjE33//////////WEaCXvzLWVh3QtMSJGMEQCIHFUwz170XHgTsqrhf+d/yiy4w9KLA0bugDoMLyrmWFtAiA76x12dG/U/JzzOU16386Y0yqJicn3E+xNwLPsa2e1CqhAgiv////////////
BEAMaD0YhZex0Tc1NTA2NyINlNhuiNxaneNy7SkvUBz7pHo1miFcZgEoob8V1ysPbJ0ARj0i0Srat5jsgxck8bjek09N07lw1s1DHsv1vp081F5fc1cRYu/serjQujB8k9c3c+19f+vWluJ1TzKKLweRhx
+djxFyhFMDRDtumYk+HGxGh5nzWQq0fewJh1ghzfqRtvJufdEqjYFHQUkw204p0s13C24ncJvK80B0U6n6uPMzdEQqr7dp/jBjqkhNaQ8dGrmkURM6vkJzbQ+r/ZHSkfzaZ90jY/dsF53XCGozmIrU4cP3Ctg3
hre0J455InVPufx2ftn0Iy7okh5ssbkC315K7aAsvbuLAYmmwFMzRdn0KryVMETtJFD5u)IQIs1bVl0/1c1zqxEfmZ48a0oqx0af6EK+3Du0LR7VJSeitQW7rqF0Rqqtvv6AYA6xbzj7n8booxbkxu/DNKg0aUGZn
MPTq9Mwv+P2Q42MHG008yhAzn7oNPH0ISp1HeROZRASASOTIIWheJNx66tlp8I9oD3KmQ5xgE1jyjixaEGbo1Y7E1Yrw==" | Inline
AccessKeyId=ASIAZCF0U445052I3XET | Inline
End of Results

```

- Target Domain - apps.dev.skillspring.com

```

(kali㉿kali)-[~/SubDomainizer]
$ python3 SubDomainizer.py -u apps.dev.skillspring.com
[!] Kali Linux [!] Kali Tools [!] Kali Docs [!] Kali Forums [!] Kali WebHunter [!] Exploit-DB [!] Google Hacking DB [!] OffSec
SubDomainizer Version 2.1

Find interesting Subdomains and secrets hidden in page, folder, External Javascripts and GitHub
* To list help about the tool...
Searching for Inline Javascripts...
Successfully got all the Inline Scripts.
Searching for External Javascript links in page...
Successfully got all the external js links.
Finding secrets, cloud URLs, subdomains in all Javascript files...
Searching completed...
Got all the important, printing and/or saving ... Front URLs for given single URL.
Start of Results

Some cloud services urls are found ...
Total Cloud URLs: 1
s3.amazonaws.com

Found some secrets(might be false positive)...
Total Possible Secrets: 1
ClientId:"7iib2j0lqnmuul37lb0mimads" | Inline
* To save the results in output.txt file.
End of Results

```

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
- Httpprobe
- 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.
https://github.com/nahamsec/recon_profile

(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.ntu.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-intel libgo-12-dev libgo2l
Use 'sudo apt autoremove' to remove them.

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

```
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
└─$ GitHub - nahamsec/bbht
  kali㉿kali:~/bbht
File Actions Edit View Help
done
Trash
File System
  README.md
  https://github.com/nahamsec/recon_profile
  Installing
  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 lazyss
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.

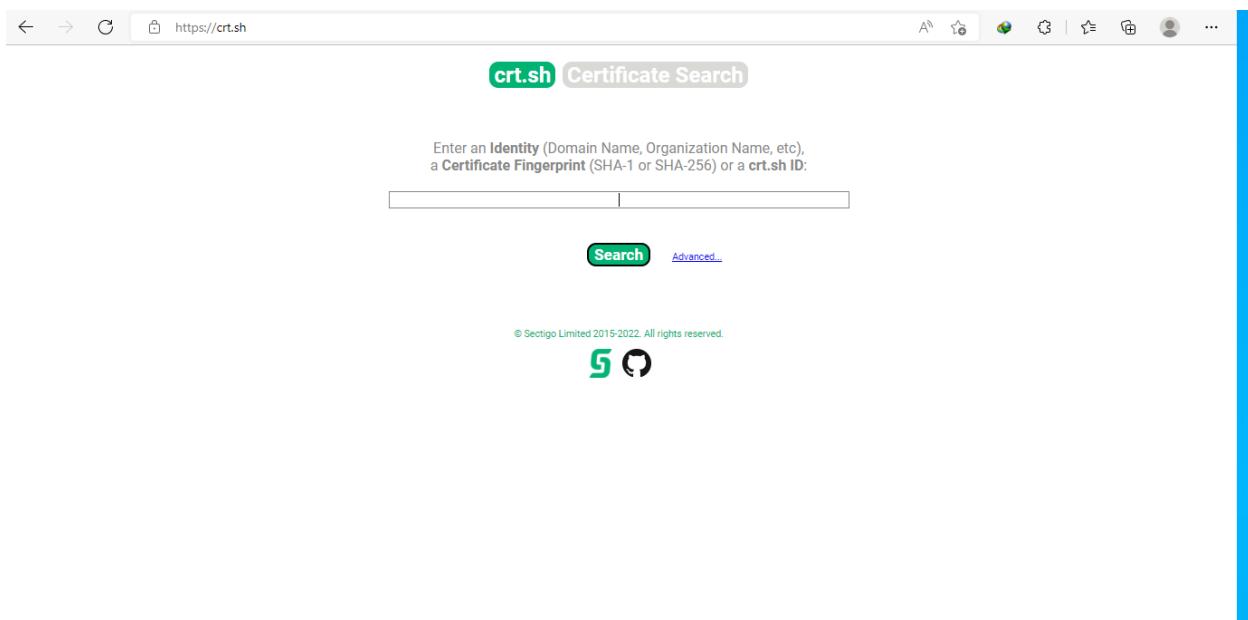
Crt.sh is a website where you can find all of the SSL or TLS certificates for a specific domain. In addition, the site's certificate monitoring is open-source.

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
	5408831467	2021-10-13	2021-10-04	2022-11-01	marketplace.dev.lifeomic.com	*.marketplace.dev.lifeomic.com marketplace.dev.lifeomic.com marketplace.dev.lifeomic.com marketplace.dev.lifeomic.com marketplace.dev.lifeomic.com
	5340404423	2021-10-04	2021-10-04	2022-11-01	marketplace.dev.lifeomic.com	*.marketplace.dev.lifeomic.com marketplace.dev.lifeomic.com
	3843990024	2020-12-29	2020-11-03	2021-12-02	marketplace.dev.lifeomic.com	*.marketplace.dev.lifeomic.com marketplace.dev.lifeomic.com
	3598980834	2020-11-03	2020-11-03	2021-12-02	marketplace.dev.lifeomic.com	*.marketplace.dev.lifeomic.com marketplace.dev.lifeomic.com
	3598769278	2020-11-03	2020-11-03	2021-12-02	marketplace.dev.lifeomic.com	*.marketplace.dev.lifeomic.com marketplace.dev.lifeomic.com

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 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 . Htprobe

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 Htprobe, which is accessible on Github.

