Journey of a Bounty Hunter

MY FIRST APPROACH INTO PENETRATION TESTING

ABSTRACT

An detailed guide of a basic web audit on behalf of an Assignment in Web Security Module of Year two Semester Two at SLIIT

Senarathne G.N.S. it20647346

Web Security – IE2062

Sri Lanka Institute of Information Technology

Web Audit Assignment

Web Security- IE2062

https://www.epam.com

Video Explanation: https://mysliit-my.sharepoint.com/:f:/g/personal/it20647346_my_sliit_lk/EnoUOH974INBumW5xiPeoeABDivymt3BzpfRNJ15bxmhfw?e=PTUbE

Submitted By:

Registration Number	Name
IT20647346	GNS Senarathne

Submitted on:

5th May 2022

Acknowledgement

I'd like to thank Dr. Lakmal Rupasinghe, the lecturer in charge of the Web Security module, and Miss Chethana Liyanapathirana for their excellent assistance and direction in completing this work.
Dr. Lakmal Rupasinghe's advice and clear explanations were especially helpful throughout the project's initial stages.

On the other side, the practical expertise provided by Miss Chathuri Udagedara was critical in completing this task. I'd want to thank them as well on this occasion.

Purpose

To secure the system's confidentiality, integrity, and availability, it's a critical need to conduct web audits and uncover any available security breachers and flows.

We were asked to undertake a web audit and bug bounty for the pre-selected platform with that goal in mind.

To select an appropriate flatform for doing the online audit, I refer to the https://www.hackerone.com bug bounty platform.

Finally, I decided to conduct this second year second semester Web Security module's project with the https://hackerone.com/epam-bbp?type=team.

Introduction

Web apps are an important part of every business. Without adequate web applications, an online firm would be unable to archive their cooperative goals. As a result, the company's web applications must be secured from cyberattacks and security flaw exploitation to keep operations running efficiently and uninterruptedly.

Bug bounty programs allow independent cybersecurity specialists to submit problems to corporations in exchange for awards or money. Security exploits and vulnerabilities are the most common types of defects, although they can also include process faults, hardware flaws, and other problems.

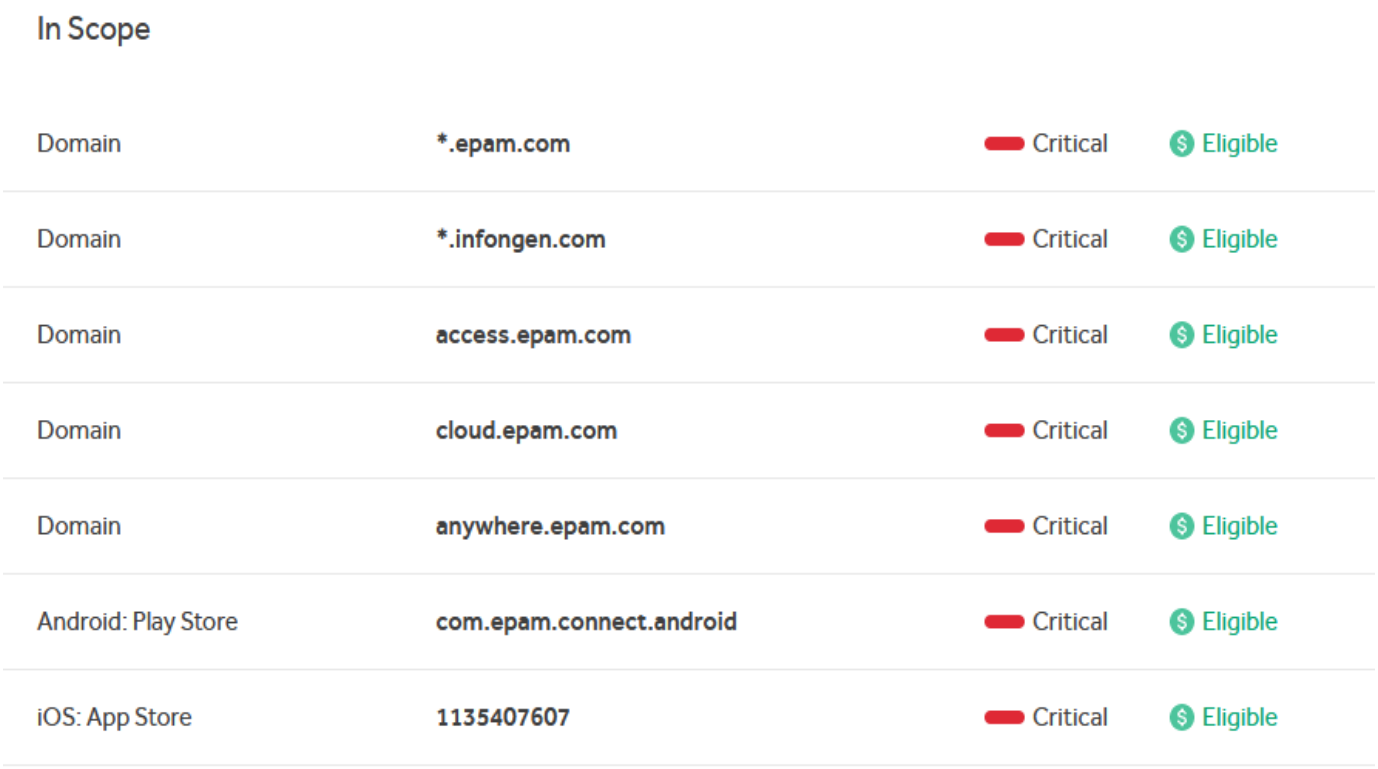
Normally, the reports are generated by a program managed by a third party. The organization will design a program that is specific to its requirements. Programs can be kept secret, and reports can be kept confidential or made public. They might happen over a predetermined length of time or without a set deadline.

In this report, I'll show you how I started my bug bounty adventure, as well as my biggest failures, as well as the first actions and tools I utilized to find the defect or weakness in the online application. The guidelines satisfied with suitable photos and thorough descriptions are provided under each section.

Scope

In scope Domains

As there are multiple domains available, I had to narrow down them to these main domains under this report. Below screenshot from hackerone.com will show the selected domains.



In Scope

Domain	*.epam.com	Critical	Eligible
Domain	*.infongen.com	Critical	Eligible
Domain	access.epam.com	Critical	Eligible
Domain	cloud.epam.com	Critical	Eligible
Domain	anywhere.epam.com	Critical	Eligible
Android: Play Store	com.epam.connect.android	Critical	Eligible
iOS: App Store	1135407607	Critical	Eligible

After selecting the domains, I have saved them all in “domains.txt” file as it is a must to have documentations in doing a web audit.

Out of Scope Domains

Following is a list of out-of-scope domains as mentioned in the hackerone.com.

- Domain - ethics.epam.com
- Domain - *.lab.epam.com
- Domain - ebn.epam.com
- Domain - carbon.epam.com
- Domain - ecsc00a03ba1.epam.com

Risk Level Information

Low	Medium	High	Critical
***.infongen.com**			
$50	$150	$300	$600
***.projects.epam.com**			
-	-	$300	$600
com.epam.connect.android			
$250	$500	$5,000	$10,000
1135407607			
$250	$500	$5,000	$10,000
access.epam.com			
$250	$500	$5,000	$10,000

Critical Severity

Critical Vulnerabilities are not limited to but include,

- Vulnerabilities that allow to execute arbitrary codes on the system.
- Mass PII (Personally Identifiable Information) leakage of the employees and customers of the company.
- Serious logical flaws in the system.

High Severity

High severity level vulnerabilities are not limited to but include,

- Sensitive information leakages such as SQL injection in non-core databases, API log replacements, sensitive information leaks because of GitHub information, hard coding, reversible encryption algorithm using or plaintext storing on server, compressed source code package leaks.
- Unauthorized access to sensitive data, such as unauthorized account actions to change key information, execute orders, change important service configurations, and so on.
- Other security flaws that have a big impact on users. Stored XSS and Blind XSS vulnerabilities on crucial pages that can automatically propagate and collect login credentials (Cookies) are examples of these.
- Unauthorized access to sensitive data, such as circumventing authentication to gain direct access to the management backend, weak backend passwords, and SSRF vulnerabilities that can be used to extract a huge amount of sensitive data from the internal network.

Medium Severity

Medium severity level vulnerabilities are not limited to but include,

- Users are affected by vulnerabilities that require interaction. Stored XSS and Reflected XSS (including Reflected DOM-XSS) vulnerabilities on common web pages, JSON Hijacking, and serious CSRF vulnerabilities are only a few examples.
- A password that was used to access the management backend was revealed to be weak.
- Unauthorized operations in general, such as changing user data and evading limitations to perform user operations.
- General faults in logical design and procedure, such as logic flaws that can be used to bypass the verification code and get access to sensitive systems, as well as bypassing constraints to perform credential stuffing attacks.
- Usual leakage of information, such as, web directory traversal, system directory traversal, and plain text password transmission over the HTTP.

Low Severity

Low severity level vulnerabilities are not limited to but include,

- Vulnerabilities that could be exploited to gain user identification information only in non-mainstream browser setups (such as IE6) Reflected XSS (including Reflected DOM-XSS) vulnerabilities and Stored XSS vulnerabilities for generic services are examples of these.
- On One Time Passwords, brute-force attacks and a lack of rate limitation are common (OTPs).
- Trivial information leakages such as path info leaks, SVN info leaks, PHP info leaks, leakage of log files, exception info leaks, config info leaks.
- Lack of rate limiting on sensitive functionality.
- Issues that are difficult to exploit but pose a security risk, such as using CSRF to turn a self-XSS into an exploited XSS, JSON Hijacking that has obtained sensitive information, clickjacking on input web pages containing sensitive information (a valid exploit must be provided in the vulnerability details), and remote code execution vulnerabilities that require man-in-the-middle attacks, all of which require an effective PoC.

- URL jumps, inappropriate system/service O&M setups, and component authorization flaws are among the other vulnerabilities that can only cause little damage.

Out of Scope Vulnerabilities

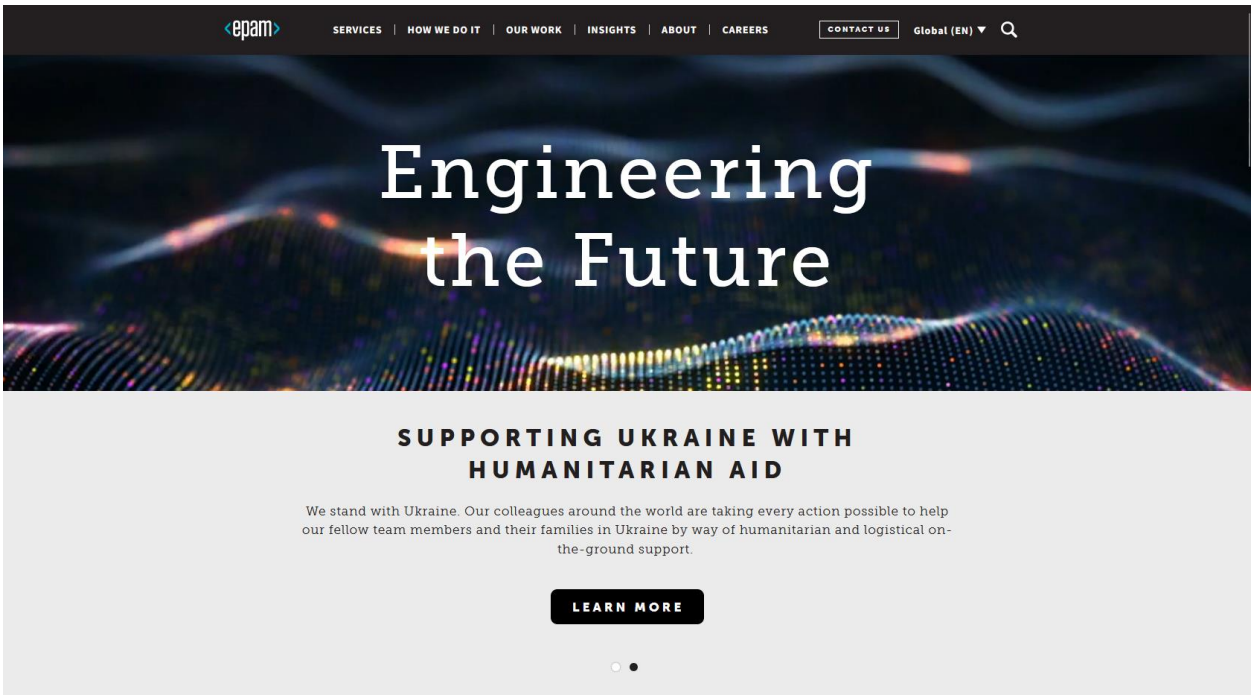
- Clickjacking
- Keys to the Google Maps API have been leaked or revealed.
- Interaction with a third-party service that hasn't yielded any results
- Problems with password complexity and length
- Post-based XSS that hasn't had any impact
- SSRF that hasn't had any influence is blind.
- Self-XSS with no discernible effect
- Unauthenticated forms or forms with no sensitive actions are vulnerable to Cross-Site Request Forgery (CSRF).
- Attacks that necessitate the usage of an MITM or physical access to a user's device.
- Libraries that were previously known to be susceptible but did not have a working Proof of Concept.
- Injection of Comma Separated Values (CSV) without revealing a vulnerability
- SSL/TLS configuration does not follow best practices.
- Any behavior that could cause our service to be disrupted (DoS).
- Issues with content spoofing and text injection without a known attack vector or the ability to edit HTML/CSS
- Issues with rate limiting or brute force
- Content Security Policy is lacking in best practices.
- Cookies with no HttpOnly or Secure flags
- Email best practices are being overlooked.
- (SPF/DKIM/DMARC records that are invalid, partial, or missing, for example.)
- Only users of obsolete or unpatched browsers are vulnerable.
  [Within 2 stable versions of the most recently released stable version]

- Issues with banner identification / Software version disclosure
- Error messages or headers that are descriptive (e.g., stack traces, application, or server errors).

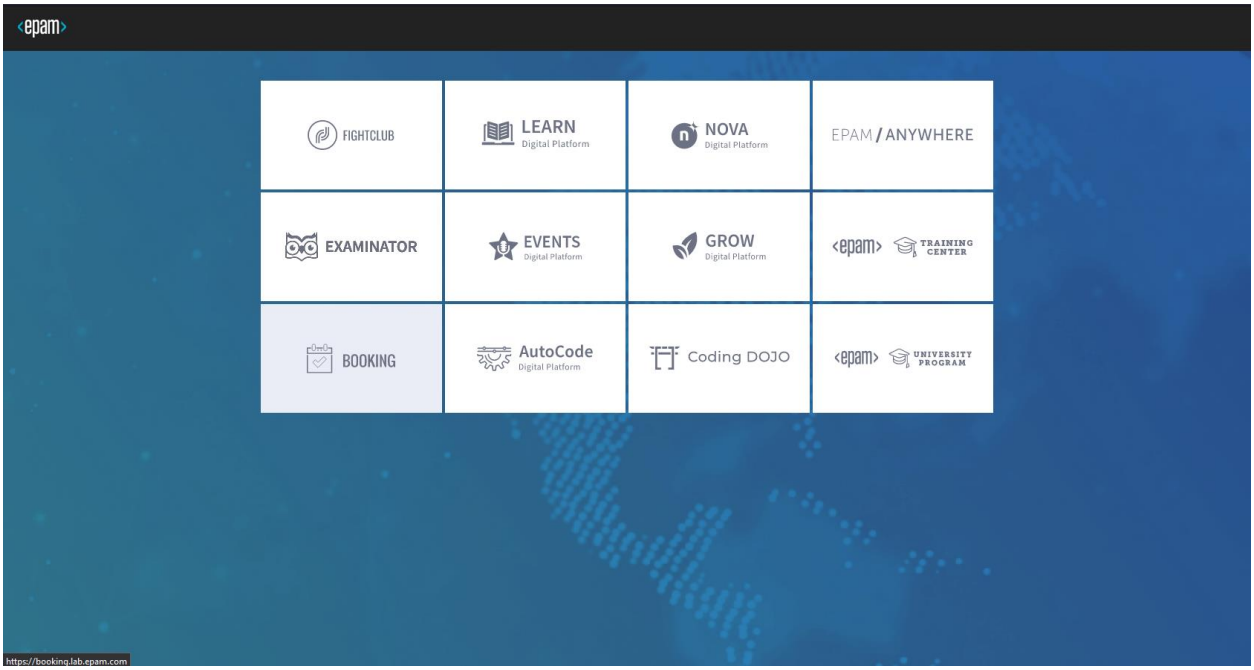
Information Gathering

To begin, I browsed in scope domains to render their webpages in order to identify the contents and basic behaviors of the webpages.