Github link - GitHub - tomnomnom/htprobe

```

kali㉿kali:[~]
└─$ git clone https://github.com/tomnomnom/httpprobe.git
fatal: destination path 'httpprobe' already exists and is not an empty directory.

(kali㉿kali:[~])
└─$ ls
bbht Desktop Documents domains.txt Downloads go httpprobe Music Pictures Public SubDomainizer Templates tools Videos

(kali㉿kali:[~])
└─$ cd httpprobe

(kali㉿kali:[~/httpprobe])
└─$ ls
Dockerfile httpprobe LICENSE main.go README.md script

(kali㉿kali:[~/httpprobe])
└─$ 

```

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

The screenshot shows a Kali Linux desktop environment with three windows open:

- Terminal Window 1:** Shows the command `git clone https://github.com/tomnomnom/httpprobe.git` being run, followed by the creation of a `httpprobe` directory and its contents: Dockerfile, httpprobe, LICENSE, main.go, README.md, and script.
- File Manager Window:** Shows the `domains.txt` file containing a large list of sub-domains, such as `ks-vendingtransactions-mq0.apps.wellness.dev.lifeomic.com`, `us-east-1.apps.wellness.dev.lifeomic.com`, etc.
- Terminal Window 2:** Shows the command `cat ../*.txt | httpprobe` being run, which processes the `domains.txt` file through the `httpprobe` tool to check for live subdomains. The output lists many sub-domains, mostly starting with `www` or `ns` followed by a number and a suffix like `.wellness.dev.lifeomic.com`.

```

kali㉿kali:~/httpprobe
```

File Actions Edit View Help

```

https://sso.lifeology.dev.lifeomic.com
https://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
https://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
https://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
https://cp.lifeology.dev.lifeomic.com
https://sip.lifeology.dev.lifeomic.com
https://shop.lifeology.dev.lifeomic.com
https://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
https://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
https://2012aomenpuqingduchang.apps.dev.lifeomic.com/phc
https://1210.corp.apps.dev.lifeomic.com/phc
http://calendar.apps.dev.lifeomic.com/phc
https://1riri.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://1riri.corp.apps.dev.lifeomic.com/phc
https://cust57.cutsr.apps.dev.lifeomic.com/phc
http://columbus.apps.dev.lifeomic.com/phc
https://cust95.apps.dev.lifeomic.com/phc
https://15iii.corp.apps.dev.lifeomic.com/phc
https://help.cutsr.apps.dev.lifeomic.com/phc
https://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://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
```

```

kali㉿kali:~/httpprobe
```

File Actions Edit View Help

```

https://source.wwutsr.apps.dev.lifeomic.com/phc
http://wwutsr.apps.dev.lifeomic.com/phc
http://us.apps.dev.lifeomic.com/phc
https://michigan.wwutsr.apps.dev.lifeomic.com/phc
http://maint.wwutsr.apps.dev.lifeomic.com/phc
https://source.wwutsr.apps.dev.lifeomic.com/phc
http://pc49.maint.wwutsr.apps.dev.lifeomic.com/phc
https://relay.source.wwutsr.apps.dev.lifeomic.com/phc
https://pdc.pc32.relay.source.wwutsr.apps.dev.lifeomic.com/phc
https://pc32.relay.source.wwutsr.apps.dev.lifeomic.com/phc
http://michigan.wwutsr.apps.dev.lifeomic.com/phc
https://srqp.wwutsr.apps.dev.lifeomic.com/phc
http://relay.source.wwutsr.apps.dev.lifeomic.com/phc
https://admin.pc32.relay.source.wwutsr.apps.dev.lifeomic.com/phc
http://pdc.pc32.relay.source.wwutsr.apps.dev.lifeomic.com/phc
https://pc32.relay.source.wwutsr.apps.dev.lifeomic.com/phc
https://printer.sadmin.pc32.relay.source.wwutsr.apps.dev.lifeomic.com/phc
http://srqp.wwutsr.apps.dev.lifeomic.com/phc
https://jih.srqp.wwutsr.apps.dev.lifeomic.com/phc
http://admin.pc32.relay.source.wwutsr.apps.dev.lifeomic.com/phc
http://printer.sadmin.pc32.relay.source.wwutsr.apps.dev.lifeomic.com/phc
http://jih.srqp.wwutsr.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>

The screenshot shows the Wayback Machine's search results page. The URL entered is <http://apps.wellness.dev.lifeomic.com/>, and the results count is 50,100,500. Below the search bar, there are navigation links: Calendar, Collections, Changes, Summary, Site Map, and URLs (which is highlighted). A table below lists two captured URLs:

URL	MIME TYPE	FROM	TO	CAPTURES	DUPES	UNIQUES
https://apps.wellness.dev.lifeomic.com/admin	text/html	Apr 11, 2021	Apr 11, 2021	1	0	1
https://apps.wellness.dev.lifeomic.com/login	text/html	Apr 11, 2021	Jun 16, 2021	3	1	2

At the bottom, there are links to FAQ, Contact Us, and Terms of Service (Dec 31, 2014), and a footer note about the Wayback Machine being an initiative of the Internet Archive.

INTERNET ARCHIVE Explore more than 687 billion web pages saved over time

[DONATE](#) **WayBackMachine** [https://apps.wellness.dev.lifeomic.com/admin|](https://apps.wellness.dev.lifeomic.com/admin) [X](#)

Results: 50 100 500

[Calendar](#) · [Collections](#) · [Changes](#) · [Summary](#) · [Site Map](#) · [URLs](#)

Saved 1 time April 11, 2021.

1999 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

1	2	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3
3	4	5	6	7	8	9	7	8	9	10	11	12	13	7	8	9
10	11	12	13	14	15	16	14	15	16	17	18	19	20	14	15	16
17	18	19	20	21	22	23	21	22	23	24	25	26	27	21	22	23
24	25	26	27	28	29	30	28			29	30	31		28	29	30
31														25	26	27

INTERNET ARCHIVE Explore more than 687 billion web pages saved over time

[DONATE](#) **WayBackMachine** <https://apps.wellness.dev.lifeomic.com/login|> [X](#)

Results: 50 100 500

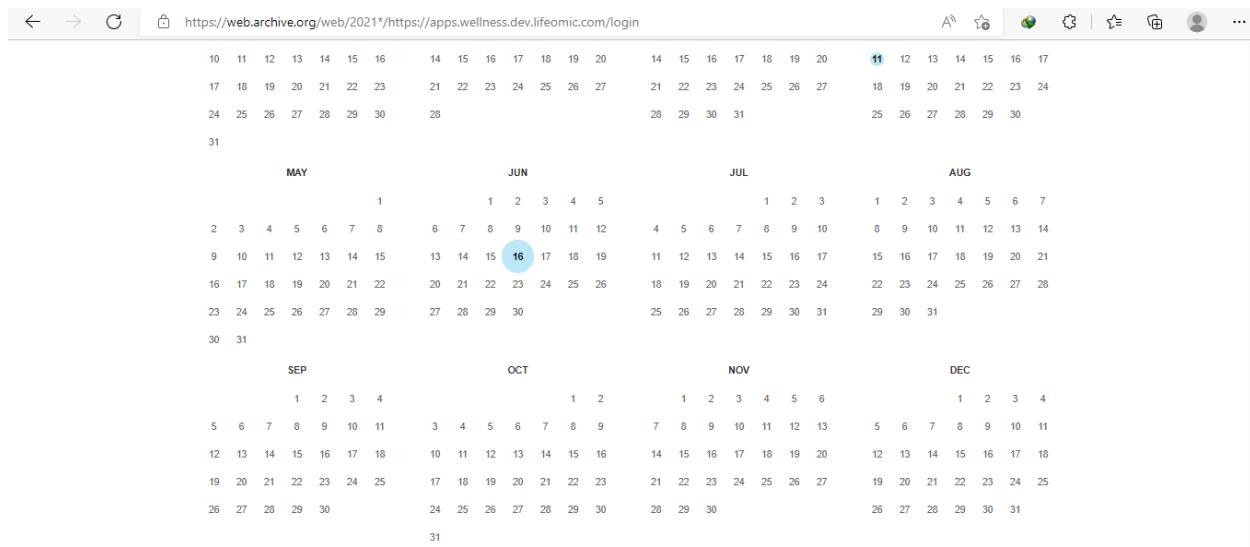
[Calendar](#) · [Collections](#) · [Changes](#) · [Summary](#) · [Site Map](#) · [URLs](#)

Saved 3 times between April 11, 2021 and June 16, 2021.

1999 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

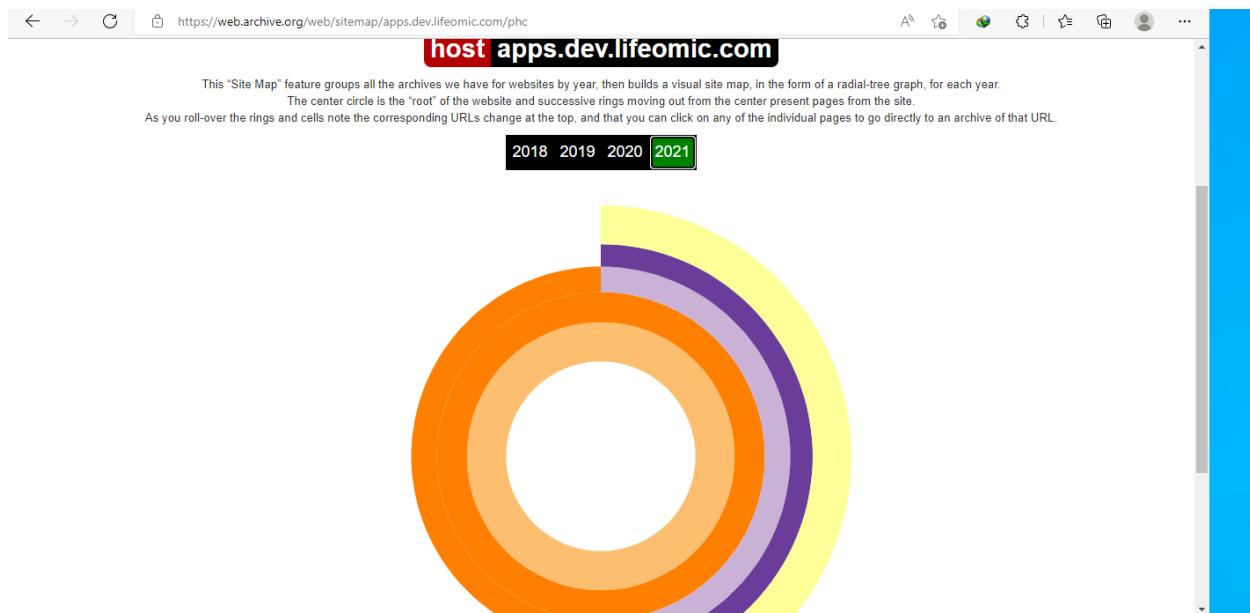
1	2	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3
3	4	5	6	7	8	9	7	8	9	10	11	12	13	7	8	9
10	11	12	13	14	15	16	14	15	16	17	18	19	20	14	15	16
17	18	19	20	21	22	23	21	22	23	24	25	26	27	21	22	23
24	25	26	27	28	29	30	28			29	30	31		28	29	30
31														25	26	27



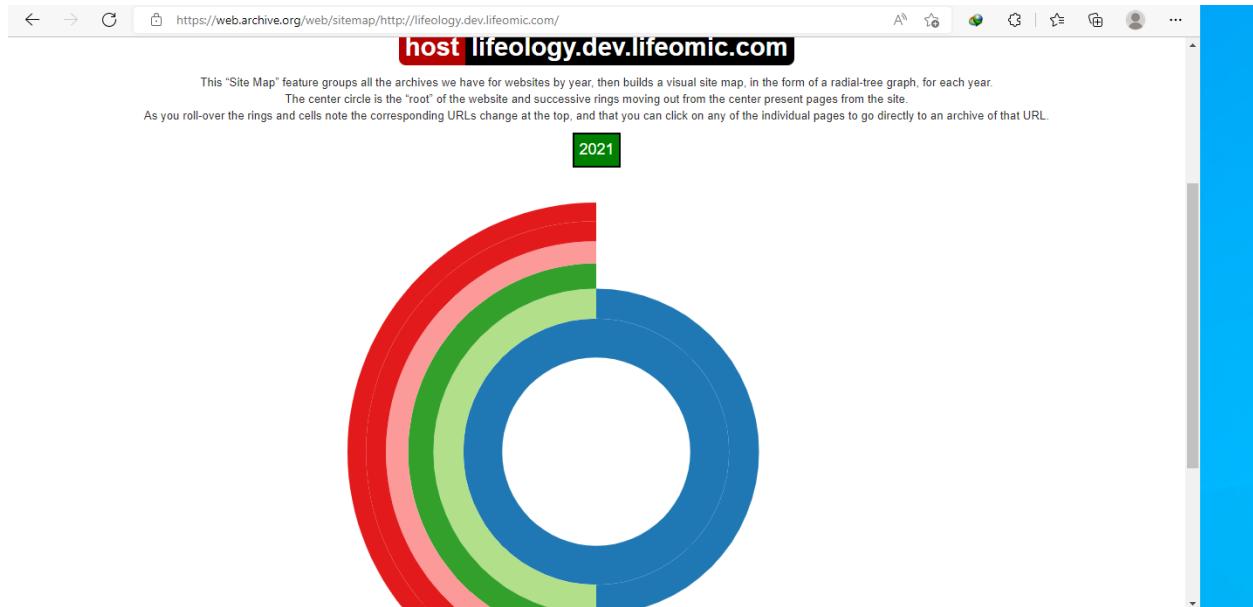
Note

This calendar view maps the number of times <https://apps.wellness.dev.lifeomic.com/login> was crawled by the Wayback Machine, *not* how many times the site was actually updated. More info in the [FAQ](#).

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>

```
(kali㉿kali)-[~]
└─$ git clone https://github.com/tomnomnom/waybackurls
Cloning into 'waybackurls'...
remote: Enumerating objects: 44, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 44 (delta 1), reused 6 (delta 1), pack-reused 36
Receiving objects: 100% (44/44), 9.76 KiB | 3.25 MiB/s, done.
Resolving deltas: 100% (15/15), done.