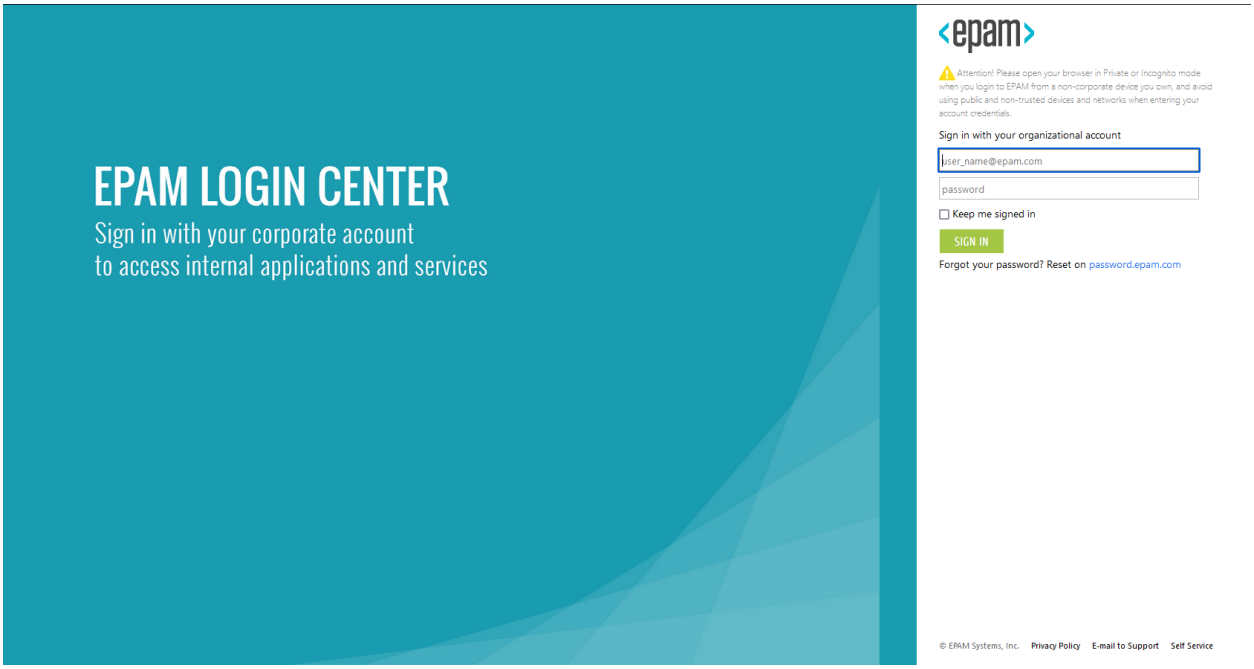
1. *.epam.com



2. access.epam.com

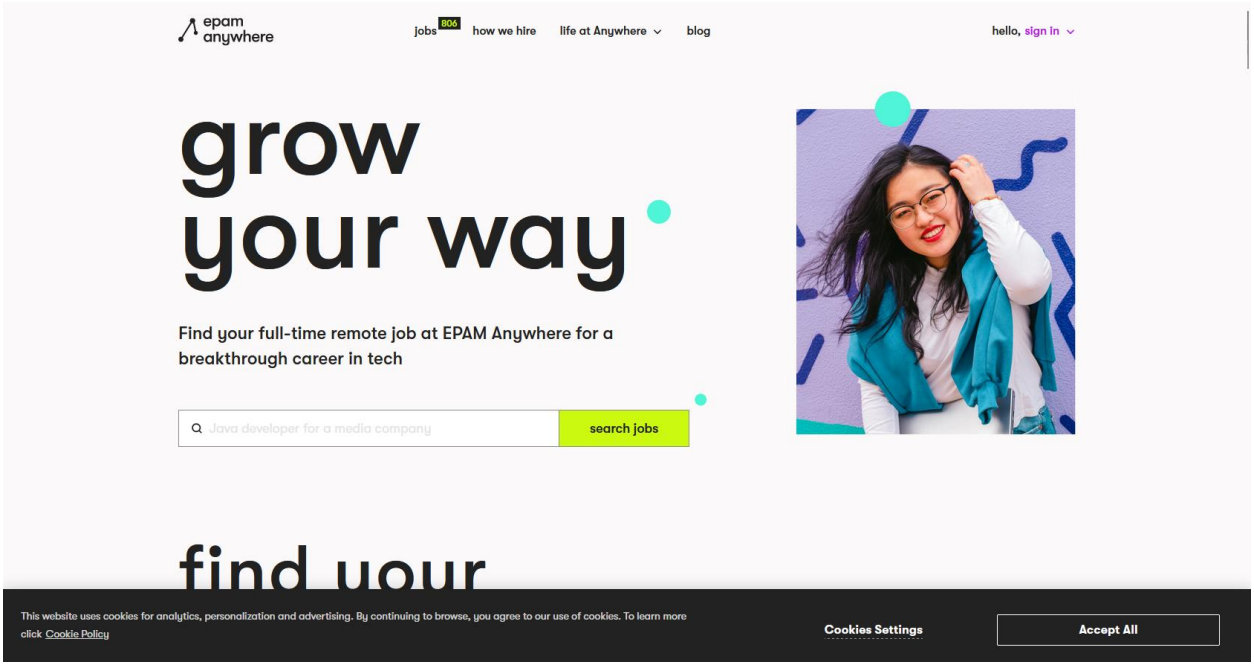


3. cloud.epam.com

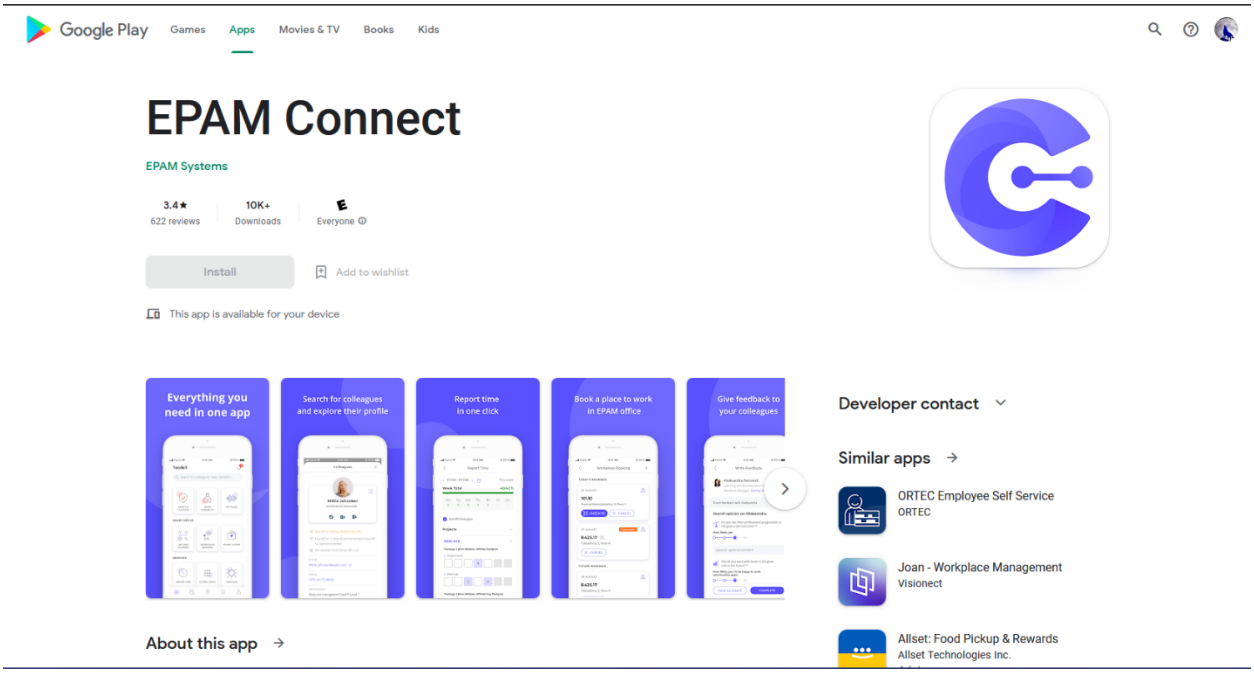


When requesting the cloud.epam.com it is internally redirected to https://www.login.epam.com/ .

4. anywhere.epam.com

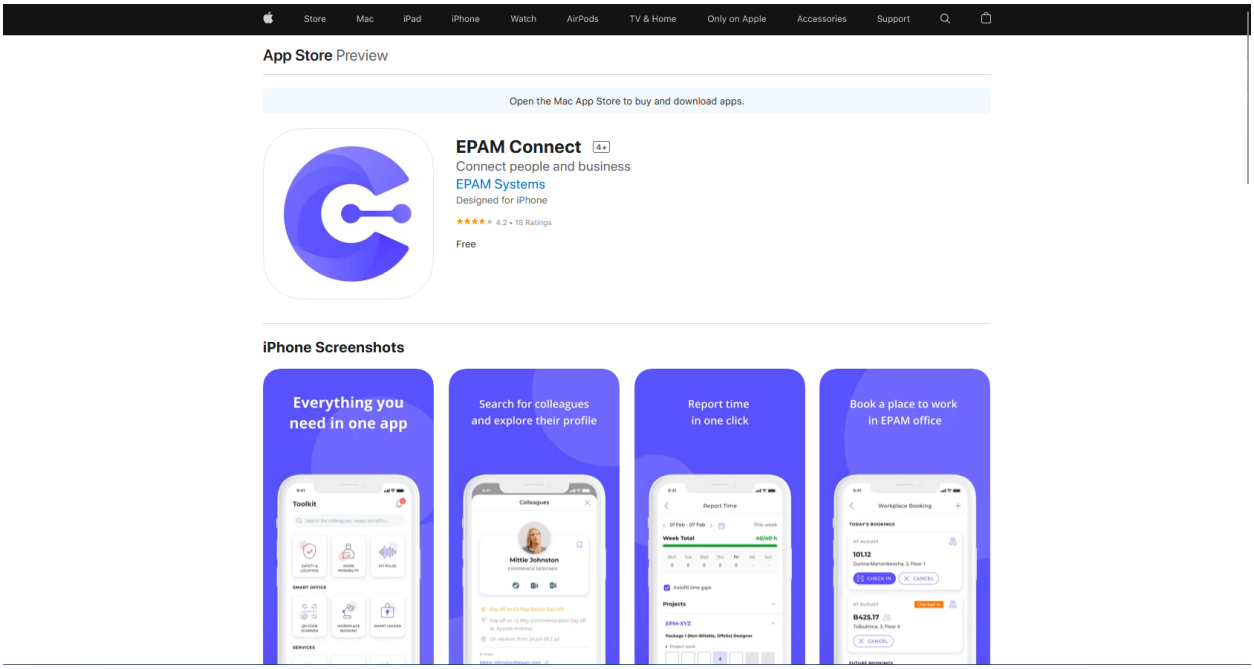


5. com.epam.connect.android



This is the android app of the relevant web service.

6. 1135407607



This is the IOS app for the relevant web service.

Assessing Subdomains

1. Subfinder

Subfinder is a subdomain research tool that gathers valid subdomains for websites using passive online data. It has a speed-optimized modular architecture and a simple modular architecture. Subfinder is a passive subdomain enumeration tool that complies with all passive source licenses and usage restrictions while keeping a consistent passive paradigm useful to both penetration testers and bug bounty hunters.

The primary features of the Subfinder tool are as follows:

- A powerful and quick resolution module, as well as a wildcard elimination module.
- Optimized for speed, it's lightning fast and uses extremely few resources.
- To get the best results, uses passive sources that have been carefully selected.
- Various output formats are supported (Json, File, Stdout).

Installation

Subfinder can be install to Linux with following command

- ***go install -v github.com/projectdiscovery/subfinder/v2/cmd/subfinder@latest***

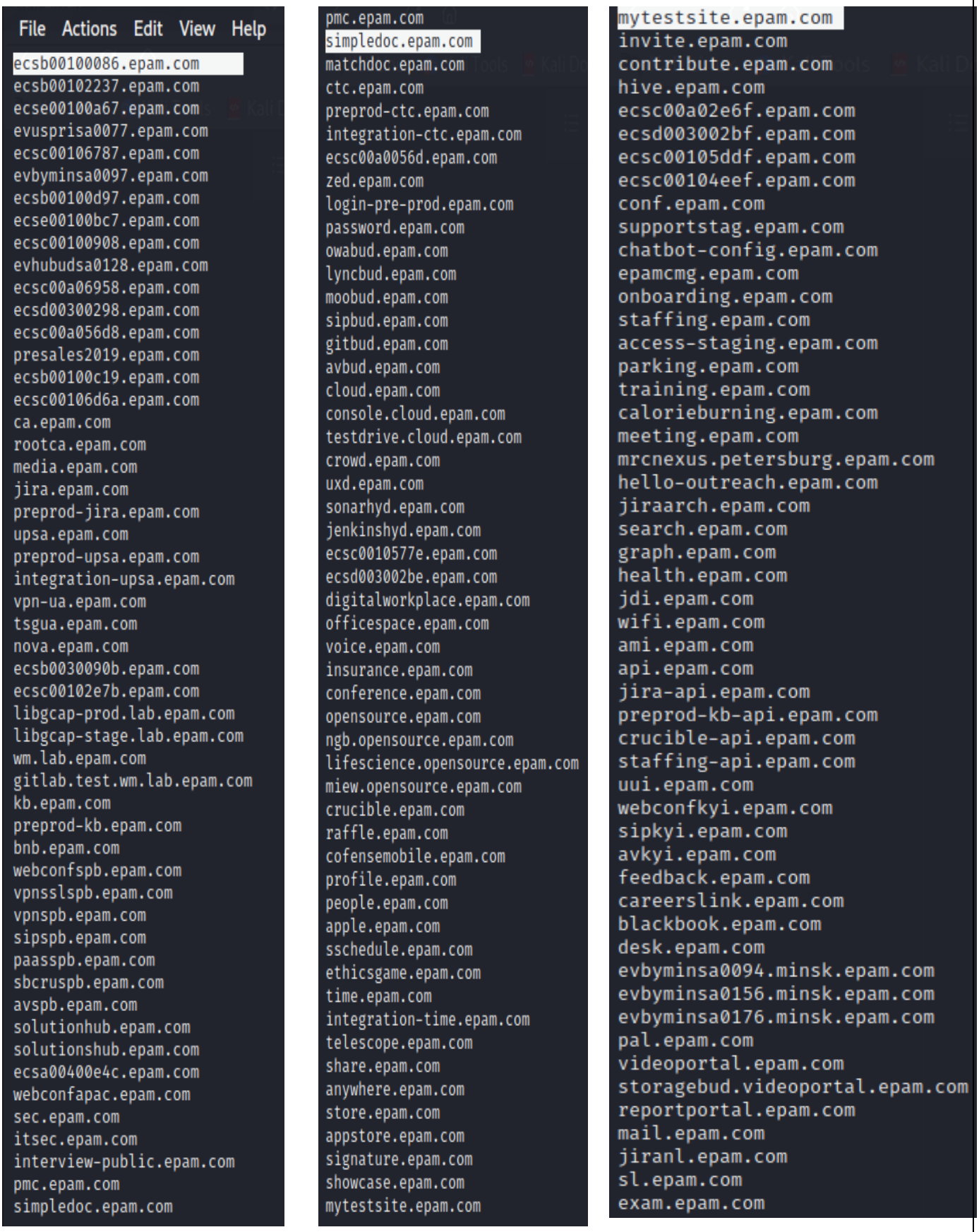
If your system failed to install subfinder as go is not installed, then install go with following command.

- **sudo apt install golang -y**

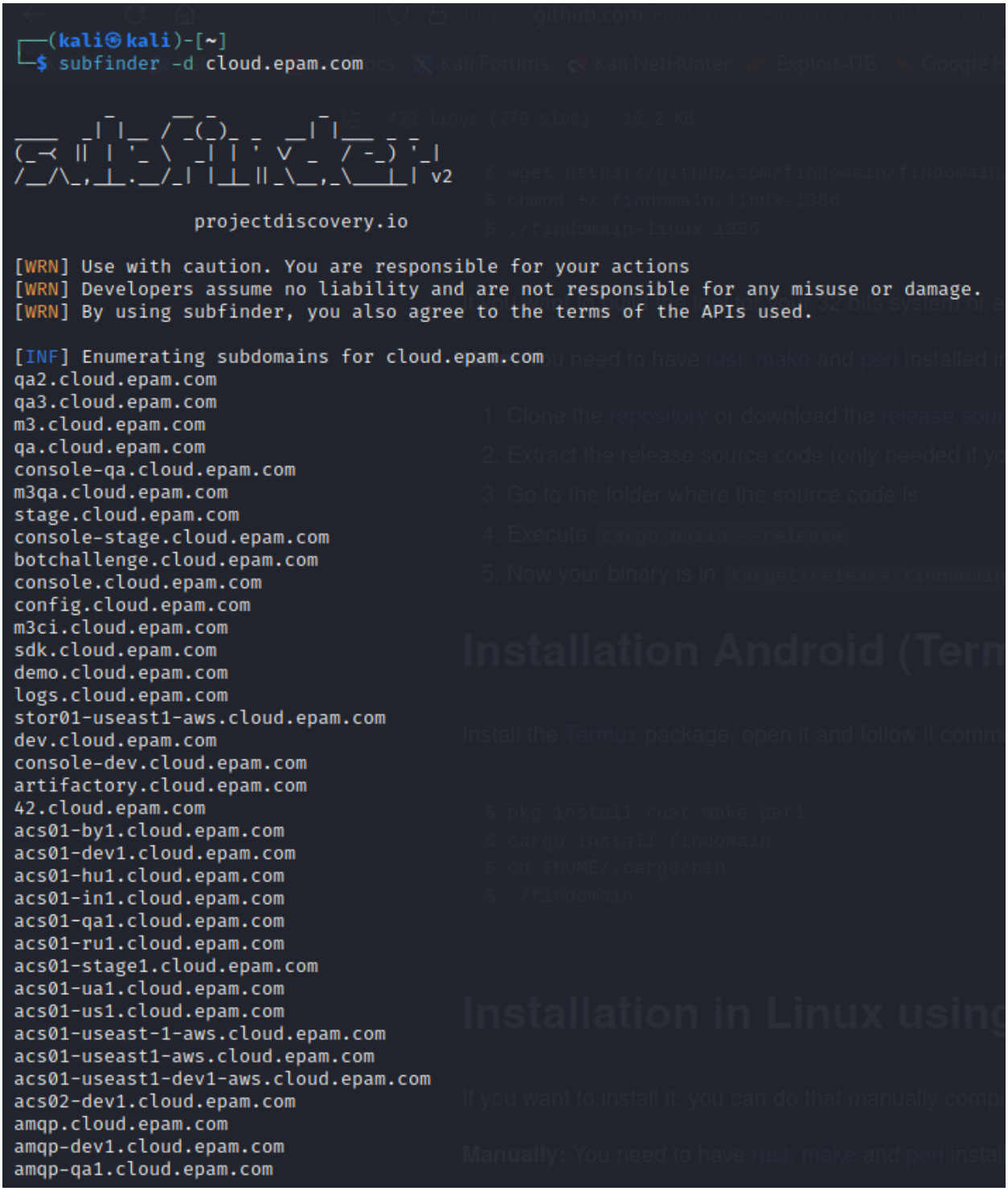

┌──(kali㉿kali)-[~]
└─$ sudo apt install subfinder
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
subfinder is already the newest version (2.3.8-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 363 not upgraded.
┌──(kali㉿kali)-[~]
└─$ subfinder
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.

Following that, I used the subfinder tool to enumerate the subdomains as follows.

1.epam.com


File Actions Edit View Help
ecsb00100086.epam.com
ecsb00102237.epam.com
ecse00100a67.epam.com
evusprisa0077.epam.com
ecsc00106787.epam.com
evbyminsa0097.epam.com
ecsb00100d97.epam.com
ecse00100bc7.epam.com
ecsc00100908.epam.com
evhubudsa0128.epam.com
ecsc00a06958.epam.com
ecsd00300298.epam.com
ecsc00a056d8.epam.com
presales2019.epam.com
ecsb00100c19.epam.com
ecsc00106d6a.epam.com
ca.epam.com
rootca.epam.com
media.epam.com
jira.epam.com
preprod-jira.epam.com
upsa.epam.com
preprod-upsa.epam.com
integration-upsa.epam.com
vpn-ua.epam.com
tsgua.epam.com
nova.epam.com
ecsb0030090b.epam.com
ecsc00102e7b.epam.com
libgcap-prod.lab.epam.com
libgcap-stage.lab.epam.com
wm.lab.epam.com
gitlab.test.wm.lab.epam.com
kb.epam.com
preprod-kb.epam.com
bnb.epam.com
webconfspb.epam.com
vpnsslspb.epam.com
vpnspb.epam.com
sipspb.epam.com
paasspb.epam.com
sbcruspb.epam.com
avspb.epam.com
solutionhub.epam.com
solutionshub.epam.com
ecsa00400e4c.epam.com
webconfapac.epam.com
sec.epam.com
itsec.epam.com
interview-public.epam.com
pmc.epam.com
simpledoc.epam.com
pmc.epam.com
simpledoc.epam.com
matchdoc.epam.com
ctc.epam.com
preprod-ctc.epam.com
integration-ctc.epam.com
ecsc00a0056d.epam.com
zed.epam.com
login-pre-prod.epam.com
password.epam.com
owabud.epam.com
lyncbud.epam.com
moobud.epam.com
sipbud.epam.com
gitbud.epam.com
avbud.epam.com
cloud.epam.com
console.cloud.epam.com
testdrive.cloud.epam.com
crowd.epam.com
uxd.epam.com
sonarhyd.epam.com
jenkinshyd.epam.com
ecsc0010577e.epam.com
ecsd003002be.epam.com
digitalworkplace.epam.com
officespace.epam.com
voice.epam.com
insurance.epam.com
conference.epam.com
opensource.epam.com
ngb.opensource.epam.com
lifescience.opensource.epam.com
miew.opensource.epam.com
crucible.epam.com
raffle.epam.com
cofensemobile.epam.com
profile.epam.com
people.epam.com
apple.epam.com
sschedule.epam.com
ethicsgame.epam.com
time.epam.com
integration-time.epam.com
telescope.epam.com
share.epam.com
anywhere.epam.com
store.epam.com
appstore.epam.com
signature.epam.com
showcase.epam.com
mytestsite.epam.com
mytestsite.epam.com
invite.epam.com
contribute.epam.com
hive.epam.com
ecsc00a02e6f.epam.com
ecsd003002bf.epam.com
ecsc00105ddf.epam.com
ecsc00104eef.epam.com
conf.epam.com
supportstag.epam.com
chatbot-config.epam.com
epamcmg.epam.com
onboarding.epam.com
staffing.epam.com
access-staging.epam.com
parking.epam.com
training.epam.com
calorieburning.epam.com
meeting.epam.com
mrcnexus.petersburg.epam.com
hello-outreach.epam.com
jiraarch.epam.com
search.epam.com
graph.epam.com
health.epam.com
jdi.epam.com
wifi.epam.com
ami.epam.com
api.epam.com
jira-api.epam.com
preprod-kb-api.epam.com
crucible-api.epam.com
staffing-api.epam.com
uui.epam.com
webconfkyi.epam.com
sipkyi.epam.com
avkyi.epam.com
feedback.epam.com
careerslink.epam.com
blackbook.epam.com
desk.epam.com
evbyminsa0094.minsk.epam.com
evbyminsa0156.minsk.epam.com
evbyminsa0176.minsk.epam.com
pal.epam.com
videoportal.epam.com
storagebud.videoportal.epam.com
reportportal.epam.com
mail.epam.com
jiranl.epam.com
sl.epam.com
exam.epam.com

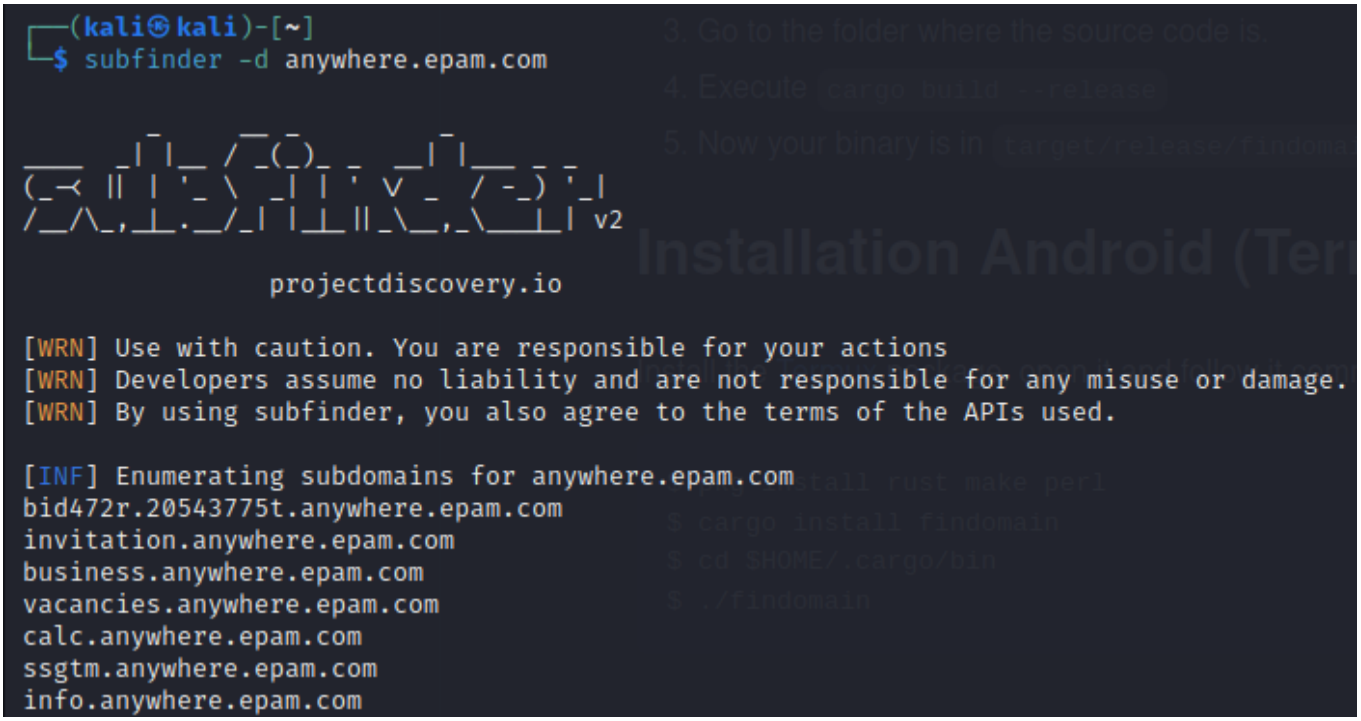
2. cloud.epam.com



There's a much longer list of subdomains here and I have saved them in a text fille called "<domain>'subs.txt".

3. access.epam.com

4. anywhere.epam.com



2. **Assetfinder**

Assertfinder is an enumeration tool for subdomains created in the Go computer language. This program basically looks for domains and subdomains that might be related to a specified domain. The Assertfinder tool now includes the following default sources.

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

Installation

Tool can be installed using following command as follows,

"sudo apt install assetfinder"

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt install assetfinder
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  assetfinder
0 upgraded, 1 newly installed, 0 to remove and 364 not upgraded.
Need to get 1,571 kB of archives.
After this operation, 4,976 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 assetfinder amd64 0.1.0+git20200415-0kali1 [1,571 kB]
Fetched 1,571 kB in 6s (268 kB/s)
Selecting previously unselected package assetfinder.
(Reading database ... 299900 files and directories currently installed.)
Preparing to unpack .../assetfinder_0.1.0+git20200415-0kali1_amd64.deb ...
Unpacking assetfinder (0.1.0+git20200415-0kali1) ...
Setting up assetfinder (0.1.0+git20200415-0kali1) ...
Processing triggers for kali-menu (2022.2.0) ...
```

Then I have used,

"assetfinder -subs-only <domain>" command to enumerate subdomains of all above four main domains and saved them on the "<domain>subs2.txt" file, some instances of using this tool to enumerate sub domains are as follows.

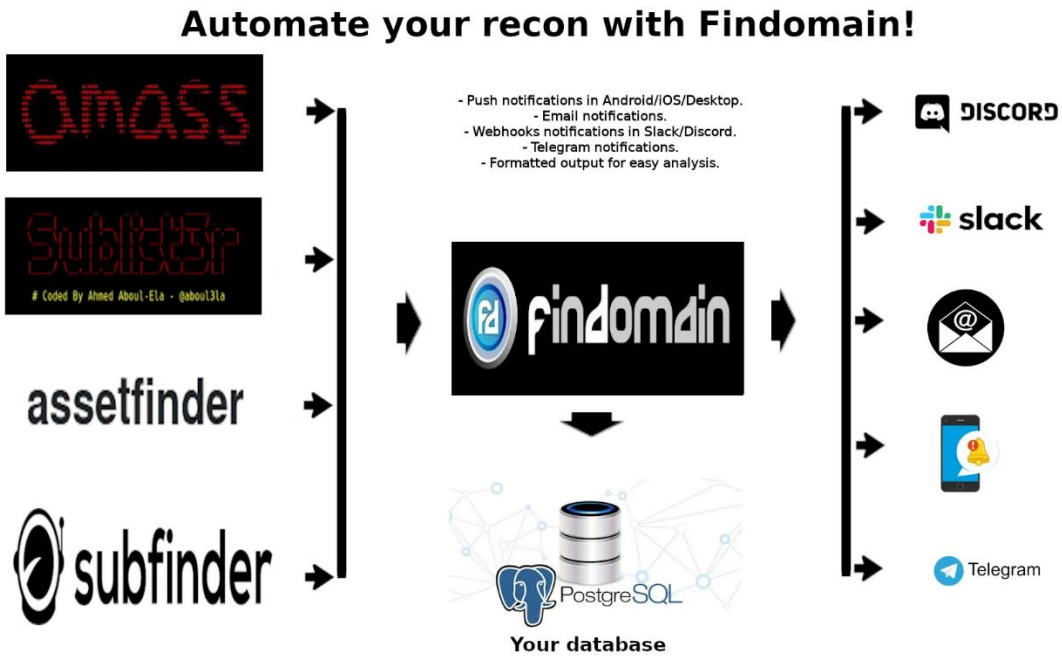
```
┌──(kali㉿kali)-[~/Desktop/assetfinder]
└─$ assetfinder --subs-only epam.com
eprumosvsa0000.epam.com
ecsb00100200.epam.com
ecsb00300210.epam.com
ecsc00a01310.epam.com
evbyminsa0220.epam.com
ecsa00401230.epam.com
ecsc00a01230.epam.com
ecsd00100430.epam.com
evbyminsd1730.epam.com
evhubudsa0140.epam.com
evusprisa0060.epam.com
evusprisa0160.epam.com
evhubudsa0470.epam.com
ecsc00a00870.epam.com
evhubudsa0080.epam.com
evhubudsa0180.epam.com
ecsa00400380.epam.com
ecsc00103f90.epam.com
ecsc001053a0.epam.com
ecse001010c0.epam.com
evhubudsa0213t0.epam.com
evhubudsa0214t0.epam.com
evusprisa0028t0.epam.com
evusprisa0111.epam.com
ecsb00100021.epam.com
ecsb00100d21.epam.com
ecsc00a05f31.epam.com
ecsb00100141.epam.com
ecsb00101051.epam.com
ecsc00a06651.epam.com
evhubudsa0261.epam.com
ecsa00400a61.epam.com
ecsb00100d61.epam.com
ecsc00103c71.epam.com
evbyminsd2091.epam.com
ecsc00a02b91.epam.com
ecsc00a03ba1.epam.com
ecsb003000b1.epam.com
ecsb00100bb1.epam.com
ecsd003002c1.epam.com
ecsc00a008d1.epam.com
ecsc00a002e1.epam.com
ecsc00105ef1.epam.com
ns1.epam.com
epbyminsd002.epam.com
ecsa00100502.epam.com
ecsd00300e02.epam.com
ecsa00100012.epam.com
ecsb00100c12.epam.com
ecsc00104722.epam.com
```

```
┌──(kali㉿kali)-[~/Desktop/assetfinder]
└─$ assetfinder --subs-only access.epam.com
access.epam.com
access.epam.com
www.access.epam.com

┌──(kali㉿kali)-[~/Desktop/assetfinder]
└─$ assetfinder --subs-only anywhere.epam.com
bid472r.20543775t.anywhere.epam.com
anywhere.epam.com
ssgtm.anywhere.epam.com
vacancies.anywhere.epam.com
business.anywhere.epam.com
calc.anywhere.epam.com
info.anywhere.epam.com
internal.anywhere.epam.com
invitation.anywhere.epam.com

┌──(kali㉿kali)-[~/Desktop/assetfinder]
└─$ assetfinder --subs-only cloud.epam.com
qa2.cloud.epam.com
qa3.cloud.epam.com
m3.cloud.epam.com
qa.cloud.epam.com
console-qa.cloud.epam.com
m3qa.cloud.epam.com
stage.cloud.epam.com
console-stage.cloud.epam.com
botchallenge.cloud.epam.com
console.cloud.epam.com
config.cloud.epam.com
m3ci.cloud.epam.com
sdk.cloud.epam.com
demo.cloud.epam.com
logs.cloud.epam.com
stor01-useast1-aws.cloud.epam.com
dev.cloud.epam.com
console-dev.cloud.epam.com
artifactory.cloud.epam.com
cloud.epam.com
cloud.epam.com
cloud.epam.com
m3native.cloud.epam.com
public-stage.cloud.epam.com
chef.rd.cloud.epam.com
graylog.rd.cloud.epam.com
jenkins.rd.cloud.epam.com
rabbitmq.rd.cloud.epam.com
test.rd.cloud.epam.com
gerrit-testportal-edp-cicd.openshift.rd.epmd-edp.cloud.epam.com
ilb-edp.cloud.epam.com
```

3. **Findomain**

Findomain is a well-known subdomain enumeration tool used by bug bounty hunters and cybersecurity experts around the world. Findomain is a comprehensive recon framework that employs cutting-edge technologies to provide warnings to webhooks, emails, Telegram chats, and push notifications to Android, iOS, Desktop, and Smart Watches via Pushover about new subdomains, their HTTP status, open ports, IP addresses, and more. For huge workloads, the tool is written in Rust and provides high performance, security, and dependability.

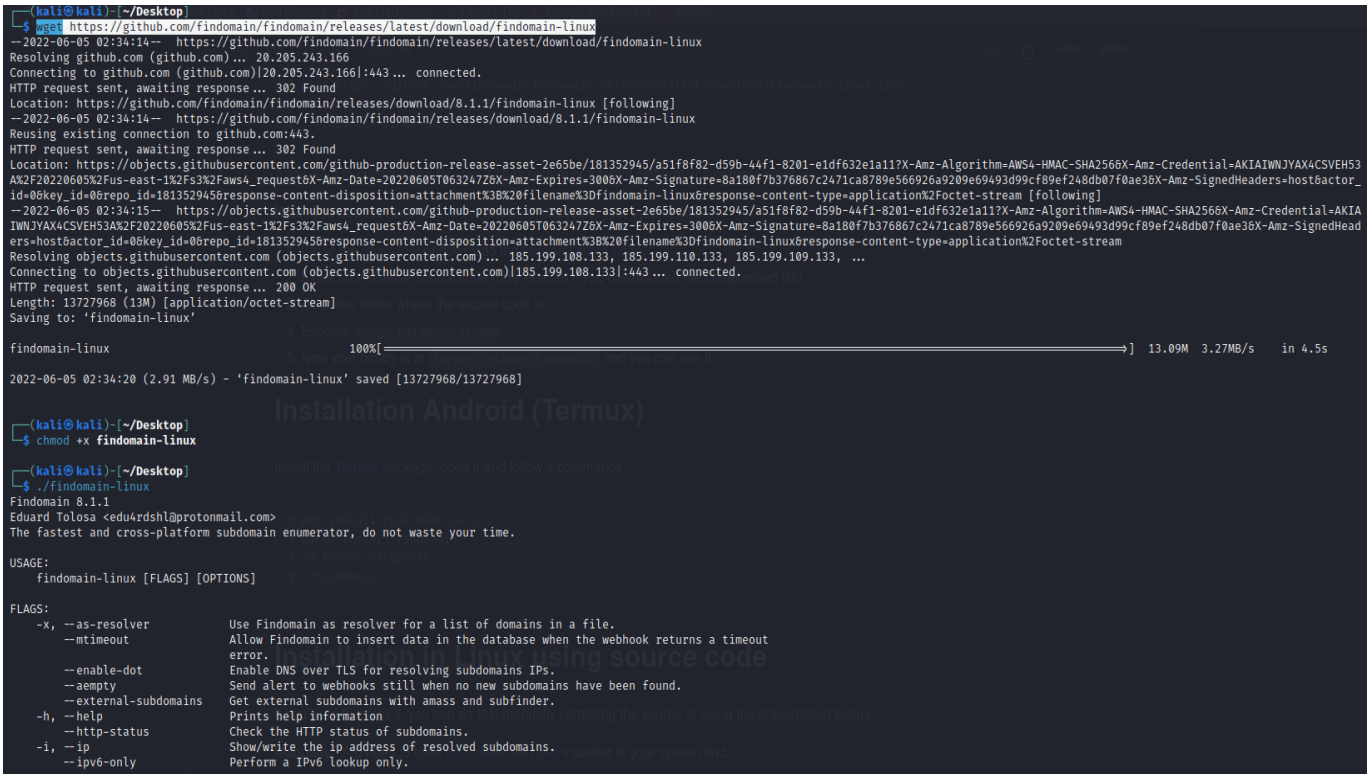
In order to provide efficient subdomain enumeration, the Finddomain tool merged the passive results of the top four tools, such as OWASP Amass, Sublist3r, Assetfinder, and Subfinder, into our method.



Installation

This tool can be installed in Kali Linux with following command,

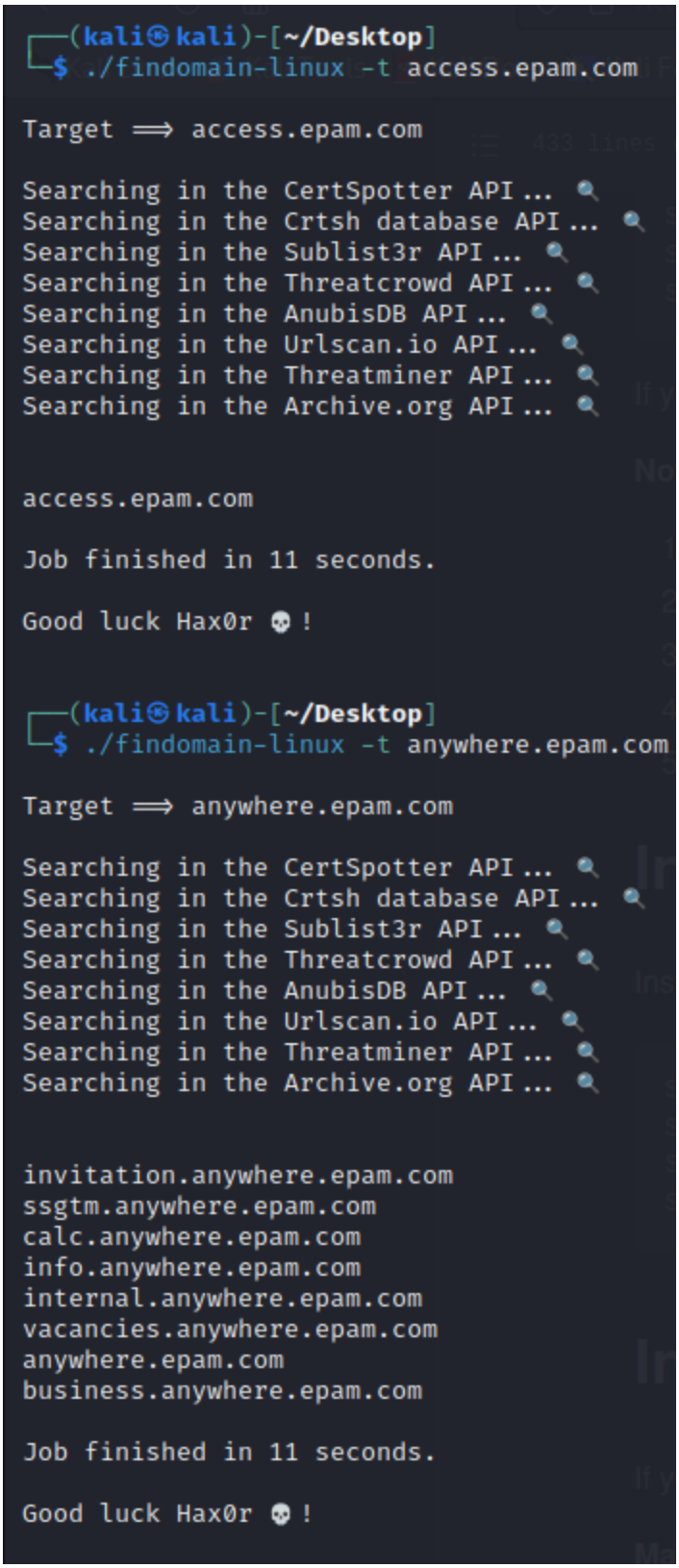
- **“wget https://github.com/findomain/findomain/releases/latest/download/findomain-linux”**
- **“chmod +x findomain-linux”**



Then ran it with “ **./findomain-linux -t <domain>** “ command to enumerate the subdomains as follows and save all of them separately on “<domain>subs3.txt”.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./findomain-linux -t epam.com

Target ⟹ epam.com

Searching in the CertSpotter API … 🔍
Searching in the Crtsh database API … 🔍
Searching in the Sublist3r API … 🔍
Searching in the Threatcrowd API … 🔍
Searching in the AnubisDB API … 🔍
Searching in the Urlscan.io API … 🔍
Searching in the Archive.org API … 🔍
Searching in the Threatminer API … 🔍


webservice.main.sergiy2.maf.wstc-wcst.projects.epam.com
maf-orest1-assets.services.wstc-wcst.projects.epam.com
api.mqa2.maf.services.wstc-wcst.projects.epam.com
dboper.cloud.epam.com
kb.opensource.epam.com
maestro01-ru1.cloud.epam.com
ecsd003002c1.epam.com
jiraeu.epam.com
www.mfa-cache.epam.com
www.media.info.epam.com
desktop.connect.epam.com
evhubudsa0074.budapest.epam.com
login.epam.com
maf-bohdan1-api.services.wstc-wcst.projects.epam.com
demo-bizfx.hca.azure.epmc-stc.projects.epam.com
npfrgs-stg.epam.com.epam.com
dev.cloud.epam.com
epbyminsd002.epam.com
preview.bondar2.maf.services.wstc-wcst.projects.epam.com
connect.epam.com
ecsb00100141.epam.com
api.main.novachok2.mas.wstc-wcst.projects.epam.com
clmstest.epam.com
sonar-testportal-edp-cicd.openshift.rd.epmd-edp.cloud.epam.com
kb-api.epam.com
api-dev.aws.rcom-bflw.projects.epam.com
webconfbud.epam.com
dev-nbty-frontend.epm-ddl.projects.epam.com
global.infra1.sche-digi.projects.epam.com
ci.wkh-lrp.projects.epam.com
prototype.amw-srd.projects.epam.com
prism.delivery.epam.com
media.sergiy2.mas.wstc-wcst.projects.epam.com
evbyminsd1989.minsk.epam.com
assets.novachok2.maf.services.wstc-wcst.projects.epam.com
preview.main.novachok2.mas.wstc-wcst.projects.epam.com
demo.staffing.epam.com
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./findomain-linux -t cloud.epam.com

Target ⟹ cloud.epam.com

Searching in the CertSpotter API … 🔍
Searching in the Sublist3r API … 🔍
Searching in the Crtsh database API … 🔍
Searching in the Threatcrowd API … 🔍
Searching in the AnubisDB API … 🔍
Searching in the Urlscan.io API … 🔍
Searching in the Threatminer API … 🔍
Searching in the Archive.org API … 🔍


stor01-in1.cloud.epam.com
stage.cloud.epam.com
keycloak-security.openshift.rd.epmd-edp.cloud.epam.com
dev.cloud.epam.com
acs01-stage1.cloud.epam.com
stor01-ua1.cloud.epam.com
acs01-by1.cloud.epam.com
dboper-stage1.cloud.epam.com
maestro02-hu1.cloud.epam.com
sonar-testportal-edp-cicd.openshift.rd.epmd-edp.cloud.epam.com
chefserver-useast1.amazon.cloud.epam.com
qa2.cloud.epam.com
console-qa.cloud.epam.com
dboper-qa1.cloud.epam.com
42.cloud.epam.com
gerrit-testportal-edp-cicd.ilb-edp.cloud.epam.com
m3dbqa.cloud.epam.com
dbbill.cloud.epam.com
maestro02-ua1.cloud.epam.com
dbbill-stage1.cloud.epam.com
amqp-stage1.cloud.epam.com
artifactory.cloud.epam.com
dboper-dev1.cloud.epam.com
maestro01-in1.cloud.epam.com
maestro3.cloud.epam.com
acs01-hu1.cloud.epam.com
dbbill-qa1.cloud.epam.com
acs01-useast1-dev1-aws.cloud.epam.com
dboper.cloud.epam.com
nexus-testportal-edp-cicd.openshift.rd.epmd-edp.cloud.epam.com
m3qa.cloud.epam.com
stor01-hu1.cloud.epam.com
elsevier.cloud.epam.com
maestro02-in1.cloud.epam.com
skyper.cloud.epam.com
```


┌──(kali㉿kali)-[~/Desktop]
└─$ ./findomain-linux -t access.epam.com
Target ⟹ access.epam.com
Searching in the CertSpotter API ... 🔍
Searching in the Crtsh database API ... 🔍
Searching in the Sublist3r API ... 🔍
Searching in the Threatcrowd API ... 🔍
Searching in the AnubisDB API ... 🔍
Searching in the Urlscan.io API ... 🔍
Searching in the Threatminer API ... 🔍
Searching in the Archive.org API ... 🔍
access.epam.com
Job finished in 11 seconds.
Good luck Hax0r 💀 !
┌──(kali㉿kali)-[~/Desktop]
└─$ ./findomain-linux -t anywhere.epam.com
Target ⟹ anywhere.epam.com
Searching in the CertSpotter API ... 🔍
Searching in the Crtsh database API ... 🔍
Searching in the Sublist3r API ... 🔍
Searching in the Threatcrowd API ... 🔍
Searching in the AnubisDB API ... 🔍
Searching in the Urlscan.io API ... 🔍
Searching in the Threatminer API ... 🔍
Searching in the Archive.org API ... 🔍
invitation.anywhere.epam.com
ssgtm.anywhere.epam.com
calc.anywhere.epam.com
info.anywhere.epam.com
internal.anywhere.epam.com
vacancies.anywhere.epam.com
anywhere.epam.com
business.anywhere.epam.com
Job finished in 11 seconds.
Good luck Hax0r 💀 !