(kali㉿kali)-[~]
└─$ ls
bbht  Desktop  Documents  domains.txt  Downloads  go  httpprobe  Music  Pictures  Public  SubDomainizer  Templates  tools  Videos  waybackurls
└─$ kali@kali: ~/waybackurls
File Actions Edit View Help

(kali㉿kali)-[~/waybackurls]
└─$ sudo apt-get install golang
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
golang is already the newest version (2:1.18-3).
The following packages were automatically installed and are no longer required:
gccgo-12 libdav1d5 libdrm-intel libgo-12-dev libgo21 python3-distlib python3-filelock python3-pip-whl python3-platformdirs python3-setuptools-whl python3-wheel
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

(kali㉿kali)-[~/waybackurls]
└─$ ls
go.mod main.go README.md script
└─$ go build main.go
└─$ mv main waybackurls
└─$ ls
go.mod main.go README.md script 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.

A   https://dns-lookup.com

DNS-Lookup - The Professional Domain Name System (DNS) & IP Lookup Checker Tool 

 **HUNTED**
And Killed for his Casque
©TIM PLOWDEN CR Helmeted Hornbill 

Lookup

Enter the URL of your site and click **Lookup**.

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.

Domain – marketplace.dev.lifeomic.com

Value
2600:9000:210b:a000:11:9ee5:42c0:93a1
2600:9000:210b:6400:11:9ee5:42c0:93a1
2600:9000:210b:9200:11:9ee5:42c0:93a1
AAAA
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

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 Name System, 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.
 - **NS (Name Server)** - Used to specify which authoritative name servers are responsible for a given host.

Domain – apps.dev.skillspring.com

<https://dns-lookup.com/apps.dev.skillspring.com>

DNS Information for apps.dev.skillspring.com

	Value
AAAA	2600:9000:210b:e00:5:47f0:d700:93a1
	2600:9000:210b:2c00:5:47f0:d700:93a1
	2600:9000:210b:3200:5:47f0:d700:93a1
AAAA	2600:9000:210b:c800:5:47f0:d700:93a1
	2600:9000:210b:6e00:5:47f0:d700:93a1
	2600:9000:210b:8000:5:47f0:d700:93a1
	2600:9000:210b:dc00:5:47f0:d700:93a1
	2600:9000:210b:6200:5:47f0:d700:93a1

	Value
A	99.84.37.119
	99.84.37.108
	99.84.37.15

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 Name System, 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 – <https://apps.wellness.dev.lifeomic.com>

<https://dns-lookup.com/apps.wellness.dev.lifeomic.com>

DNS Information for apps.wellness.dev.lifeomic.com

	Value
A	99.84.126.30 99.84.126.25 99.84.126.38 99.84.126.128

	Value
AAAA	2600:9000:2162:fa00:14:87e2:5ac0:93a1 2600:9000:2162:5c00:14:87e2:5ac0:93a1 2600:9000:2162:a800:14:87e2:5ac0:93a1 2600:9000:2162:3800:14:87e2:5ac0:93a1 2600:9000:2162:0:14:87e2:5ac0:93a1 2600:9000:2162:8600:14:87e2:5ac0:93a1 2600:9000:2162:9200:14:87e2:5ac0:93a1

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 Name System, 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.
- **NS (Name Server)** - Used to specify an authoritative name server for a given host.

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

<https://dns-lookup.com/lifeology.dev.lifeomic.com>

DNS Information for lifeology.dev.lifeomic.com

	Value
AAAA	2600:9000:21dd:2e00:e:d841:6fc0:93a1
	2600:9000:21dd:600:e:d841:6fc0:93a1
	2600:9000:21dd:6800:e:d841:6fc0:93a1
	2600:9000:21dd:8c00:e:d841:6fc0:93a1
	2600:9000:21dd:c800:e:d841:6fc0:93a1
	2600:9000:21dd:5a00:e:d841:6fc0:93a1
	2600:9000:21dd:6000:e:d841:6fc0:93a1
	2600:9000:21dd:9200:e:d841:6fc0:93a1

	Value
A	13.226.39.6
	13.226.39.122
	13.226.39.47

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 Name System, 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.
- **NS (Name Server)** - Used to specify an authoritative name server for a given host.