5. Sublist3r

Sublist3r is a Python-based utility for enumerating a website's subdomains. The Open-Source Intelligence [OSINT] idea underpins this technology. This means that pen testers can use this technology to gather information, analyze it, and make conclusions based on readily available information. To enumerate subdomains, Sublist3r predominantly employs Google, Yahoo, Baidu, Bing, and Ask, with Netcraft, Virustotal, ThreatCrowd, ReverseDNS, and DNSdumpster being utilized in exceptional circumstances.

The "subbrute" utility has been combined with Sublist3r in recent upgrades to expand the ability of identifying additional subdomains using brute-force with an upgraded wordlist and compatibility increased to Python 3.

Installation

I have cloned the tool from git hub with the command

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

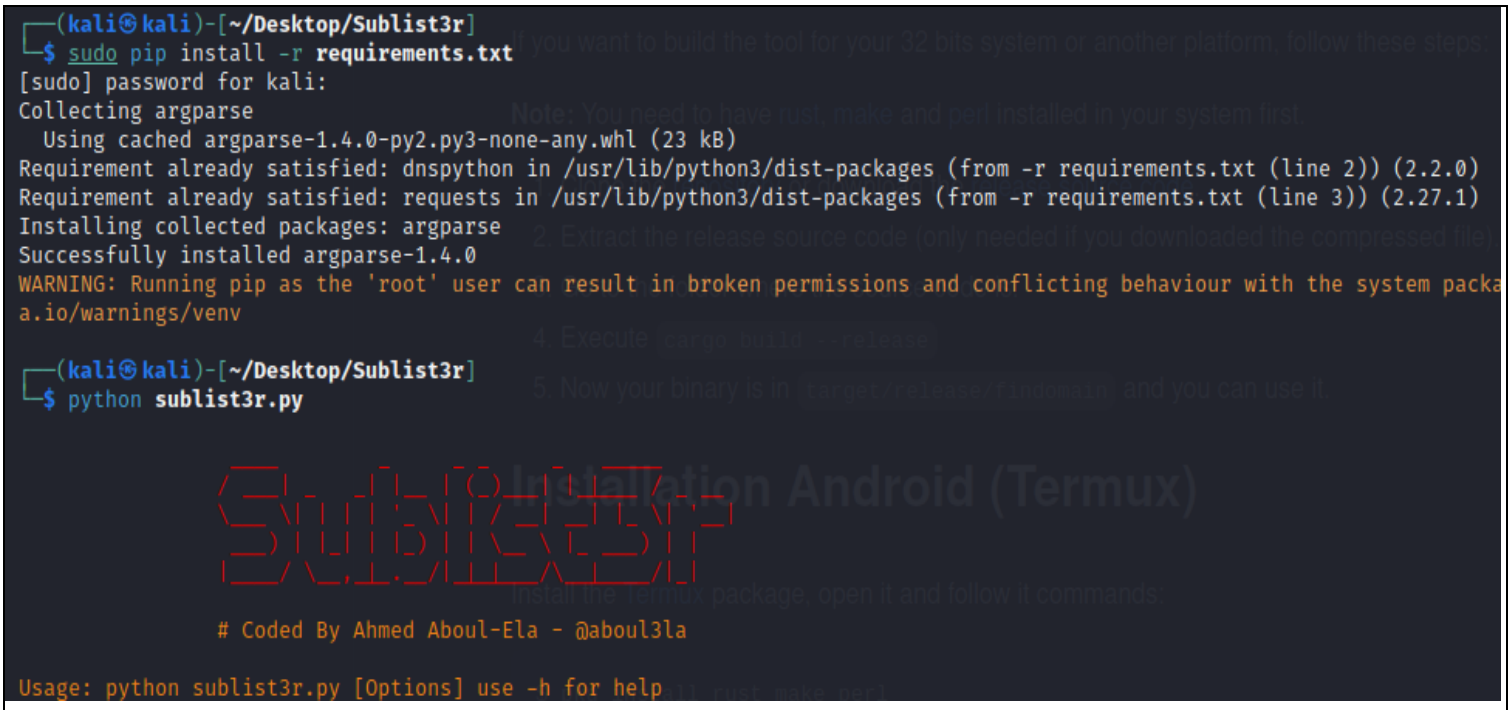
in my desktop.

As this tool needs some additional dependencies like dnspython, argparse and requests python modules, I had to install them using the requirements document in cloned folder with following command.

" sudo pip install -r requirements.txt"

Installation with a tool interface is shown below.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ git clone https://github.com/aboul3la/Sublist3r.git
Cloning into 'Sublist3r' ...
remote: Enumerating objects: 383, done.
remote: Total 383 (delta 0), reused 0 (delta 0), pack-reused 383
Receiving objects: 100% (383/383), 1.12 MiB | 947.00 KiB/s, done.
Resolving deltas: 100% (212/212), done.
```



To run the tool, we need to navigate into Sublist3r directory and use command “python sublist3r.py -d <domain>” to search for subdomains whereas “-d” flag stand for domain.

You can see the enumeration of subdomains of above four domains here. But it showed an error from virustotal and did not return any results for three of the above domains.

```
┌──(kali㉿kali)-[~/Desktop/Sublist3r]
└─$ python sublist3r.py -d epam.com

                 ____        _ _     _   _____
                / ___| _   _| | |__ | (_)___ / _ __
                \___ \| | | | | '_ \| | | |_ \| '__|
                 ___) | |_| | | |_) | | |___) | |
                |____/ \__,_|_|_.__/|_|_|____/|_|

                # Coded By Ahmed Aboul-El

[-] Enumerating subdomains now for epam.c
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blc
[-] Total Unique Subdomains Found: 365
www.epam.com
access.epam.com
access-staging.epam.com
adaptation.epam.com
adss.epam.com
ami.epam.com
anywhere.epam.com
api.epam.com
apple.epam.com
appstore.epam.com
asmt.epam.com
assist.epam.com
autodiscover.epam.com
auxlogin.epam.com
avbud.epam.com
avkyi.epam.com
avmsq.epam.com
avpct.epam.com
avspb.epam.com
benefits.epam.com
blackbook.epam.com
bnb.epam.com
evhubudsa0134.budapest.epam.com
evhubudsa0134_ip2.budapest.epam.com
evhubudsd25fb.budapest.epam.com
```

```
┌──(kali㉿kali)-[~/Desktop/Sublist3r]
└─$ python sublist3r.py -d anywhere.epam.com

                 ____        _ _     _   _____
                / ___| _   _| | |__ | (_)___ / _ __
                \___ \| | | | | '_ \| | | |_ \| '__|
                 ___) | |_| | | |_) | | |___) | |
                |____/ \__,_|_|_.__/|_|_|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for anywhere.epam.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
```

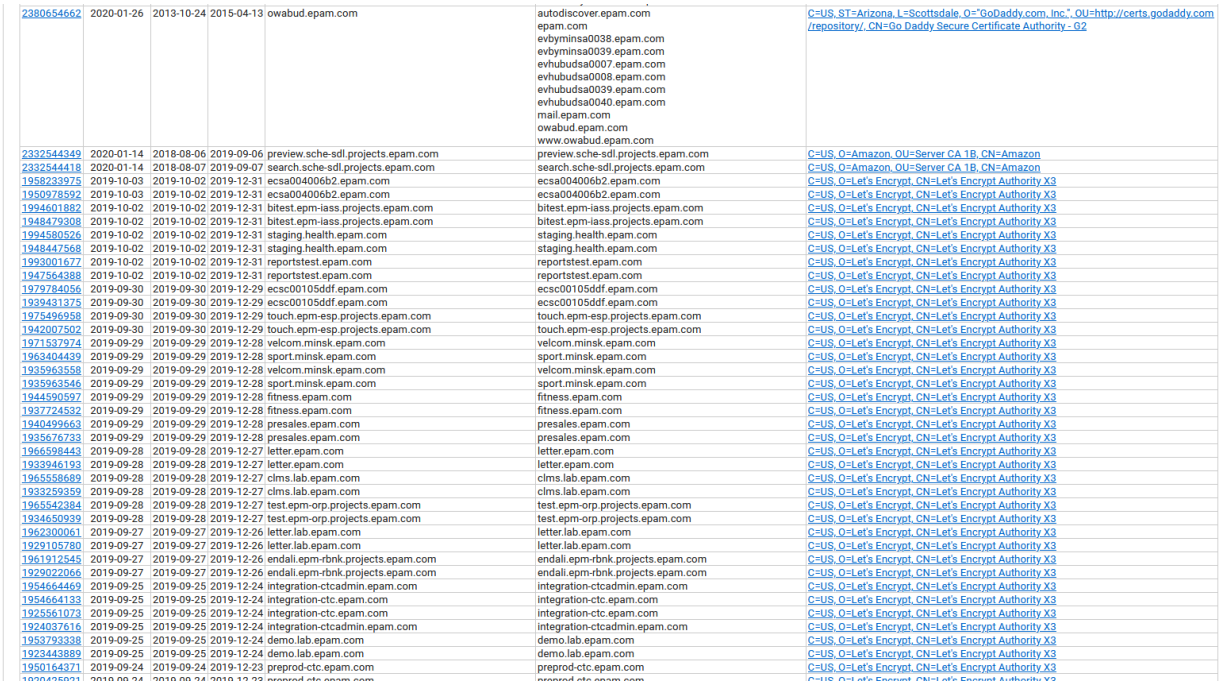
```
sl.epam.com
solutionhub.epam.com
solutionhubs.epam.com
solutionshub.epam.com
sonarhyd.epam.com
spowamsq.epam.com
sschedule.epam.com
staffing.epam.com
staffing-api.epam.com
startup.epam.com
status.epam.com
store.epam.com
support.epam.com
supportstag.epam.com
survey.epam.com
surveys.epam.com
svnmsq.epam.com
technology.epam.com
telescope.epam.com
time.epam.com
training.epam.com
tsgeu.epam.com
tsgin.epam.com
tsgmsq.epam.com
tsgru.epam.com
tsgua.epam.com
tsgus.epam.com
university.epam.com
upsa.epam.com
upsa-ru.epam.com
uui.epam.com
uxd.epam.com
vacation.epam.com
videoportal.epam.com
storagebud.videoportal.epam.com
voice.epam.com
volunteers.epam.com
vpn.epam.com
vpn-cn.epam.com
vpn-ru.epam.com
vpn-ua.epam.com
vpnspb.epam.com
vpnsslspb.epam.com
vpnsslszx.epam.com
vts.epam.com
webconfapac.epam.com
webconfkyi.epam.com
webconfmsq2.epam.com
webconfspb.epam.com
webstats.epam.com
wifi.epam.com
zed.epam.com
```

```
└─$ python sublist3r.py -d cloud.epam.com

                 # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for cloud.epam.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests

┌──(kali㉿kali)-[~/Desktop/Sublist3r]
└─$ python sublist3r.py -d access.epam.com

                 # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for access.epam.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
```

5. Crt.sh

Crt.sh stands for "certificates.Saint Helena," and it's a website where visitors can look for all of the SSL or TLS certificates for a certain domain. The site is free source and used to keep track of the certifications. The site features a graphical user interface that makes gathering information a breeze. The purpose of the site is to make the certificate records as open as feasible. The certificate algorithms are also available in ciphertext format for users.

I used this platform to gather information about the subdomains as well as their SSL/TLS certificate issuers and saved them in a separate file. Screenshots from the crt.sh are as follows.



2380654662	2020-01-26	2013-10-24	2015-04-13	owabud.epam.com	autodiscover.epam.com epam.com evbyminsa0038.epam.com evbyminsa0039.epam.com evhubudsa0007.epam.com evhubudsa0008.epam.com evhubudsa0039.epam.com evhubudsa0040.epam.com mail.epam.com owabud.epam.com www.owabud.epam.com	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com /repository/, CN=Go Daddy Secure Certificate Authority - G2
2332544349	2020-01-14	2018-08-06	2019-09-06	preview.sche-sdl.projects.epam.com	preview.sche-sdl.projects.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
2332544418	2020-01-14	2018-08-07	2019-09-07	search.sche-sdl.projects.epam.com	search.sche-sdl.projects.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
1958233975	2019-10-03	2019-10-02	2019-12-31	ecsa004006b2.epam.com	ecsa004006b2.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1950978592	2019-10-03	2019-10-02	2019-12-31	ecsa004006b2.epam.com	ecsa004006b2.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1994601882	2019-10-02	2019-10-02	2019-12-31	bitest.epm-iass.projects.epam.com	bitest.epm-iass.projects.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1948479308	2019-10-02	2019-10-02	2019-12-31	bitest.epm-iass.projects.epam.com	bitest.epm-iass.projects.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1994580526	2019-10-02	2019-10-02	2019-12-31	staging.health.epam.com	staging.health.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1948447568	2019-10-02	2019-10-02	2019-12-31	staging.health.epam.com	staging.health.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1993001677	2019-10-02	2019-10-02	2019-12-31	reportstest.epam.com	reportstest.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1947564388	2019-10-02	2019-10-02	2019-12-31	reportstest.epam.com	reportstest.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1979784056	2019-09-30	2019-09-30	2019-12-29	ecsc00105ddf.epam.com	ecsc00105ddf.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1939431375	2019-09-30	2019-09-30	2019-12-29	ecsc00105ddf.epam.com	ecsc00105ddf.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1975496958	2019-09-30	2019-09-30	2019-12-29	touch.epm-esp.projects.epam.com	touch.epm-esp.projects.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1942007502	2019-09-30	2019-09-30	2019-12-29	touch.epm-esp.projects.epam.com	touch.epm-esp.projects.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1971537974	2019-09-29	2019-09-29	2019-12-28	velcom.minsk.epam.com	velcom.minsk.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1963404439	2019-09-29	2019-09-29	2019-12-28	sport.minsk.epam.com	sport.minsk.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1935963558	2019-09-29	2019-09-29	2019-12-28	velcom.minsk.epam.com	velcom.minsk.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1935963546	2019-09-29	2019-09-29	2019-12-28	sport.minsk.epam.com	sport.minsk.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1944590597	2019-09-29	2019-09-29	2019-12-28	fitness.epam.com	fitness.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1937724532	2019-09-29	2019-09-29	2019-12-28	fitness.epam.com	fitness.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1940499663	2019-09-29	2019-09-29	2019-12-28	presales.epam.com	presales.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1935676733	2019-09-29	2019-09-29	2019-12-28	presales.epam.com	presales.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1966598443	2019-09-28	2019-09-28	2019-12-27	letter.epam.com	letter.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1933946193	2019-09-28	2019-09-28	2019-12-27	letter.epam.com	letter.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1965558689	2019-09-28	2019-09-28	2019-12-27	clms.lab.epam.com	clms.lab.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1933259359	2019-09-28	2019-09-28	2019-12-27	clms.lab.epam.com	clms.lab.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1965542384	2019-09-28	2019-09-28	2019-12-27	test.epm-orp.projects.epam.com	test.epm-orp.projects.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1934650939	2019-09-28	2019-09-28	2019-12-27	test.epm-orp.projects.epam.com	test.epm-orp.projects.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1962300061	2019-09-27	2019-09-27	2019-12-26	letter.lab.epam.com	letter.lab.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1929105780	2019-09-27	2019-09-27	2019-12-26	letter.lab.epam.com	letter.lab.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1961912545	2019-09-27	2019-09-27	2019-12-26	endali.epm-rbnk.projects.epam.com	endali.epm-rbnk.projects.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1929022066	2019-09-27	2019-09-27	2019-12-26	endali.epm-rbnk.projects.epam.com	endali.epm-rbnk.projects.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1954664469	2019-09-25	2019-09-25	2019-12-24	integration-ctcadmin.epam.com	integration-ctcadmin.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1954664133	2019-09-25	2019-09-25	2019-12-24	integration-ctc.epam.com	integration-ctc.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1925561073	2019-09-25	2019-09-25	2019-12-24	integration-ctc.epam.com	integration-ctc.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1924037616	2019-09-25	2019-09-25	2019-12-24	integration-ctcadmin.epam.com	integration-ctcadmin.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1953793338	2019-09-25	2019-09-25	2019-12-24	demo.lab.epam.com	demo.lab.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1923443889	2019-09-25	2019-09-25	2019-12-24	demo.lab.epam.com	demo.lab.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1950164371	2019-09-24	2019-09-24	2019-12-23	preprod-ctc.epam.com	preprod-ctc.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

crt.sh Identity Search Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'cloud.epam.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	
6865774745	2022-06-04	2022-06-04	2022-09-02	dev.cloud.epam.com	dev.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6865769611	2022-06-04	2022-06-04	2022-09-02	dev.cloud.epam.com	dev.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6825268913	2022-05-29	2022-05-29	2022-08-27	sdk.cloud.epam.com	sdk.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6825263030	2022-05-29	2022-05-29	2022-08-27	sdk.cloud.epam.com	sdk.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6825248360	2022-05-29	2022-05-29	2022-08-27	stage.cloud.epam.com	stage.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6825248846	2022-05-29	2022-05-29	2022-08-27	stage.cloud.epam.com	stage.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6648882770	2022-05-01	2022-05-01	2022-07-30	cloud.epam.com	cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6642580926	2022-05-01	2022-05-01	2022-07-30	cloud.epam.com	cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6481043124	2022-04-05	2022-04-05	2022-07-04	dev.cloud.epam.com	dev.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6481042822	2022-04-05	2022-04-05	2022-07-04	dev.cloud.epam.com	dev.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6441938074	2022-03-30	2022-03-30	2022-06-28	sdk.cloud.epam.com	sdk.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6441938584	2022-03-30	2022-03-30	2022-06-28	sdk.cloud.epam.com	sdk.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6441912530	2022-03-30	2022-03-30	2022-06-28	stage.cloud.epam.com	stage.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6441908478	2022-03-30	2022-03-30	2022-06-28	stage.cloud.epam.com	stage.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6269742991	2022-03-02	2022-03-02	2022-05-31	cloud.epam.com	cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6269737635	2022-03-02	2022-03-02	2022-05-31	cloud.epam.com	cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6120296983	2022-02-04	2022-02-04	2022-05-05	dev.cloud.epam.com	dev.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6105789106	2022-02-04	2022-02-04	2022-05-05	dev.cloud.epam.com	dev.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6083874067	2022-01-29	2022-01-29	2022-04-29	sdk.cloud.epam.com	sdk.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6068765001	2022-01-29	2022-01-29	2022-04-29	sdk.cloud.epam.com	sdk.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6083840454	2022-01-29	2022-01-29	2022-04-29	stage.cloud.epam.com	stage.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6068746896	2022-01-29	2022-01-29	2022-04-29	stage.cloud.epam.com	stage.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6083827728	2022-01-29	2022-01-29	2022-04-29	qa2.cloud.epam.com	qa2.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6068966777	2022-01-29	2022-01-29	2022-04-29	qa2.cloud.epam.com	qa2.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3
6083798551	2022-01-29	2022-01-29	2022-04-29	qa3.cloud.epam.com	qa3.cloud.epam.com	C=US, O=Let's Encrypt, CN=R3

crt.sh Identity Search Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'access.epam.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
6446172712	2022-03-31	2022-03-28	2023-04-26	access.epam.com	access.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
6426544423	2022-03-28	2022-03-28	2023-04-26	access.epam.com	access.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
6425322888	2022-03-28	2022-03-28	2023-04-26	access.epam.com	access.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
4535593275	2021-05-16	2021-04-27	2022-05-26	access.epam.com	access.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
4437136505	2021-04-27	2021-04-27	2022-05-26	access.epam.com	access.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
4437089762	2021-04-27	2021-04-27	2022-05-26	access.epam.com	access.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
4433649222	2021-04-26	2021-04-26	2022-05-25	access.epam.com	access.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
2523958918	2020-03-02	2020-02-05	2022-02-05	access.epam.com	access.epam.com www.access.epam.com	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
2419169617	2020-02-05	2020-02-05	2022-02-05	access.epam.com	access.epam.com www.access.epam.com	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2

crt.sh Identity Search Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'anywhere.epam.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
6700465555	2022-05-10	2022-05-10	2022-08-08	ssgtm.anywhere.epam.com	ssgtm.anywhere.epam.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
6700302686	2022-05-10	2022-05-10	2022-08-08	ssgtm.anywhere.epam.com	ssgtm.anywhere.epam.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
6628214397	2022-04-29	2022-04-29	2023-04-28	business.anywhere.epam.com	business.anywhere.epam.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
6628214290	2022-04-29	2022-04-29	2023-04-28	business.anywhere.epam.com	business.anywhere.epam.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2
6546498159	2022-04-15	2022-04-15	2023-05-14	vacancies.anywhere.epam.com	vacancies.anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
6501382295	2022-04-08	2022-04-08	2022-07-07	ssgtm.anywhere.epam.com	ssgtm.anywhere.epam.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
6275681116	2022-03-03	2022-03-03	2023-04-01	calc.anywhere.epam.com	calc.anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
6275642939	2022-03-03	2022-03-03	2023-04-01	calc.anywhere.epam.com	calc.anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
6134670219	2022-02-08	2022-02-08	2023-03-09	ssgtm.anywhere.epam.com	ssgtm.anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
6133504022	2022-02-08	2022-02-08	2022-05-09	ssgtm.anywhere.epam.com	ssgtm.anywhere.epam.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
6046323376	2022-01-25	2022-01-25	2022-04-25	ssgtm.anywhere.epam.com	ssgtm.anywhere.epam.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5997706704	2022-01-17	2022-01-17	2022-04-17	ssgtm.anywhere.epam.com	ssgtm.anywhere.epam.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5996370916	2022-01-17	2022-01-17	2022-04-17	ssgtm.anywhere.epam.com	ssgtm.anywhere.epam.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5956311302	2022-01-11	2022-01-11	2022-04-11	ssgtm.anywhere.epam.com	ssgtm.anywhere.epam.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5951700584	2022-01-10	2022-01-10	2022-04-10	ssgtm.anywhere.epam.com	ssgtm.anywhere.epam.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5813624253	2021-12-17	2021-12-17	2022-03-17	ssgtm.anywhere.epam.com	ssgtm.anywhere.epam.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5461322638	2021-10-22	2021-10-22	2022-10-21	info.anywhere.epam.com	info.anywhere.epam.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
5461322485	2021-10-22	2021-10-22	2022-10-21	info.anywhere.epam.com	info.anywhere.epam.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2
5442318362	2021-10-19	2021-10-19	2022-01-17	ssgtm.anywhere.epam.com	ssgtm.anywhere.epam.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5313654963	2021-09-30	2021-09-30	2022-10-29	internal.anywhere.epam.com	internal.anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5256768941	2021-09-20	2021-09-14	2022-10-12	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5237169944	2021-09-17	2021-09-14	2022-10-12	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5216417294	2021-09-14	2021-09-14	2022-10-12	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
5213640879	2021-09-14	2021-09-14	2022-10-12	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
4529584887	2021-05-15	2021-05-15	2022-06-13	vacancies.anywhere.epam.com	vacancies.anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
4528827712	2021-05-15	2021-05-15	2022-06-13	vacancies.anywhere.epam.com	vacancies.anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3946656272	2021-01-18	2021-01-18	2022-02-16	vacancies.anywhere.epam.com	vacancies.anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3521527062	2020-10-17	2020-10-14	2021-11-12	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3506945876	2020-10-14	2020-10-14	2021-11-12	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3506945203	2020-10-14	2020-10-14	2021-11-12	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3506941373	2020-10-14	2020-10-14	2021-11-12	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3506941409	2020-10-14	2020-10-14	2021-11-12	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3503065075	2020-10-13	2020-10-10	2021-11-09	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3490874817	2020-10-10	2020-10-10	2021-11-09	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3490874054	2020-10-10	2020-10-10	2021-11-09	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3490836563	2020-10-10	2020-10-10	2021-11-09	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3490818688	2020-10-10	2020-10-10	2021-11-09	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3448352963	2020-09-30	2020-09-30	2021-10-30	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
3427615814	2020-09-25	2020-09-25	2021-10-25	anywhere.epam.com	anywhere.epam.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
2327760733	2020-01-11	2020-01-11	2020-04-10	invitation.anywhere.epam.com	invitation.anywhere.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2318018336	2020-01-11	2020-01-11	2020-04-10	invitation.anywhere.epam.com	invitation.anywhere.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2101661119	2019-11-12	2019-11-12	2020-02-10	invitation.anywhere.epam.com	invitation.anywhere.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2101661105	2019-11-12	2019-11-12	2020-02-10	invitation.anywhere.epam.com	invitation.anywhere.epam.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Finding a Live Sub-Domain

6. Httprobe

Httprobe is a utility that quickly searches for live http and https servers. This tool can be used to rapidly determine which subdomains are active if a user has a list of them. Users must be familiar with Golang because this tool was written in that language. Users must first print their domain list and pass it to httprobe in order to use httprobe.
Some of httprobe's primary characteristics are as follows:

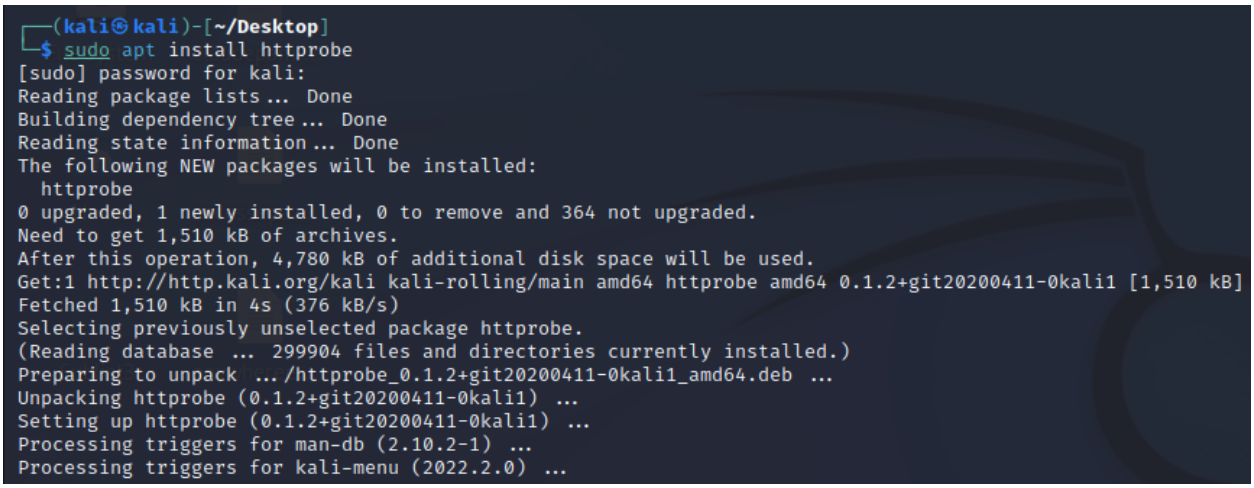
- httprobe by default looks for http on port 80 and https on port 443.
- Using the '-p' argument, we may add more ports.
- The default ports will be disregarded if the '-s' argument is used.
- If the user anticipates a long response time from the destination server, the '-t' argument can be used to provide a custom timeout. Milliseconds are used to set the time.
- Users can use 'httprobe' in conjunction with other tools like 'assetfinder,"subfinder,' and so on.

Installation

I have installed httprobe with the command

“sudo apt install httprobe”

The installation process is as follows,



Then I used the text files which were used to store the subdomain lists generated with findomain as the input for httprobe to find the live sub-domains.

Used this command:

“cat <filepath> | httprobe”

After successfully scanned the subdomains in the text files it returned the live sub-domains categorized according to the implemented protocol. (HTTP or HTTPS)

Here’s the results of all four domains using httprobe: (saved by me in separate text files for four domains named “<domain>live.txt”.)

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat epamcom.txt | httprobe
http://evusprisa0004.princeton.epam.com
https://interview-public.epam.com
http://interview-public.epam.com
https://reportportal.epam.com
http://reportportal.epam.com
http://m3demo.cloud.epam.com
http://ecsa00401230.epam.com
https://vpn-us.epam.com
http://vpn-us.epam.com
https://letter.lab.epam.com
https://upload.videoportal.epam.com
http://upload.videoportal.epam.com
https://vacation.epam.com
https://officespace.epam.com
http://vacation.epam.com
http://officespace.epam.com
http://learnstudio.epam.com
http://epam-advisor-stage.epm-path.projects.epam.com
https://grow.epam.com
http://evusprisa0072.princeton.epam.com
https://lyncdiscover.epam.com
http://grow.epam.com
http://lyncdiscover.epam.com
https://static-aws.epm-ldi.projects.epam.com
http://static-aws.epm-ldi.projects.epam.com
https://demolab-staging.epm-ddl.projects.epam.com
http://demolab-staging.epm-ddl.projects.epam.com
http://graph-collector-api.connect.epm-plx.projects.epam.com
https://moobud.epam.com
http://showcase.epam.com
https://university.epam.com
http://university.epam.com
https://teams-notify-stage.epm-ppa.projects.epam.com
https://hdo.epam.com
http://teams-notify-stage.epm-ppa.projects.epam.com
http://hdo.epam.com
http://velcom.minsk.epam.com
https://sharepoint.epam.com
http://lifescience.opensource.epam.com
http://sharepoint.epam.com
http://delivery.epam.com
https://ecsa0040088e.epam.com
https://jiraeu.epam.com
http://ecsa0040088e.epam.com
http://jiraeu.epam.com
https://ecse00500ab0.epam.com
http://ecse00500ab0.epam.com
https://dhm2-performance.health.epam.com
http://dhm2-performance.health.epam.com
https://jira-api.epam.com
http://jira.epam.com
http://exam.epam.com
https://disc.crm.epam.com
http://disc.crm.epam.com
https://video.epam.com
https://rd.lab.epam.com
http://rd.lab.epam.com
http://video.epam.com
http://dev-admin.osdu-gcp.go3-nrg.project
https://spa-staging.amwl-apps.projects.ep
http://spa-staging.amwl-apps.projects.epa

┌──(kali㉿kali)-[~/Desktop]
└─$ cat accessepam.txt | httprobe
https://access.epam.com
http://access.epam.com

┌──(kali㉿kali)-[~/Desktop]
└─$ cat cloudepam.txt | httprobe
https://config.cloud.epam.com
https://stage.cloud.epam.com
http://stage.cloud.epam.com
https://m3qa.cloud.epam.com
http://m3qa.cloud.epam.com
https://sdk.cloud.epam.com
http://sdk.cloud.epam.com
https://dev.cloud.epam.com
https://cloud.epam.com
http://cloud.epam.com
http://dev.cloud.epam.com
http://qa.cloud.epam.com
https://maestro3.cloud.epam.com
http://maestro3.cloud.epam.com
http://m3demo.cloud.epam.com

┌──(kali㉿kali)-[~/Desktop]
└─$ cat anywhereepam.txt | httprobe
https://vacancies.anywhere.epam.com
http://vacancies.anywhere.epam.com
https://calc.anywhere.epam.com
http://calc.anywhere.epam.com
https://anywhere.epam.com
https://ssgtm.anywhere.epam.com
http://anywhere.epam.com
http://ssgtm.anywhere.epam.com
https://info.anywhere.epam.com
http://info.anywhere.epam.com
https://business.anywhere.epam.com
http://business.anywhere.epam.com
```

DNS Enumeration

1. DNS Lookup

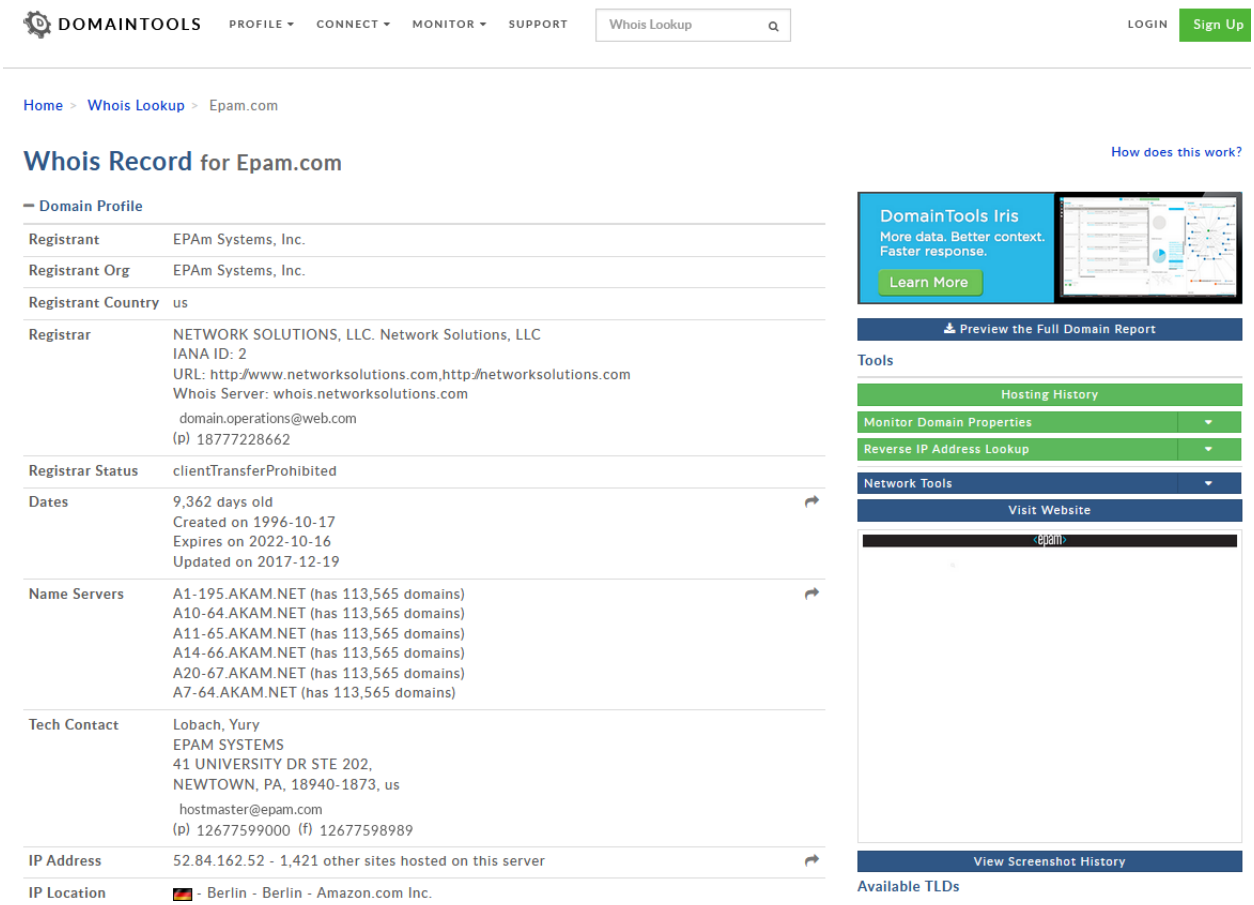
WHOIS is a framework for obtaining information on an internet resource like a domain name, an IP address block, or an autonomous system. This protocol is used to store information in a database and to deliver the information in a human-readable format from the database. RFC 3912 contains complete WHOIS documentation.

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

This tool will produce a list which contain following details when we enter a domain name or a Ip address of a site,

- Details of the owner of the Domain
- IP address of the given site if searched with Domain
- Hosting server's details

I have searched for all four domains and got the following result which I have saved in separate text files.

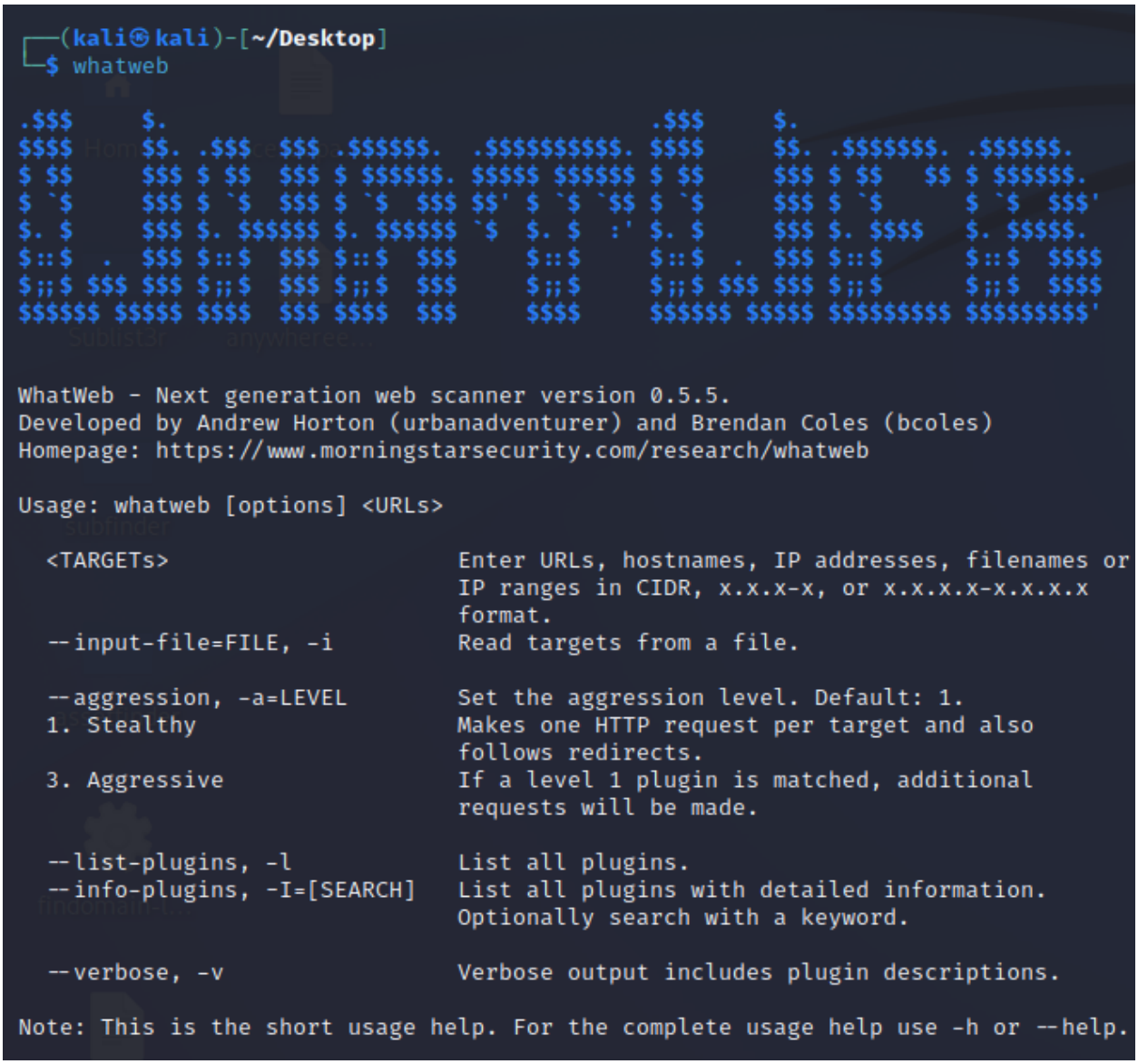


2. Whatweb

WhatWeb is a Kali Linux open-source program that detects web technologies such content management systems (CMS), blogging platforms, statistical/analytics packages, JavaScript libraries, web servers, and embedded devices. There are approximately 1700 plugins on WhatWeb, each of which detects something different. Version numbers, email addresses, account IDs, web framework modules, SQL problems, and other data are all recognized by WhatWeb.