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>

```
(kali㉿kali)-[~]
$ whatweb -v https://apps.wellness.dev.lifeomic.com
WhatWeb report for https://apps.wellness.dev.lifeomic.com
Status : 302 Found
Title  : <None>
IP    : 54.230.112.6
Country : UNITED STATES, US

Summary : CloudFront, HTTPServer[CloudFront], RedirectLocation[/admin], UncommonHeaders[x-amz-apigw-id,x-amzn-requestid,x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 9c5cc34178b30326464fbbe2768215f0.cloudflare.net (CloudFront)]

Detected Plugins:
[ CloudFront ]
  CloudFront Server

[ HTTPServer ]
  HTTP server header string. This plugin also attempts to identify the operating system from the server header.
  String      : CloudFront (from server string)

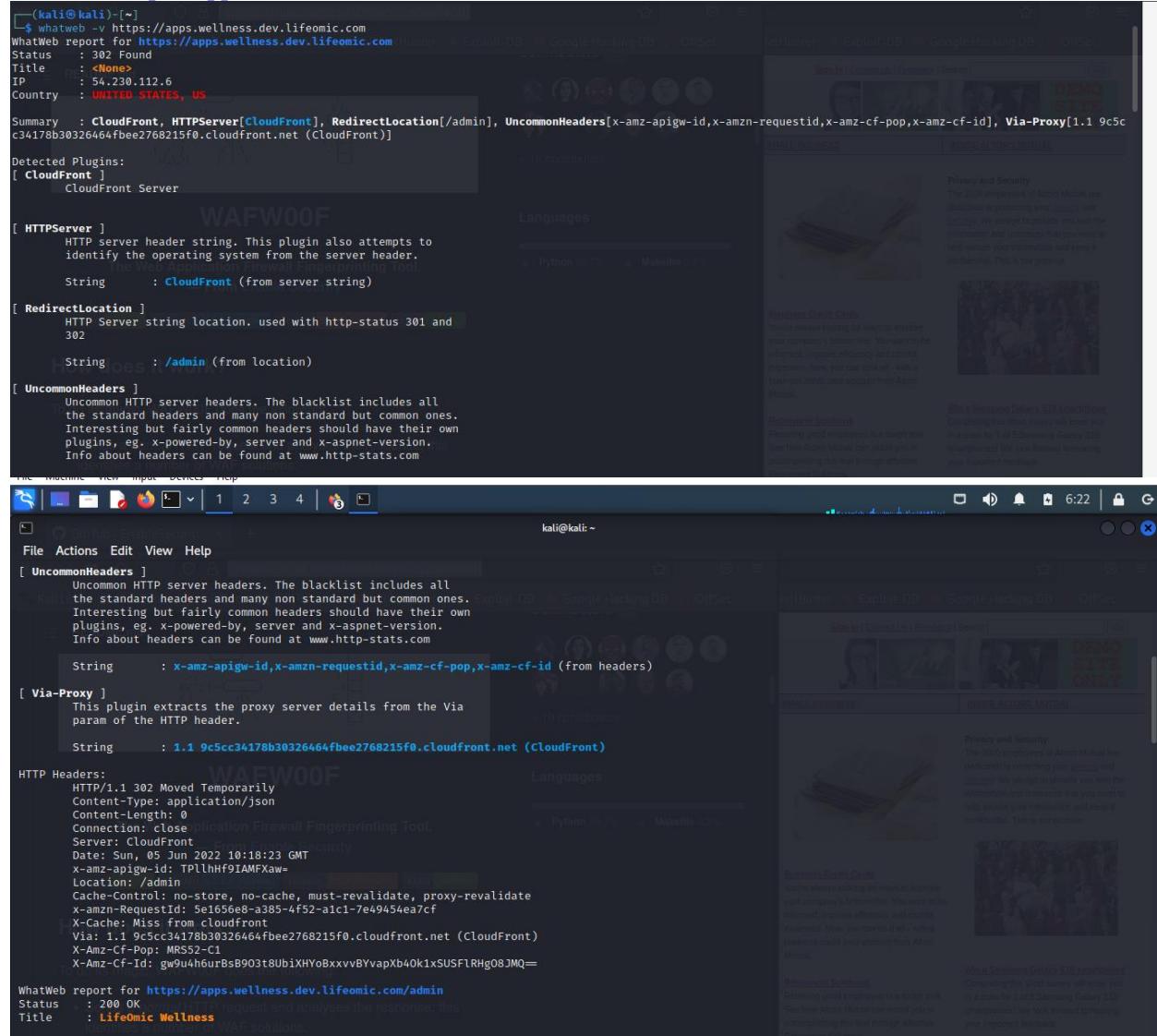
[ RedirectLocation ]
  HTTP Server string location. used with http-status 301 and 302
  String      : /admin (from location)

[ 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-aspen-version.
  Info about headers can be found at www.http-stats.com
  String      : x-amz-apigw-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 9c5cc34178b30326464fbbe2768215f0.cloudflare.net (CloudFront)

HTTP Headers:
HTTP/1.1 302 Moved Temporarily
Content-Type: application/json
Content-Length: 0
Connection: close
Server: CloudFront
Date: Sun, 05 Jun 2022 10:18:23 GMT
X-Amz-Apigw-Id: TPl1HHf9IAmFxaw=
Location: /admin
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
X-Amzn-Requestid: 5e1656e8-a385-4f52-a1c1-7e49454ea7cf
X-Cache: Miss from cloudfront
Via: 1.1 9c5cc34178b30326464fbbe2768215f0.cloudflare.net (CloudFront)
X-Amz-Cf-Pop: MRSS2-C1
X-Amz-Cf-Id: gw9u4h6urBsB903t8UbiXHYoBxxvvBYvapXb4Ok1xSUSFLRHg08JMQ==

WhatWeb report for https://apps.wellness.dev.lifeomic.com/admin
Status : 200 OK
Title  : LifeOmic Wellness
```



```

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 ] The Web Application Firewall Fingerprinting Tool.
    CloudFront Server — From Enable Security.

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

[ How does it work? ]
[ HTTPServer ]
    HTTP server header string. This plugin also attempts to
    identify the operating system from the server header.
    To do this it will attempt to match the following
    String : CloudFront (from server string)

[ Script ]
    This plugin sends a community request and analyzes the response; this
    includes a number of WAF solutions.

[ 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://www.html5rocks.com/en/mobile/x-frame-options
    http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.


```

The screenshot shows the WhatWeb report interface. On the left, a large text area displays the detected plugins and their configurations. On the right, there are two side-by-side preview windows of the target website's content. The top window shows a page with sections like 'Privacy and Security' and 'Business Credit Cards'. The bottom window shows a similar page with sections like 'Retirement Solutions' and 'Win a Samsung Galaxy S10 smartphone'. Both windows include small icons and navigation links.

```

[+] Quantum Entomology - + kali@kali: ~
File Actions Edit View Help

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

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

[ X-XSS-Protection ]
  This plugin retrieves the X-XSS-Protection value from the
  HTTP header. - More Info:
  http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.aspx
  String      : 1; mode=block

HTTP Headers:
  HTTP/1.1 200 OK
  Content-Type: text/html; charset=utf-8
  Transfer-Encoding: chunked
  Connection: close
  Server: CloudFront
  Date: Sun, 05 Jun 2022 10:18:27 GMT
  referrer-policy: strict-origin
  x-dns-prefetch-control: off
  x-xss-protection: 1; mode=block
  To do its magic, WAFW00F does the following:
  Analyses a number of WAF solutions

[+] GitHub - EnableSecurity/wafw00f - + kali@kali: ~
File Actions Edit View Help
  String      : 1; mode=block

HTTP Headers:
  HTTP/1.1 200 OK
  Content-Type: text/html; charset=utf-8
  Transfer-Encoding: chunked
  Connection: close
  Server: CloudFront
  Date: Sun, 05 Jun 2022 10:18:27 GMT
  referrer-policy: strict-origin
  x-dns-prefetch-control: off
  x-xss-protection: 1; mode=block
  surrogate-control: no-store
  strict-transport-security: max-age=15552000; includeSubDomains
  x-frame-options: DENY
  x-amzn-Remapped-content-length: 3896
  x-download-options: noopener
  x-amz-apigw-id: TPlMBH0TIAmF8Gw=
  Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
  x-content-type-options: nosniff
  Expires: 0
  X-Amzn-Trace-Id: Root-1-629c82f3-2d0d24f0590125920eb88bfa; Sampled=1
  Pragma: no-cache
  x-amzn-RequestId: 109b8a33-7a19-4f12-a7a9-77725d2f49b8
  Content-Encoding: gzip
  Vary: Accept-Encoding
  X-Cache: Miss from cloudfront
  Via: 1.1 3b4d1163775ea43e2848ada2f6a68950.cloudfront.net (CloudFront)
  X-Amz-Cf-Pop: MRS52-C1
  X-Amz-Cf-Id: h_Vd3MaYbmMovxFZkI3L30uZh_NxTPfp_VCfidgcV3r2p1M05qRFmw==

  To do its magic, WAFW00F does the following:
  Analyses a number of WAF solutions