Whatweb basically have three types of aggressions. Stealthy which is default level of aggression is the fastest and requires only one http request to a website. This mechanism is most suitable for scanning publicly available websites. More aggressive modes have been developed for used in penetration testing. Following is a list of key features which the whatweb possess,

- Having 1700+ plugins
- Ability to define custom plugins in the command line
- Managing the tradeoff between reliability, speed, and stealth.
- As a result, there is a sense of assurance.
- Example URLs are included in the plugins
- Fuzzy matching
- Tunning performance by controlling the number of simultaneous scans
- Using IP ranges in the style of Nmap
- Having multiple formats of logs: Brief, Verbose, XML, JSON, MagicTree, RubyObject, MongoDB, SQl, and ElasticSearch
- Controlling the redirection of webpages
- Proxy support including TOR
- Authentication with basic HTTP
- Custom HTTP headers



As all of my selected domains are publicly available, I had to use default aggression level when scanning.

I used the command

"whatweb -v <domain>"

To scan the four domains and stored the details in text files for further references.

The results are as follows for the four domains:

1. *.epam.com

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Desktop]
└─$ whatweb -v epam.com
WhatWeb report for http://epam.com
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 3.214.134.159
Country   : UNITED STATES, US

Summary   : RedirectLocation[https://www.epam.com], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], UncommonHeaders[x-content-type-options], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]

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

        String       : https://www.epam.com (from location)

[ 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=31536000; includeSubDomains; preload

[ 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       : x-content-type-options (from headers)

[ 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       : SAMEORIGIN

[ 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/1.1 301 Moved Permanently
```

2. Cloud.epam.com

```
┌──(kali㉿kali)-[~/Desktop]
└─$ whatweb -v cloud.epam.com
WhatWeb report for http://cloud.epam.com
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 13.224.250.101
Country   : UNITED STATES, US

Summary   : CloudFront, HTTPServer[CloudFront], RedirectLocation[https://cloud.epam.com/], UncommonHeaders[x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 db8d6eb1919ade2943f
ront)]

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       : https://cloud.epam.com/ (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-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : 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 db8d6eb1919ade2943f4a573a505ba66.cloudfront.net (CloudFront)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Server: CloudFront
        Date: Sun, 05 Jun 2022 11:10:40 GMT
        Content-Type: text/html
        Content-Length: 183
        Connection: close
        Location: https://cloud.epam.com/
        X-Cache: Redirect from cloudfront
```

3. access.epam.com

```
┌──(kali㉿kali)-[~/Desktop]
└─$ whatweb -v access.epam.com
WhatWeb report for http://access.epam.com
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 13.224.250.121
Country   : UNITED STATES, US

Summary   : CloudFront, HTTPServer[CloudFront], RedirectLocation[https://access.epam.com/], UncommonHeaders[referrer-policy,content-security-policy
roxy[1.1 61bff898c9646bbcc7f7eadde4d76fe4.cloudfront.net (CloudFront)], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]

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       : https://access.epam.com/ (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-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : referrer-policy,content-security-policy,x-content-type-options,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 61bff898c9646bbcc7f7eadde4d76fe4.cloudfront.net (CloudFront)

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

        String       : SAMEORIGIN

[ X-XSS-Protection ]
```

4. anywhere.epam.com

```
┌──(kali㉿kali)-[~/Desktop]
└─$ whatweb -v anywhere.epam.com
WhatWeb report for http://anywhere.epam.com
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 13.224.250.40
Country   : UNITED STATES, US

Summary   : CloudFront, HTTPServer[CloudFront], RedirectLocation[https://anywhere.epam.com/], UncommonHeaders[x-amz-cf-pop,x-amz-cf-id
udFront)]

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       : https://anywhere.epam.com/ (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-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : 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 ccd5ce8e69d2dc421327946b6ecb3cbc.cloudfront.net (CloudFront)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Server: CloudFront
        Date: Sun, 05 Jun 2022 11:32:59 GMT
        Content-Type: text/html
        Content-Length: 183
        Connection: close
        Location: https://anywhere.epam.com/
```

3. NS Lookup and Dig

For collecting information from a DNS server, Nslookup (name server lookup) is useful. It's a network administration tool that searches the Domain Name System (DNS) for domain name or IP address mapping information, as well as any other DNS records. It's also used to diagnose DNS problems.

Installation

Installation of DNS utilities including NS Lookup and Dig can be done with following command:

"sudo apt install dnsutils"

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt install dnsutils
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  dnsutils
0 upgraded, 1 newly installed, 0 to remove and 364 not upgraded.
Need to get 271 kB of archives.
After this operation, 283 kB of additional disk space will be used.
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 dnsutils all 1:9.18.1-1 [271 kB]
Fetched 271 kB in 3s (107 kB/s)
Selecting previously unselected package dnsutils.
(Reading database ... 299910 files and directories currently installed.)
Preparing to unpack .../dnsutils_1%3a9.18.1-1_all.deb ...
Unpacking dnsutils (1:9.18.1-1) ...
Setting up dnsutils (1:9.18.1-1) ...
```

Here is the result obtain through using the 'nslookup' command on four domains and they were saved manually in four text documents.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nslookup epam.com
Server:         192.168.137.2
Address:        192.168.137.2#53

Non-authoritative answer:
Name:   epam.com
Address: 3.214.134.159
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nslookup cloud.epam.com
Server:         192.168.137.2
Address:        192.168.137.2#53

Non-authoritative answer:
Name:   cloud.epam.com
Address: 13.224.250.93
Name:   cloud.epam.com
Address: 13.224.250.45
Name:   cloud.epam.com
Address: 13.224.250.125
Name:   cloud.epam.com
Address: 13.224.250.101
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nslookup access.epam.com
Server:         192.168.137.2
Address:        192.168.137.2#53

Non-authoritative answer:
Name:   access.epam.com
Address: 13.224.250.121
Name:   access.epam.com
Address: 13.224.250.67
Name:   access.epam.com
Address: 13.224.250.128
Name:   access.epam.com
Address: 13.224.250.101
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nslookup anywhere.epam.com
Server:         192.168.137.2
Address:        192.168.137.2#53

Non-authoritative answer:
Name:   anywhere.epam.com
Address: 13.224.250.58
Name:   anywhere.epam.com
Address: 13.224.250.40
Name:   anywhere.epam.com
Address: 13.224.250.26
Name:   anywhere.epam.com
Address: 13.224.250.100
```

In Linux, the "dig" command is used to gather DNS information. Domain Information Groper is a tool that collects information on Domain Name Servers. The "dig" command is useful for troubleshooting DNS problems, as well as displaying DNS information, although it didn't provide much information about the target at the time.

Here shown below the result of dig command on four domains which were saved in text files.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig epam.com

; <<>> DiG 9.18.1-1-Debian <<>> epam.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18409
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;epam.com.                      IN      A

;; ANSWER SECTION:
epam.com.               5       IN      A       3.214.134.159

;; Query time: 3 msec
;; SERVER: 192.168.137.2#53(192.168.137.2) (UDP)
;; WHEN: Sun Jun 05 09:07:52 EDT 2022
;; MSG SIZE  rcvd: 53
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig cloud.epam.com

; <<>> DiG 9.18.1-1-Debian <<>> cloud.epam.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33089
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;cloud.epam.com.                        IN      A

;; ANSWER SECTION:
cloud.epam.com.         5       IN      A       13.224.250.101
cloud.epam.com.         5       IN      A       13.224.250.125
cloud.epam.com.         5       IN      A       13.224.250.45
cloud.epam.com.         5       IN      A       13.224.250.93

;; Query time: 3 msec
;; SERVER: 192.168.137.2#53(192.168.137.2) (UDP)
;; WHEN: Sun Jun 05 09:08:19 EDT 2022
;; MSG SIZE  rcvd: 107
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig access.epam.com

; <<>> DiG 9.18.1-1-Debian <<>> access.epam.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36140
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;access.epam.com.               IN      A

;; ANSWER SECTION:
access.epam.com.        5       IN      A       13.224.250.101
access.epam.com.        5       IN      A       13.224.250.128
access.epam.com.        5       IN      A       13.224.250.67
access.epam.com.        5       IN      A       13.224.250.121

;; Query time: 4 msec
;; SERVER: 192.168.137.2#53(192.168.137.2) (UDP)
;; WHEN: Sun Jun 05 09:08:37 EDT 2022
;; MSG SIZE  rcvd: 108
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig anywhere.epam.com

; <<>> DiG 9.18.1-1-Debian <<>> anywhere.epam.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29179
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;anywhere.epam.com.             IN      A

;; ANSWER SECTION:
anywhere.epam.com.      5       IN      A       13.224.250.100
anywhere.epam.com.      5       IN      A       13.224.250.26
anywhere.epam.com.      5       IN      A       13.224.250.40
anywhere.epam.com.      5       IN      A       13.224.250.58

;; Query time: 0 msec
;; SERVER: 192.168.137.2#53(192.168.137.2) (UDP)
;; WHEN: Sun Jun 05 09:08:58 EDT 2022
;; MSG SIZE  rcvd: 110
```

Archived Information Enumeration

1. Wayback machine

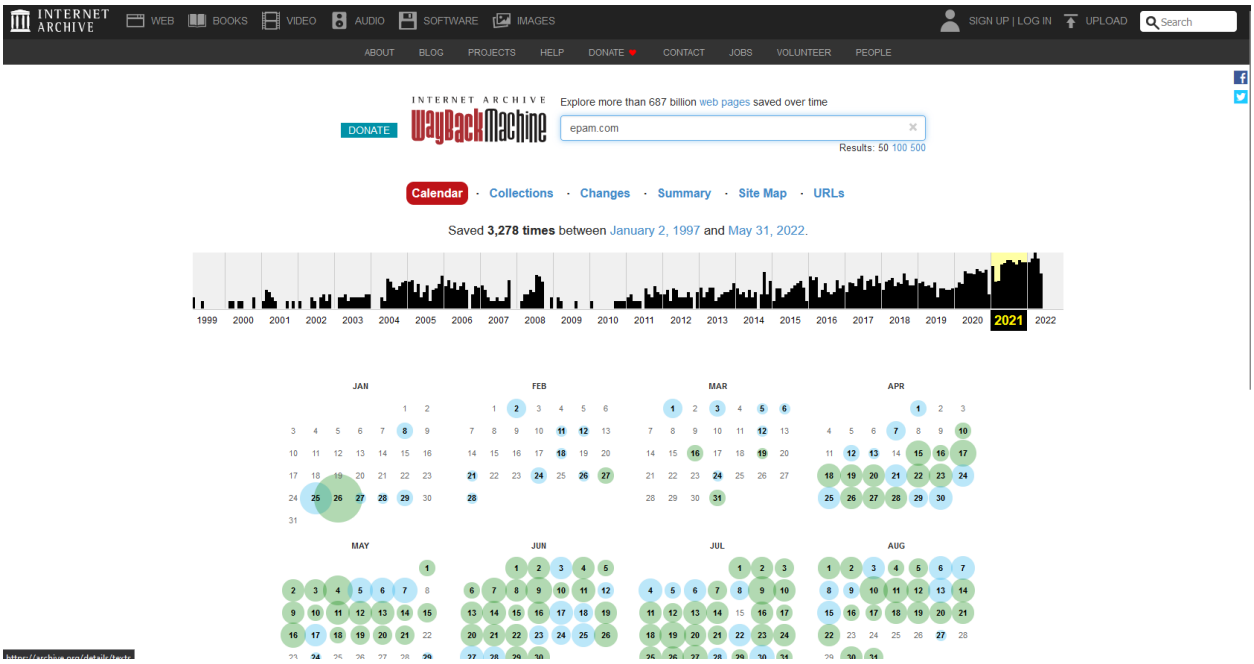
Accessible via https://web.archive.org/

The Wayback Machine, a digital archiver, was funded by Brewster Kahle and Bruse Gillit. It was originally made public in 2001, and it lets users to "go back in time" to view how websites appeared in the past. The Wayback Machine now has over 613 billion online pages stored. It was created with the goal of providing "universal access to all knowledge" by archiving copies of defunct web pages.

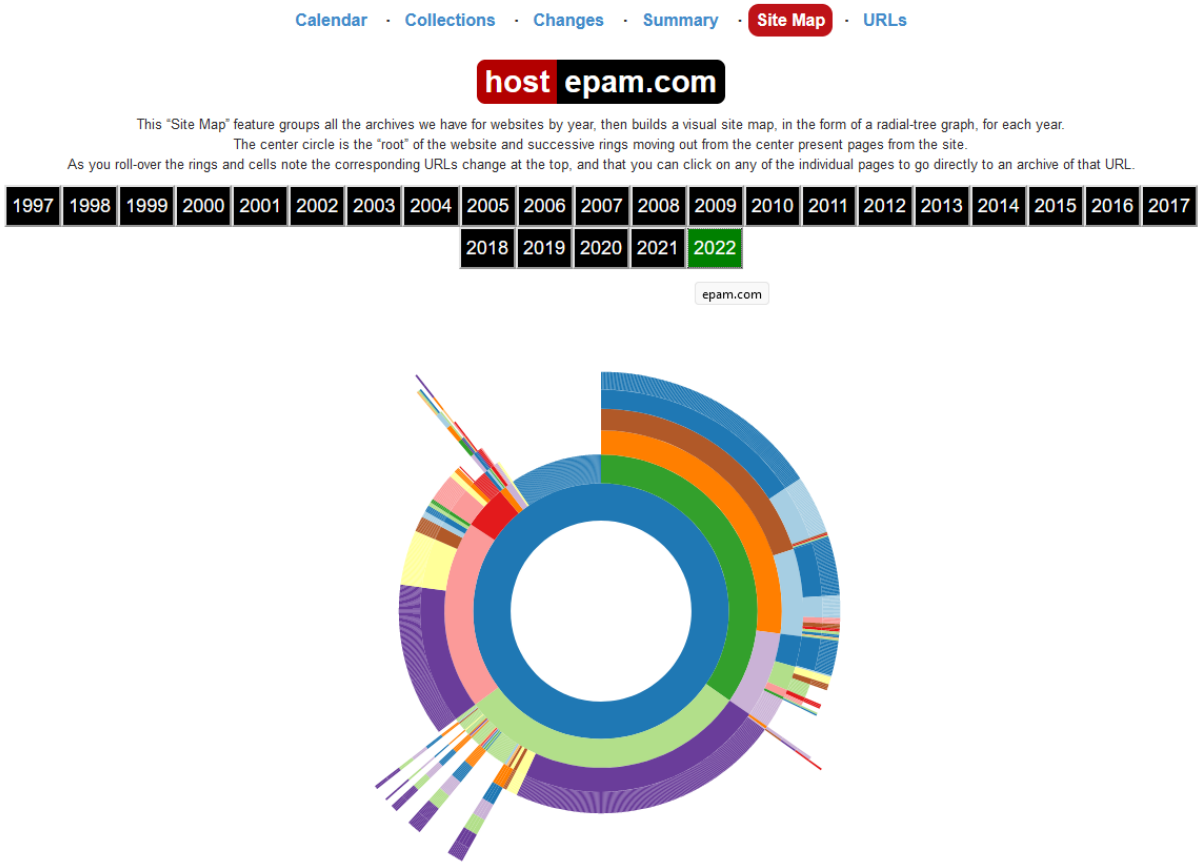
This site is quite useful for information collecting because it discovers some interesting material while crawling.

- New technologies which have been implemented
- Old endpoints which have been forgotten
- Confidential information (including JS files, php files)

Here's the interface of Wayback Machine which scanned epam.com. As usual I have recorded found detail for four domains in separate files.



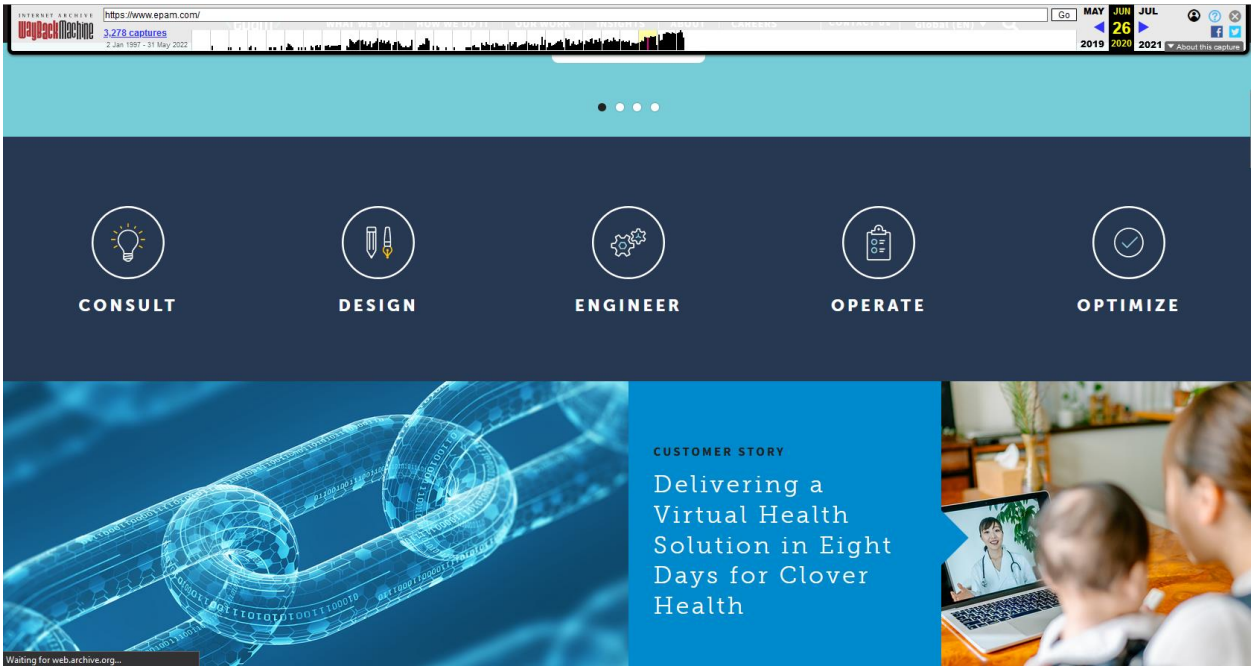
The site map feature allows us to view available subdomains and the way the have changed over time.



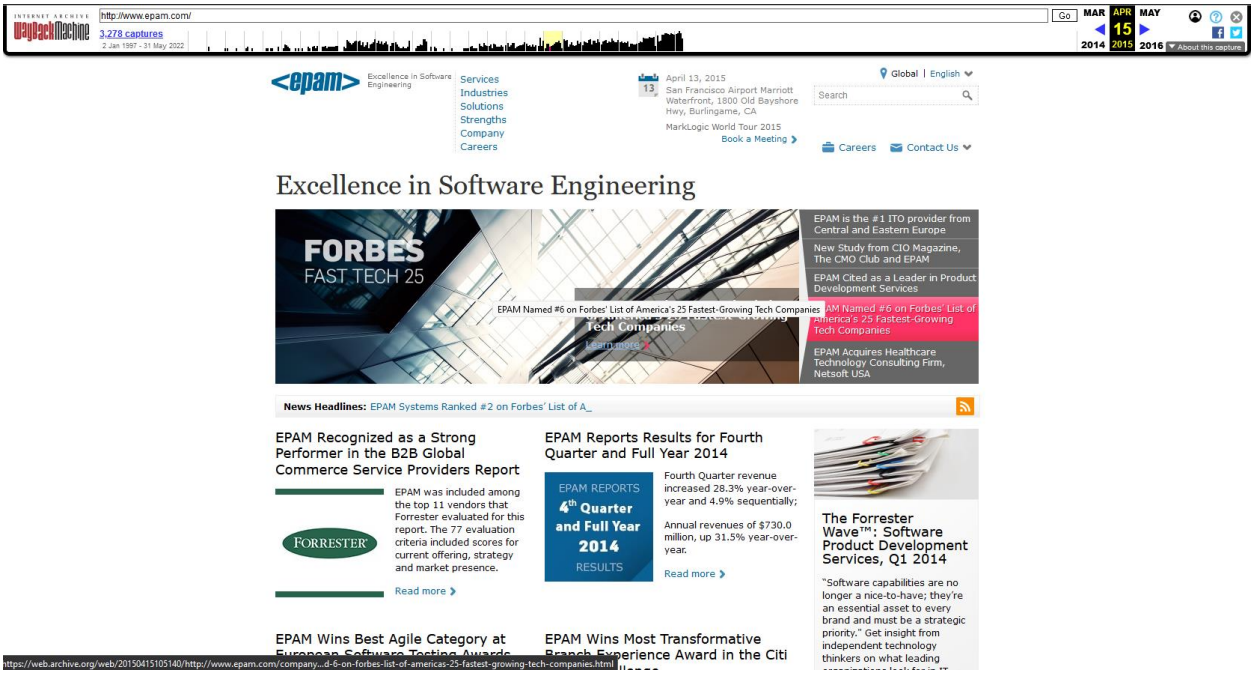
Here are the snaps of how four domains have been changed over the time.

epam.com – 2021

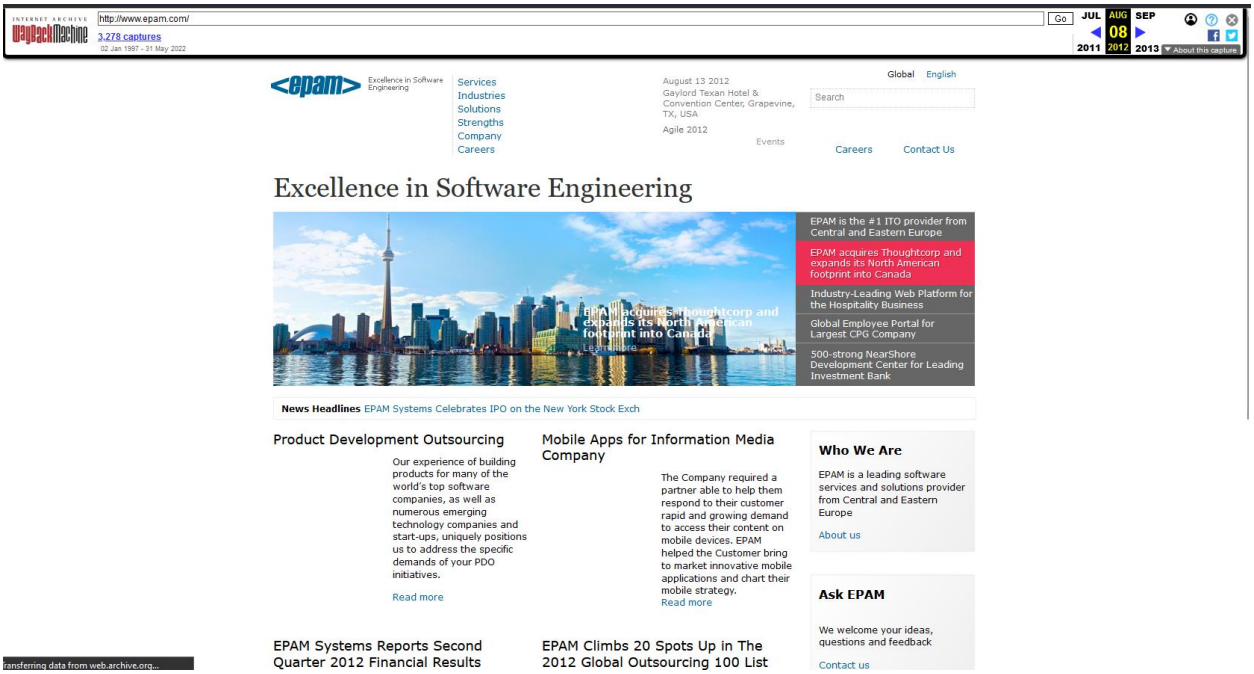
epam.com – 2020



epam.com – 2015



epam.com – 2012



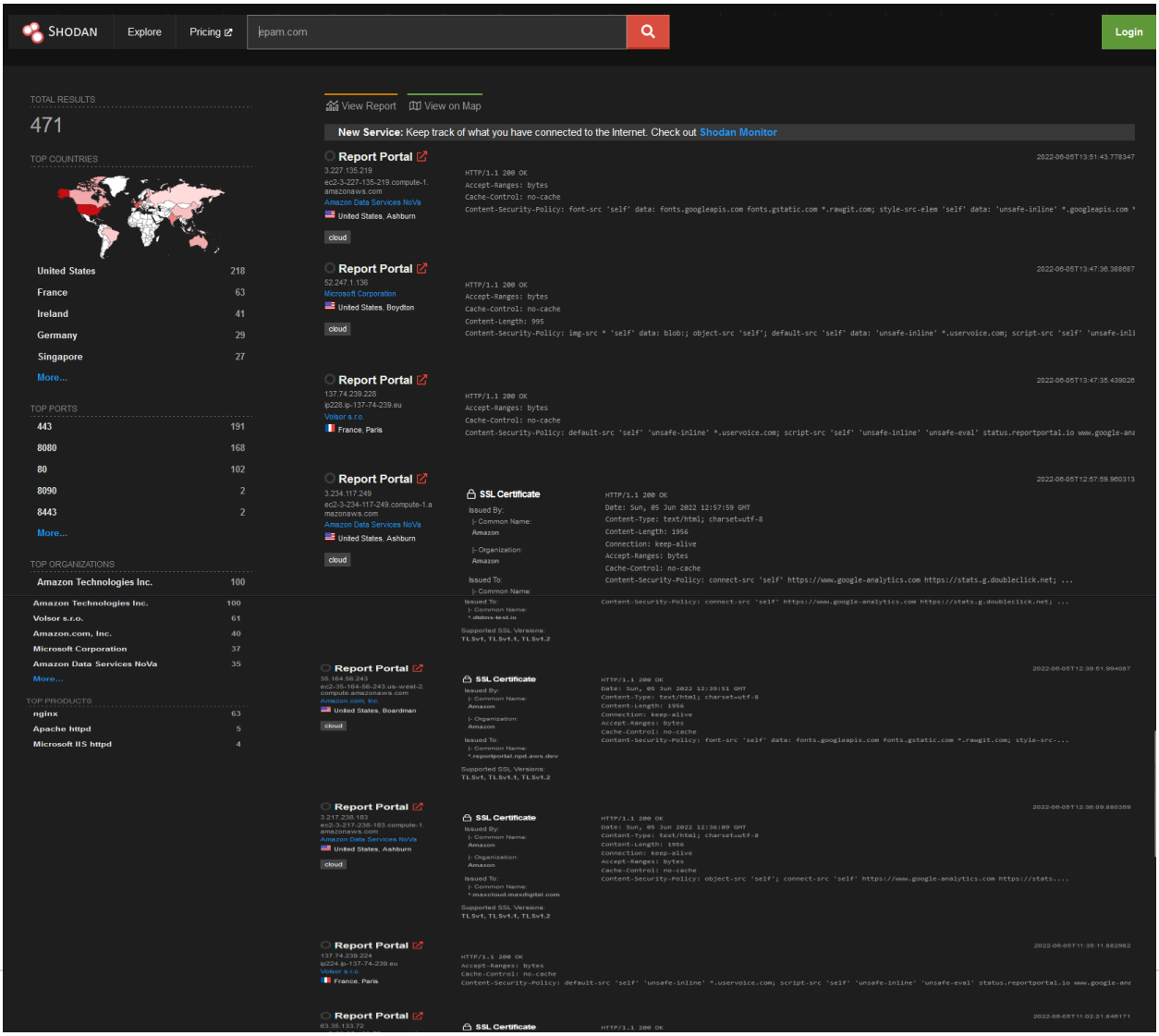
Same process was done for all the four domains and recorded needed information on text files.

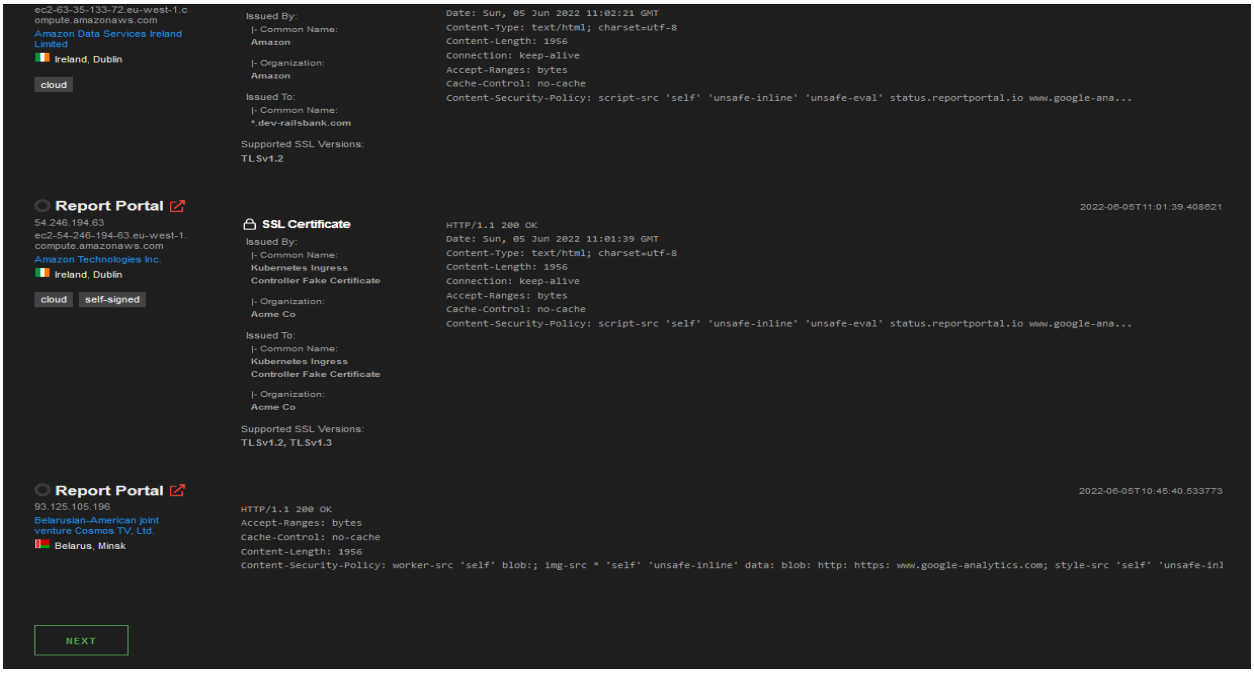
Enumeration of Public Devices

1. Shodan

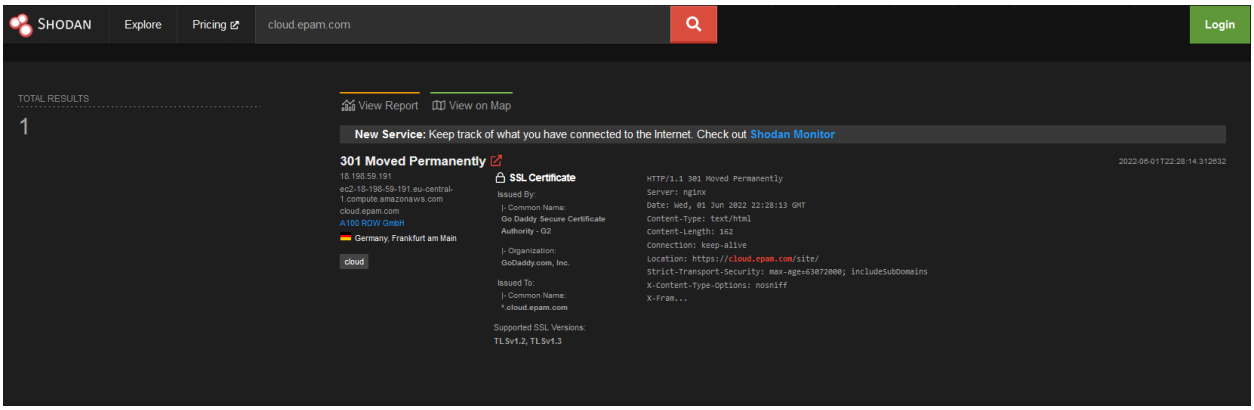
Accessible at https://www.shodan.io/

Shodan is a search engine for internet-connected devices. Shodan basically gathers data on all devices that are directly linked to the Internet. Shodan searches for a range of publicly available information when a device is directly connected to the Internet. Shodan will list the target domain if it exposes any public IP address service on a certain port. We may get not only the IP address, but also information about the site server, banners, Internet provider, Secure shell, File transfer protocol, and other things. Here are the findings on epam.com domain in shodan.io.

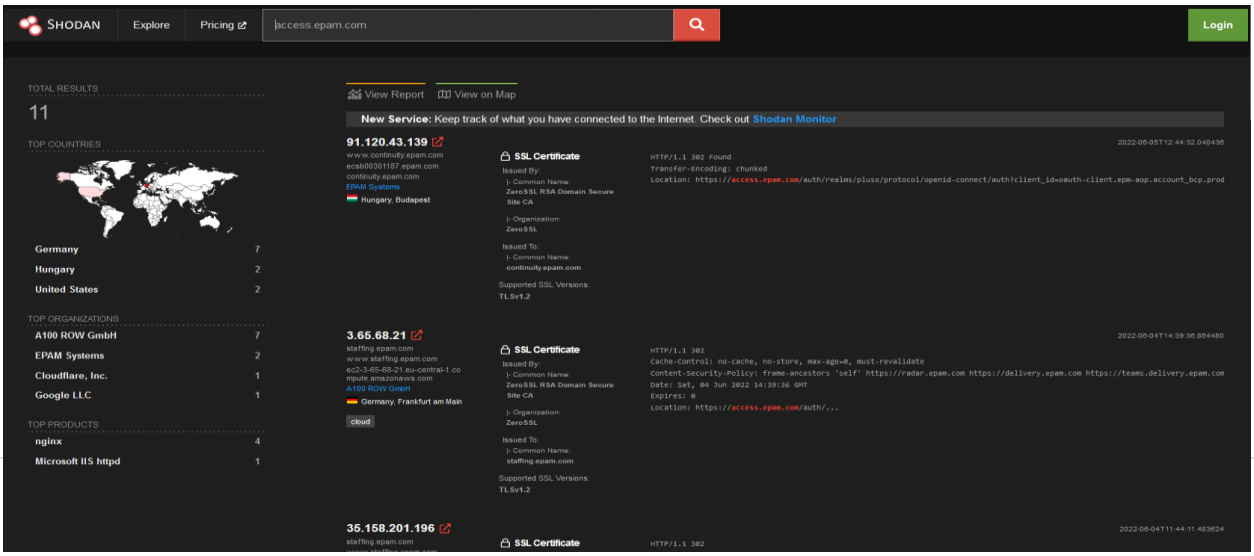




Here’s the results for cloud.epam.com:



Here’s the results for access.epam.com:



Unfortunately, there are no results from Shodan for anywhere.epam.com.

The details discovered and enumerated through Shodan on three domains were recorded.

Vulnerability Analyzing Phrase

OWASP Top 10 Security Risks and Vulnerabilities 2022

The OWASP Top 10 is a standard awareness document for web application security and developers. It reflects widespread agreement on the most serious security threats to web applications. As a result, I used the OWSAP top 10 list to find the vulnerabilities in the targeted domains.

- A01 Broken Access Control
- A02 Cryptographic Failures
- A03 Injection
- A04 Insecure Design
- A05 Security Misconfiguration
- A06 Vulnerable and Outdated Components
- A07 Identification and Authentication Failures
- A08 Software and Data Integrity Failures

- A09 Security Logging and Monitoring Failures

- A10 Server Side Request Forgery (SSRF)

1. Legion

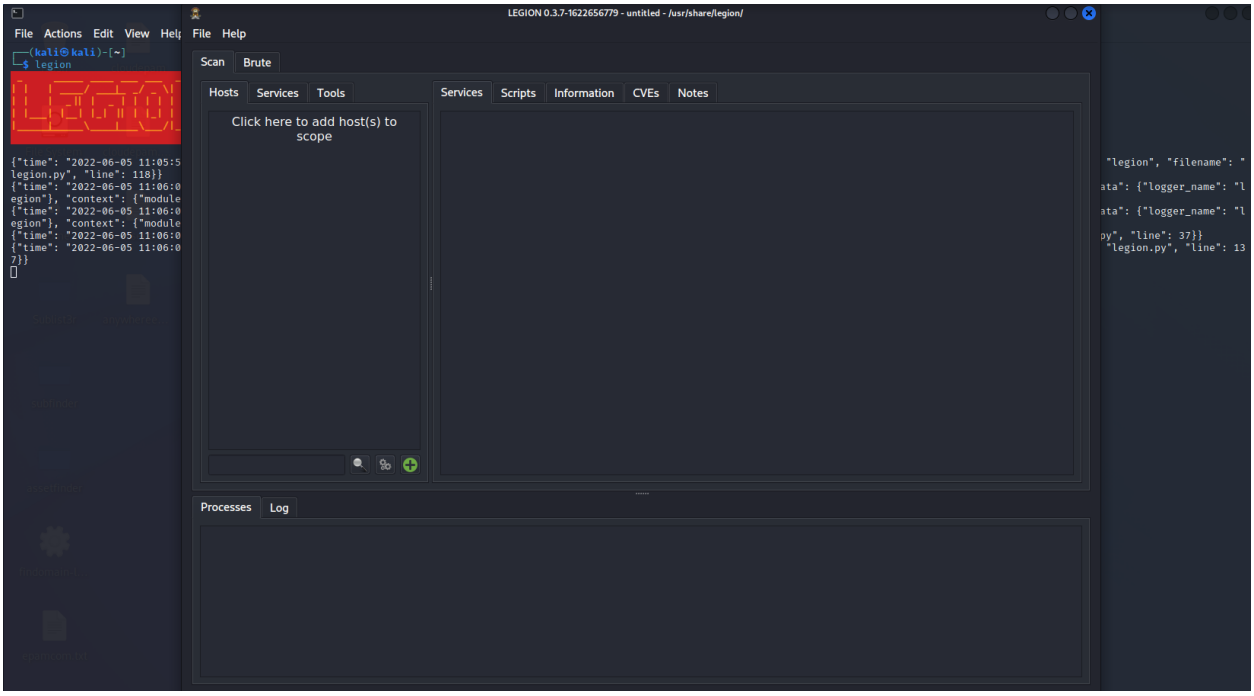
Legion is a semi-automated network penetration testing tool that aids in information system discovery, reconnaissance, and exploitation. It is open source, user-friendly, and super-extensible. With around 100 auto-scheduled scripts, this program integrates with NMAP, Shodan, whataweb, nikto, Vulners, Hydra, SMBenum, dirbuster, sslyzer, webslayer, and other tools to automate recon and scanning. Here are some of the most important features:

- Legion is simple to use and owing to a graphical interface with extensive context menus and panels, pen-testers can quickly locate and exploit attack routes on hosts.
- Tasks are saved in real time automatically.
- The modular nature allows users to quickly configure Legion and call their own scripts/tools.
- Stage scanning with a high level of customization for ninja-like IPS evasion CPEs (Common Platform Enumeration) and CVEs (Common Vulnerabilities and Exposures) are automatically recognized, as are Project outcomes.