```

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/wafw00fNetHunter
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.
```

A screenshot of a terminal window titled '(kali㉿kali)-[~/wafw00f]'. The command '\$ wafw00f' has been entered. The output is a colorful ASCII art representation of a dog's head and body, with various HTTP error codes overlaid: '404 Hack Not Found', '405 Not Allowed', '403 Forbidden tool', '502 Bad Gateway', and '500 Internal Error'. Below the dog art, the text '~ WAFW00F : v2.1.0 ~' and 'The Web Application Firewall Fingerprinting Toolkit' is displayed. At the bottom, usage instructions are provided: 'Usage: wafw00f url1 [url2 [url3 ...]]' and 'example: wafw00f http://www.victim.org/'.

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

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

[!] WAFW00F v2.1.0 - The Web Application Firewall Fingerprinting Toolkit
[!] From Enable Security
[!] Version: v2.1.0 (stable) License: MIT-GPLv3 Build: Passsing

~ 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>

```
(kali㉿kali)-[~/wafw00f]
$ wafw00f https://lifeology.dev.lifeomic.com
```

WAFW00F
The Web Application Firewall Fingerprinting Tool.
From Enable Secu...
Woof!

~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://lifeology.dev.lifeomic.com
[+] The site <https://lifeology.dev.lifeomic.com> is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2

+ 19 contributors
Languages
Python 99.7% Makefile 0.3%
Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Allianz Mutual.
Retirement Solutions

Domain – apps.dev.lifeomic.com/phc

```
(kali㉿kali)-[~/wafw00f]
$ wafw00f apps.dev.lifeomic.com/phc
```

WAFW00F
The Web Application Firewall Fingerprinting Tool.
From Enable Secu...
Woof!

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.dev.lifeomic.com/phc
[+] The site <https://apps.dev.lifeomic.com/phc> is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2

+ 19 contributors
Languages
Python 99.7% Makefile 0.3%
Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Allianz Mutual.
Retirement Solutions

Domain – apps.dev.skillspring.com

```
(kali㉿kali)-[~/wafw00f]
$ wafw00f https://apps.dev.skillspring.com
```

WAFW00F
The Web Application Firewall Fingerprinting Tool.
From Enable Secu...
Woof!

~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://apps.dev.skillspring.com
[+] The site <https://apps.dev.skillspring.com> is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2

+ 19 contributors
Languages
Python 99.7% Makefile 0.3%
Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Allianz Mutual.
Retirement Solutions

Domain – marketplace.dev.lifeomic.com

(kali㉿kali)-[~/wafw00f]\$ wafw00f https://marketplace.dev.lifeomic.com

WAFW00F

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error

The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://marketplace.dev.lifeomic.com
[+] The site https://marketplace.dev.lifeomic.com is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2

Vulnerability Assessment

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 Suite Professional v2021.10.3 - Temporary Project - licensed to bewhale

Tasks

- Running
- Paused
- Finished
- Live task
- Scan
- Intruder attack

Issue activity

#	Task	Time	Action	Issue type	Host
14	3	10:29:54 4 Jun 2022	Issue found	DOM data manipulation (DOM-based)	https://marketplace.../re
13	3	10:29:54 4 Jun 2022	Issue found	Link manipulation (DOM-based)	https://marketplace.../s/
12	3	10:29:54 4 Jun 2022	Issue found	DOM data manipulation (DOM-based)	https://marketplace.../s/
11	3	10:29:54 4 Jun 2022	Issue found	DOM data manipulation (DOM-based)	https://marketplace.../rc
10	3	10:29:54 4 Jun 2022	Issue found	DOM data manipulation (DOM-based)	https://marketplace.../s/
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.../s/
7	3	10:25:20 4 Jun 2022	Issue found	Email addresses disclosed	https://marketplace.../s/
6	3	10:25:20 4 Jun 2022	Issue found	Cacheable HTTPS response	https://marketplace.../s/
5	3	10:25:20 4 Jun 2022	Issue found	Cross-domain Referer leakage	https://marketplace.../s/
4	3	10:25:20 4 Jun 2022	Issue found	Cross-domain Referer leakage	https://marketplace.../s/
3	3	10:25:20 4 Jun 2022	Issue found	Cross-domain Referer leakage	https://marketplace.../s/
2	3	10:25:20 4 Jun 2022	Issue found	Cacheable HTTPS response	https://marketplace.../s/
1	2	10:25:14 4 Jun 2022	Issue found	TLS certificate	https://marketplace.../

Event log

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/f/a931512-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.burpsuite.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

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



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 Suite Professional v2021.10.3 - Temporary Project - licensed to bwhale

Tasks

- 2. Live audit from Proxy (all traffic)
- Audit checks - passive
- Capturing:
- Issues: 0 (0 errors)
- View details >
- 3. Crawl and audit of lifeology.dev.lifeomic.com
- Default configuration
- Auditing: 25m 12s remaining
- 8117 requests (5 errors)
- 12 locations crawled View details >

Event log

Time	Type	Source	Message
13:12:44 Jun 2022	Info	Task 3	Discarding log entries as Logger memory limit reached.
12:56:14 Jun 2022	Error	Task -1	Communication error: lifeology.dev.lifeomic.com
12:55:46 Jun 2022	Info	Task 3	Audit started.
12:55:46 Jun 2022	Info	Task 3	Identifying items to audit.
12:55:46 Jun 2022	Info	Task 3	Crawl completed.
12:50:18 Jun 2022	Info	Task 3	fonts.gstatic.com is using HTTP/2
12:50:15 Jun 2022	Info	Task 3	js.stripe.com is using HTTP/2
12:50:15 Jun 2022	Info	Task 3	sessions.bugsnag.com is using HTTP/2
12:50:11 Jun 2022	Info	Task 3	fonts.googleapis.com is using HTTP/2
12:50:11 Jun 2022	Info	Task 3	cdnjs.cloudflare.com is using HTTP/2
12:50:09 Jun 2022	Info	Task 3	lifeology.dev.lifeomic.com is using HTTP/2
12:49:54 Jun 2022	Info	Task 3	Crawl started.
12:49:54 Jun 2022	Info	Suite	This version of Burp Suite was released over three months ago. Please consider Proxyscience https://proxyscience.com.
12:49:11 Jun 2022	Info	Proxy	Proxy service started on 177.0.0.1:8080

Issue activity

Task	Time	Action	Issue type	Host
18	3	13:11:07 4 Jun 2022	Issue found	① Cross-origin resource sharing https://lifeology.dev... /lc
17	3	13:11:07 4 Jun 2022	Issue found	② Cross-origin resource sharing: arbitrary ... https://lifeology.dev... /lc
16	3	13:09:44 4 Jun 2022	Issue found	③ Cross-origin resource sharing https://lifeology.dev... /lc
15	3	13:09:44 4 Jun 2022	Issue found	④ Cross-origin resource sharing: arbitrary ... https://lifeology.dev... /lc
14	3	13:05:52 4 Jun 2022	Issue found	⑤ Backup file https://lifeology.dev... /st
13	3	12:57:36 4 Jun 2022	Issue found	⑥ Open redirection (DOM-based) https://lifeology.dev... /lc
12	3	12:57:36 4 Jun 2022	Issue found	⑦ Open redirection (DOM-based) https://lifeology.dev... /lc
11	3	12:57:05 4 Jun 2022	Issue found	⑧ Open redirection (DOM-based) https://lifeology.dev... /lc
10	3	12:57:05 4 Jun 2022	Issue found	⑨ Open redirection (DOM-based) https://lifeology.dev... /lc
9	3	12:56:51 4 Jun 2022	Issue found	⑩ Open redirection (DOM-based) https://lifeology.dev... /lc
8	3	12:56:51 4 Jun 2022	Issue found	⑪ Open redirection (DOM-based) https://lifeology.dev... /lc
7	3	12:55:54 4 Jun 2022	Issue found	⑫ Strict transport security not enforced https://lifeology.dev... /lc
6	3	12:55:54 4 Jun 2022	Issue found	⑬ Cacheable HTTPS response https://lifeology.dev... /st
5	3	12:55:54 4 Jun 2022	Issue found	⑭ Email address disclosure https://lifeology.dev... /lc

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.

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

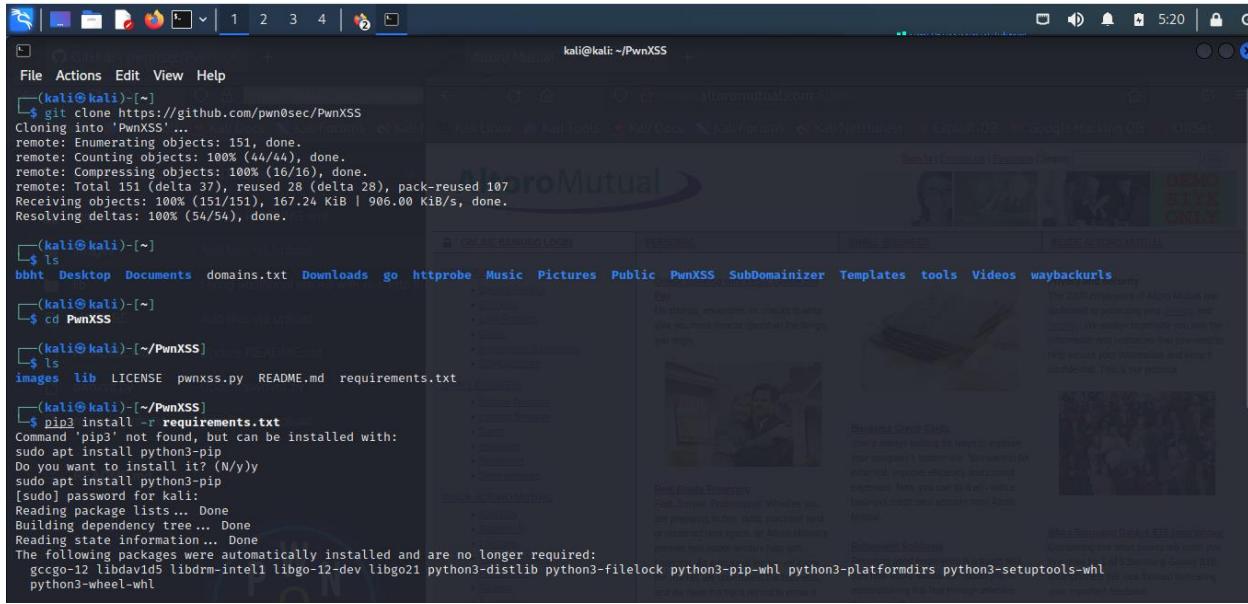
- [CWE-601: URL Redirection to Untrusted Site \('Open Redirect'\)](#)

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>



```
(kali㉿kali)-[~]
└─$ git clone https://github.com/pwn0sec/PwnXSS
Cloning into 'PwnXSS'...
remote: Enumerating objects: 151, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 151 (delta 37), reused 28 (delta 28), pack-reused 107
Receiving objects: 100% (151/151), 167.24 KiB | 906.00 KiB/s, done.
Resolving deltas: 100% (54/54), done.

(kali㉿kali)-[~]
└─$ ls
bbht Desktop Documents domains.txt Downloads go httpprobe Music Pictures Public PwnXSS SubDomainizer Templates tools Videos waybackurls

(kali㉿kali)-[~]
└─$ cd PwnXSS

(kali㉿kali)-[~/PwnXSS]
└─$ ls
images lib LICENSE pwnxss.py README.md requirements.txt

(kali㉿kali)-[~/PwnXSS]
└─$ pip3 install -r requirements.txt
Command 'pip3' not found, but can be installed with:
sudo apt install python3-pip
Do you want to install it? (N/y)
sudo apt install python3-pip
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
gccgo-12 libdav1d libdrm-intel1 libgo-12-dev libgo21 python3-distlib python3-filelock python3-pip-whl python3-platformdirs python3-setuptools-whl
python3-wheel-whl
```

Target domain – marketplace.dev.lifeomic.com

```
(kali㉿kali)-[~/PwnXSS]
$ python3 pwnxss.py -u https://marketplace.dev.lifeomic.com
[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] 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] 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] 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] 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
```

```

kali㉿kali: ~/PwnXSS
File Actions Edit View Help
[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
*****
[05:28:28] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/resource/fd56ffcf-8ed8-4594-ac87-a9788608014c
[05:28:29] [INFO] Connection established 200
[05:28:29] [WARNING] Found link with query: c=REPORT_EXTRACTOR Maybe a vuln XSS point
[05:28:29] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=<script>alert(document.cookie)</script>
[05:28:29] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[05:28:31] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[05:28:32] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/fd56ffcf-8ed8-4594-ac87-a9788608014c/install
[05:28:33] [INFO] Connection failed 404
*****
[05:28:34] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/search?c=REPORT_EXTRACTOR
[05:28:35] [INFO] Connection established 200
*****
[05:28:36] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/resource/fa931512-d8be-453e-82d4-e0d8a2cd0be7
[05:28:37] [INFO] Connection established 200
[05:28:37] [WARNING] Found link with query: c=SEARCH_LAYOUT Maybe a vuln XSS point
[05:28:37] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=<script>alert(document.cookie)</script>
[05:28:37] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[05:28:38] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[05:28:40] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/fa931512-d8be-453e-82d4-e0d8a2cd0be7/install
[05:28:41] [INFO] Connection failed 404
*****
[05:28:42] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/search?c=SEARCH_LAYOUT
[05:28:43] [INFO] Connection established 200
*****
[05:28:44] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/resource/f0ff0538-b554-4962-9f5e-55e2e814fdb8
[05:28:45] [INFO] Connection established 200
[05:28:45] [WARNING] Found link with query: c=APP_TILE Maybe a vuln XSS point
[05:28:45] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[05:28:37] [INFO] Connection established 200
[05:28:37] [WARNING] Found link with query: c=SEARCH_LAYOUT Maybe a vuln XSS point
[05:28:37] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=<script>alert(document.cookie)</script>
[05:28:37] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[05:28:38] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[05:28:40] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/fa931512-d8be-453e-82d4-e0d8a2cd0be7/install
[05:28:41] [INFO] Connection failed 404
*****
[05:28:42] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/search?c=SEARCH_LAYOUT
[05:28:43] [INFO] Connection established 200
*****
[05:28:44] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/resource/f0ff0538-b554-4962-9f5e-55e2e814fdb8
[05:28:45] [INFO] Connection established 200
[05:28:45] [WARNING] Found link with query: c=APP_TILE Maybe a vuln XSS point
[05:28:45] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=<script>alert(document.cookie)</script>
[05:28:45] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[05:28:46] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[05:28:48] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/search?c=APP_TILE
[05:28:49] [INFO] Connection established 200
*****
[05:28:50] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/resource/f9e641d2-2884-41b2-a698-5ddb83db1f29
[05:28:51] [INFO] Connection established 200
[05:28:51] [WARNING] Found link with query: c=REPORT_EXTRACTOR Maybe a vuln XSS point
[05:28:51] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=<script>alert(document.cookie)</script>
[05:28:51] [INFO] Query (GET) : https://marketplace.dev.lifeomic.com/search?c=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[05:28:52] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[05:28:54] [INFO] Checking connection to: https://marketplace.dev.lifeomic.com/f9e641d2-2884-41b2-a698-5ddb83db1f29/install
[05:28:55] [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.

```
(kali㉿kali)-[~/PwnXSS]
$ python3 pwnxss.py -u https://lifeology.dev.lifeomic.com
PWNXSS {v0.5 Final}
https://github.com/pwn0sec/PwnXSS

<<<<< STARTING >>>>>

[05:26:38] [INFO] Starting PwnXSS ...
*****
[05:26:38] [INFO] Checking connection to: https://lifeology.dev.lifeomic.com
[05:26:40] [INFO] Connection established 200

(kali㉿kali)-[~/PwnXSS]
$ python3 pwnxss.py -u https://apps.dev.lifeomic.com/phc
PWNXSS {v0.5 Final}
https://github.com/pwn0sec/PwnXSS

<<<<< STARTING >>>>>

[05:44:25] [INFO] Starting PwnXSS ...
*****
[05:44:25] [INFO] Checking connection to: https://apps.dev.lifeomic.com/phc
[05:44:26] [INFO] Connection established 200

(kali㉿kali)-[~/PwnXSS]
$ python3 pwnxss.py -u https://apps.dev.skillspring.com
PWNXSS {v0.5 Final}
https://github.com/pwn0sec/PwnXSS

<<<<< STARTING >>>>>

[05:42:08] [INFO] Starting PwnXSS ...
*****
[05:42:08] [INFO] Checking connection to: https://apps.dev.skillspring.com
[05:42:10] [INFO] Connection established 200

(kali㉿kali)-[~/PwnXSS]
$ python3 pwnxss.py -u https://apps.wellness.dev.lifeomic.com
PWNXSS {v0.5 Final}
https://github.com/pwn0sec/PwnXSS

<<<<< STARTING >>>>>

[05:24:24] [INFO] Starting PwnXSS ...
*****
[05:24:24] [INFO] Checking connection to: https://apps.wellness.dev.lifeomic.com
[05:24:26] [INFO] Connection established 200
```

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 \(zaproxy.org\)](https://www.zaproxy.org/)

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

The screenshot shows the OWASP ZAP 2.11.1 interface. The top window is titled "Automated Scan" and displays a message about launching an automated scan against an application. It includes fields for "URL to attack" (https://apps.wellness.dev.lifeomic.com), "Use traditional spider" (checked), and "Use ajax spider" (unchecked). The bottom windows show the "Alerts" and "Response" panes. The "Alerts" pane lists five vulnerabilities under "Content Security Policy (CSP) Header Not Set" and "Cross-Domain Misconfiguration". The "Response" pane shows a raw HTTP response with a JSON error message: {"error": "Missing Authentication Token"}. The status bar at the bottom indicates "Primary Proxy: localhost:8080" and "Current Scans: 53".

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

The screenshot shows the Netsparker interface for scanning the URL apps.dev.skillspring.com. The main window displays a vulnerability titled "[Possible] Password Transmitted over Query String" with a severity of MEDIUM. The vulnerability details indicate that the application is transmitting passwords over a query string, specifically in the URL <https://apps.dev.skillspring.com/login?originalUrl=https://apps.dev.skillspring.com/app-switcher>. The notes mention that although a form with a GET method is detected, it may not be submitted directly and may be submitted using e.g. AJAX with POST method. The input name is identified as "password". The classification section shows scores for PCI DSS 3.2 (6.5.4), OWASP 2013 (A6), and OWASP 2017 (A3). The left sidebar shows a tree view of scanned files and folders, and the right sidebar contains a knowledge base and various audit metrics.

(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>

The screenshot shows the Netsparker application interface. The main title bar reads "lifeology.dev.lifeomic.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)". The top menu includes File, Home, View, Reporting, Help, Link Tools, Vulnerability Tools, and a search bar. The Vulnerability Tools section is active, showing icons for Retest, Generate Exploit, Execute SQL Commands, Get Shell, Exploit LFI, Short Names, Ignored from this Scan, Configure Send To Actions, Configure Web Application Firewall, and WAF Rules.

The central pane displays a scan result for "lifeology.dev.lifeomic.com:443 (48) .well-known". A prominent alert message says "[Possible] BREACH Attack Detected" with a "MEDIUM" severity rating. Below this, the "Certainty" is listed as ":", the "URL" is "https://lifeology.dev.lifeomic.com/auth/v1/social-idp?app=login&destination&identity_provider=Facebook&login-app-redirect-url=https://app.dev.lifeology.io/admin/courses&redirectDomain=%20WAITFOR%20DELAY%20'0:0:25'--&state=8d68ca58-dbda-4319-bbf7-26fa4ac0487&subdomain", and the "Reflected Parameter(s)" is "identity_provider".

The "Sensitive Keyword(s)" are "token,nonce". On the right side, there's a "CLASSIFICATION" section with entries for OWASP 2013 (A9), OWASP 2017 (A9), and CWE (310). A sidebar titled "Knowledge Base" lists various security topics like AJAX / XML HTTP Request, Cookies, and SSL.

(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

CONFIRMED MEDIUM

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

List of Supported Weak Ciphers :

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)

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.

<http://capec.mitre.org/data/definitions/217.html>

CLASSIFICATION	
PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217
WASC	4
ISO27001	

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 `regedit32` 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

marketplace.dev.lifeomic.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)

HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM

Certainty : ███████████

URL : <https://marketplace.dev.lifeomic.com/>

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

Issues - Previous Settings

Scanning finished.

Scan Finished | Previous Settings | Default Security Checks | Default Report Policy | Activity

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>