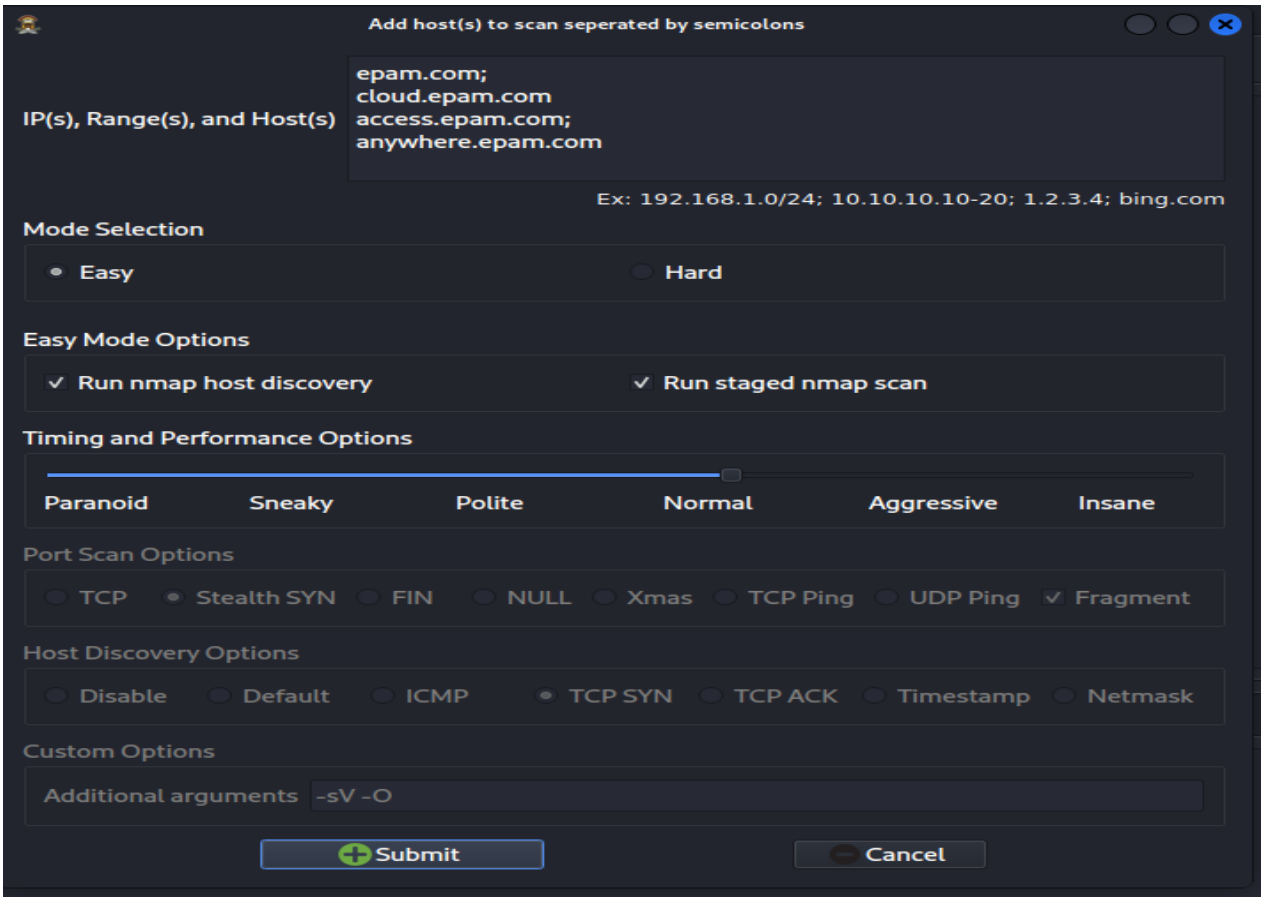
Installation

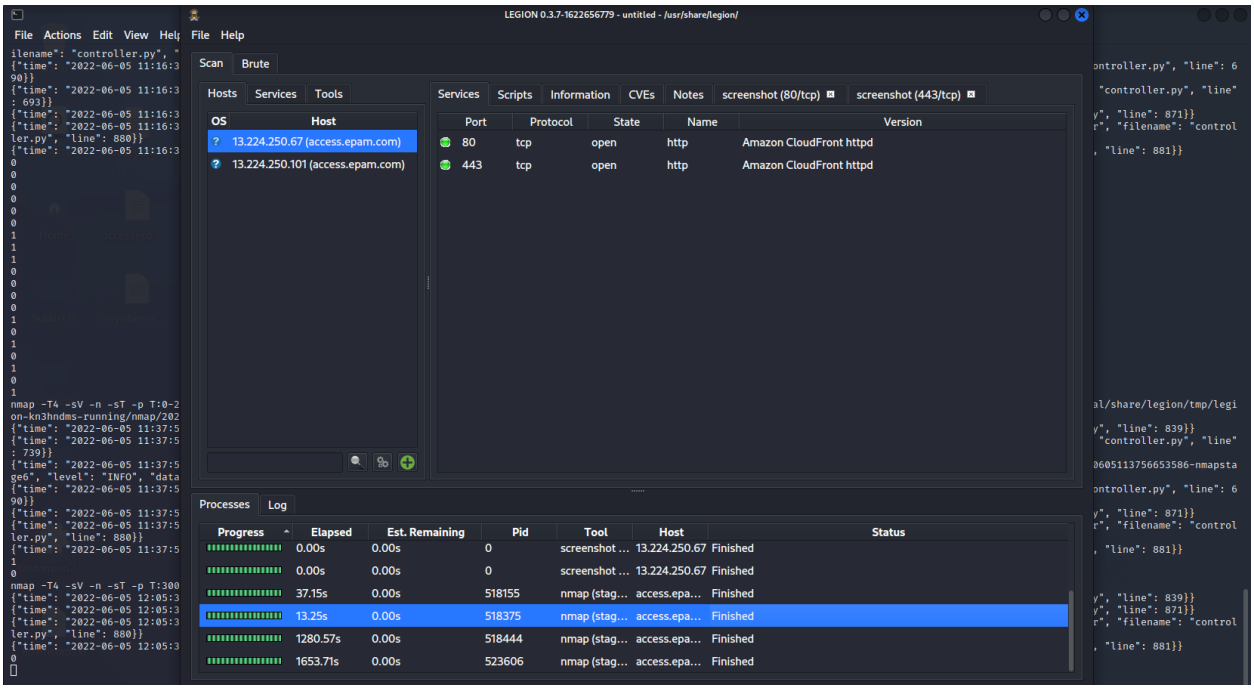
This tool is also can be found in Kali Linux systems prebuilt.

Tool will look as follows when launched:



I ran a scan for all four domains using legion in easy mode with normal aggression.





After a few rounds of scanning, the tool returns open ports information and basic domain information, but it failed to detect any basic vulnerabilities.

2. Netsparker

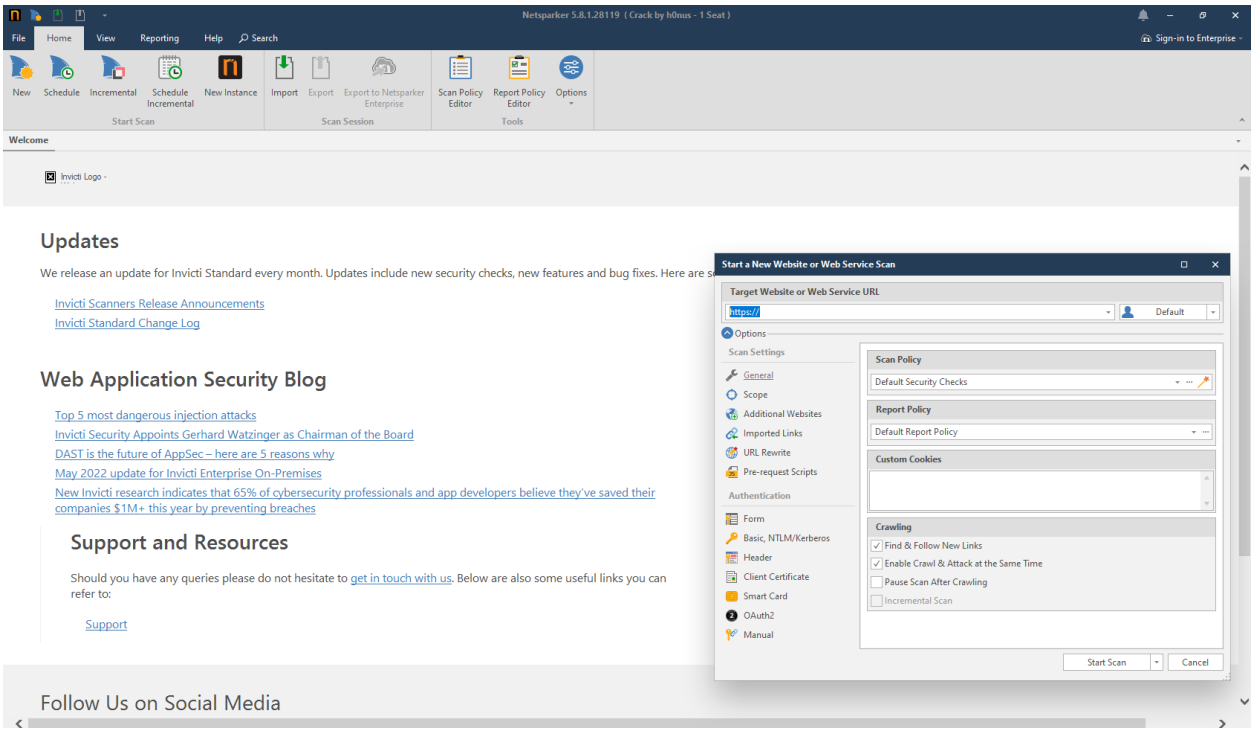
Netsparker is a commercial web application security scanner that is fully automated. It checks websites, web applications, and web services for security problems and reports them. This utility is a web application security scanner that automatically exploits detected vulnerabilities in a read-only and secure manner to confirm issues. The Netsparker utility has a number of significant features, which are listed below.

- High accuracy
- Detailed Report
- Proof-based scanning
- Proof of concept
- Proof of exploit

Installation

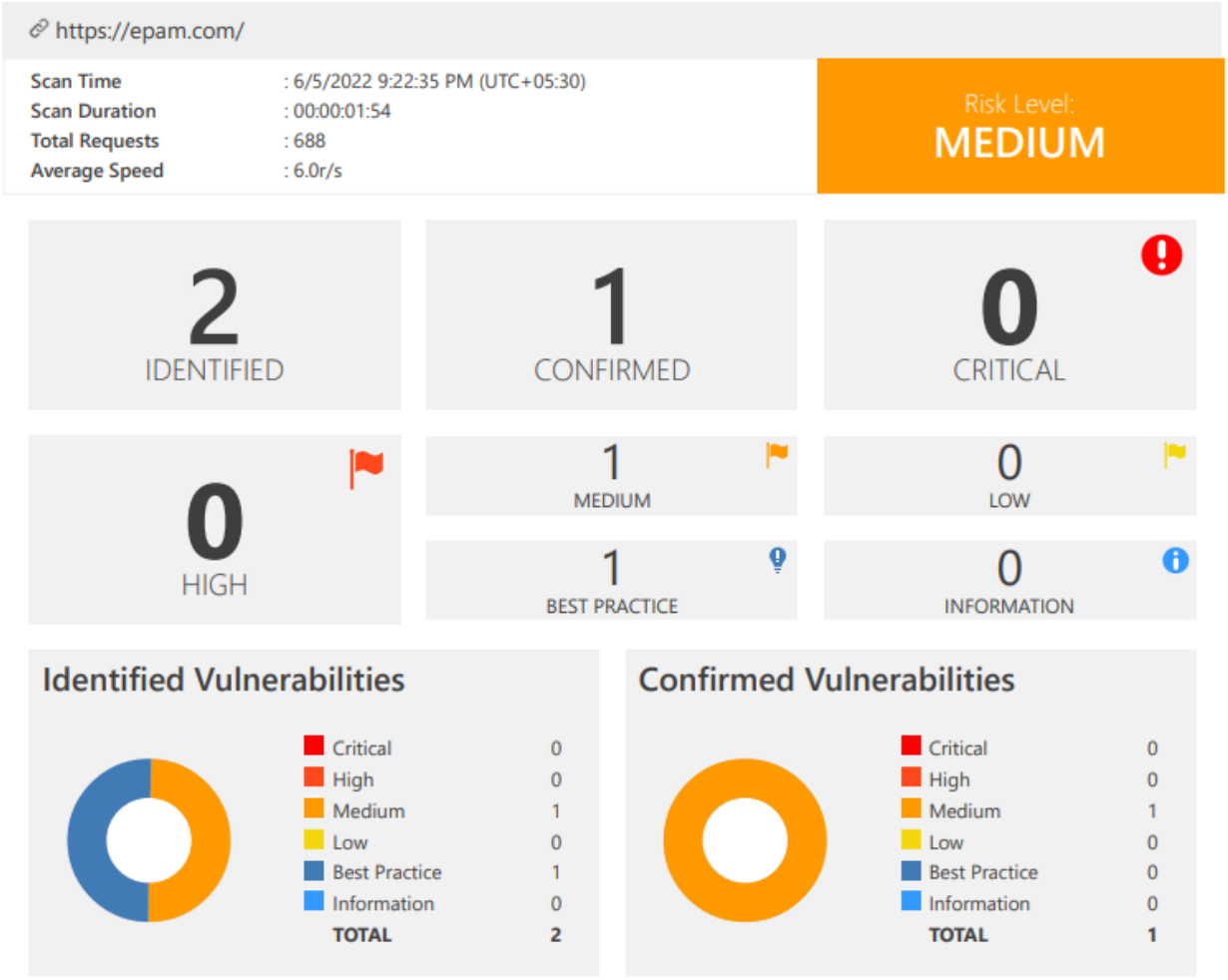
Users must purchase the Netsparker pro editions in order to perform real-time, accurate scanning.

Accessible via : https://www.netsparker.com/



I used this version and scanned the target domains one by one and obtained the results. The analysis of discovered vulnerabilities are as follows.

1. Targeted Domain: epam.com



1. Weak Ciphers Enabled

Severity : Medium
Method : GET
OWASP : No 02 type

Impact

Attackers might be able to decrypt the SSL traffic between the server and the visitors.

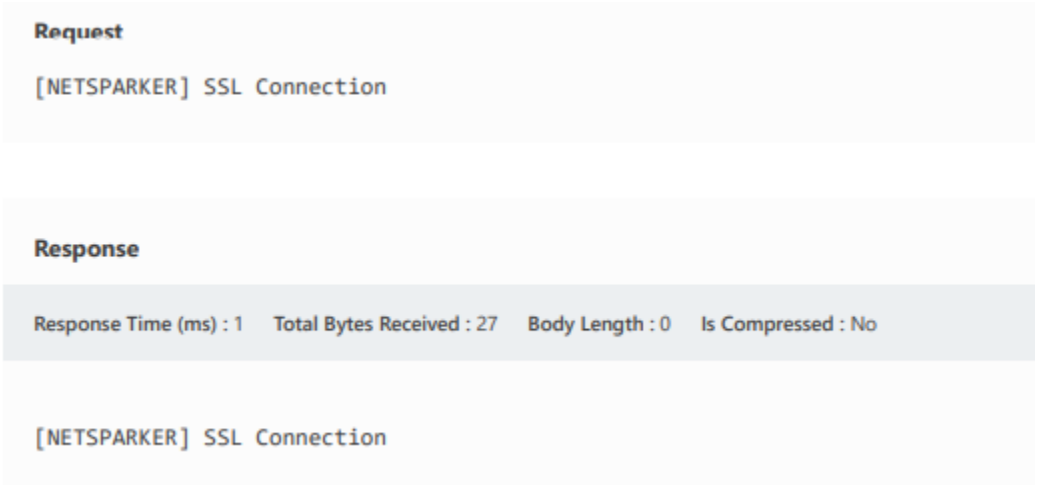
External References:

- 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

Supported weak Ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)

Way Identified the vulnerability



Actions to do:

1. You should modify the SSLCipherSuite directive in httpd.conf for Apache

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

2. For Lighttpd:

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

3. You should make some changes to the system registry for Microsoft IIS.

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

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

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

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

Remedy

Admin should configure the web server to disallow the usage of weak ciphers.

Classification

CLASSIFICATION

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

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

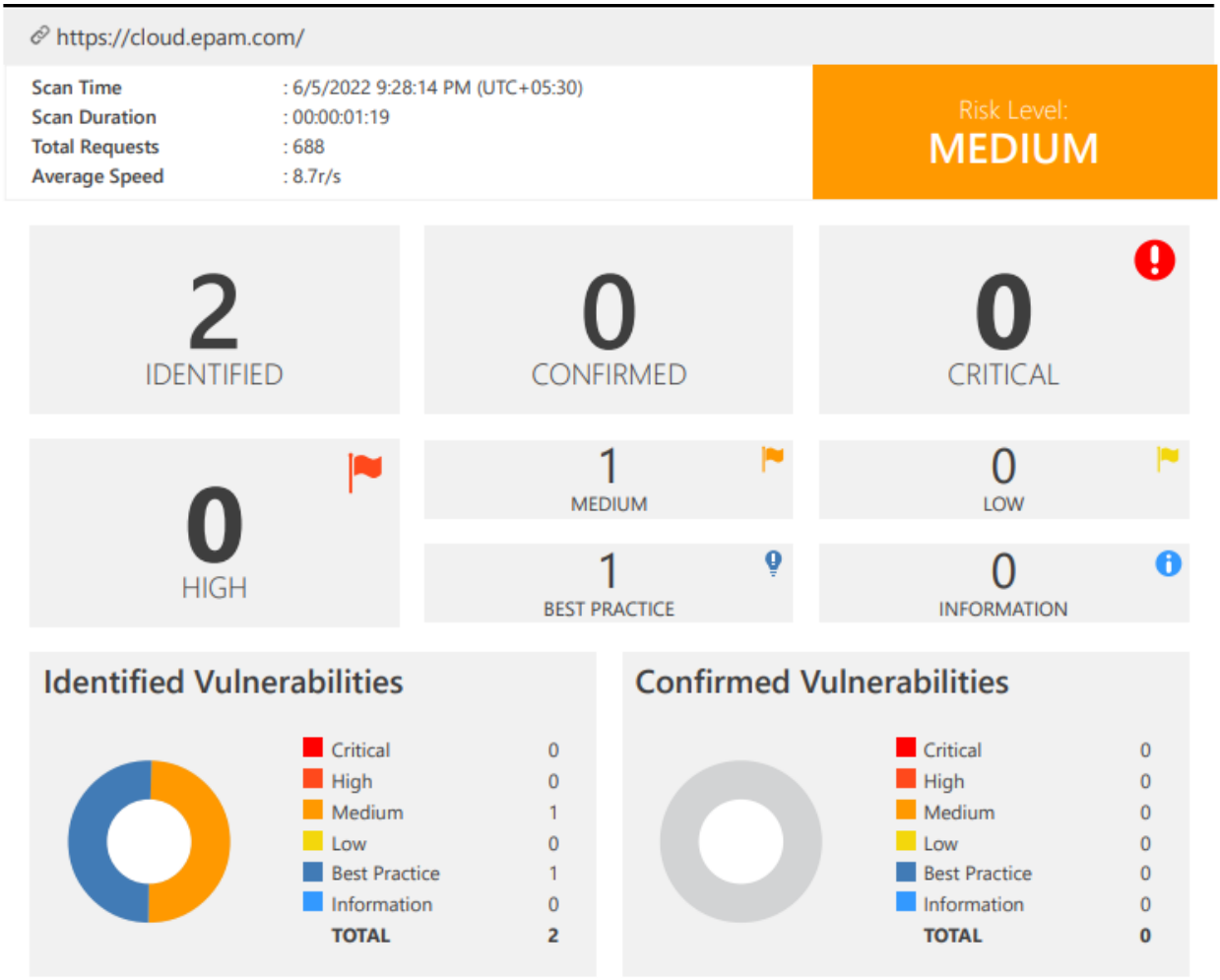
CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

2. Targeted Domain: cloud.epam.com

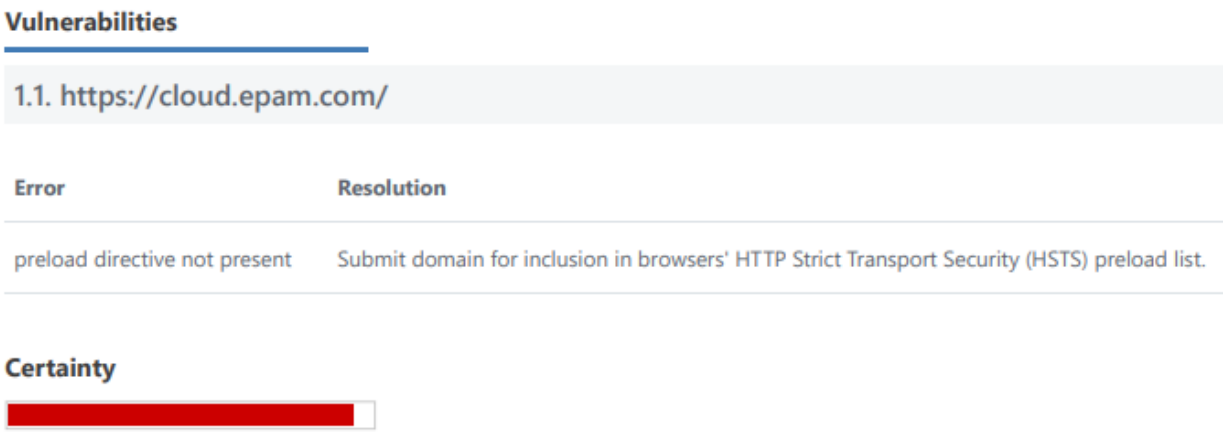


A. <u>HTTP Strict Transport Security (HSTS) Errors and Warnings</u>

Severity : Medium
Method : GET
OWASP : No 06 type

<u>Impact</u>

The HSTS Warning and Error may allow attackers to circumvent HSTS, allowing them to view and change your website communications.



Remedy

After addressed the problems and warnings, you should think about adding your domain to the HSTS preload list. This will ensure that browsers connect to your website using HTTPS by default, actively preventing users from accessing it over HTTP. Because this list is hardcoded in users' browsers, HSTS will be enabled even before they visit your page for the first time, removing the requirement for Trust on First Use (TOFU) and its dangers and drawbacks. Your website will not meet the conditions required to enter the browser's preload list unless you fix the issues and warnings.

Browser vendors have declared,

- A valid certificate should be served.
- Redirect all domains from HTTP to HTTPS on the same host if you're listening on port 80. All subdomains should be served over HTTPS: If a DNS record for the www subdomain exists, you must support HTTPS for that subdomain.
- For HTTPS requests, add a HSTS header to the base domain:
- The maximum age must be 31536000 seconds (1 year)
- The directive include Sub Domains must be provided.
- It is necessary to specify the preload directive.
- If you're delivering an additional redirect from your HTTPS site, that redirect (rather than the page it redirects to) must carry the HSTS header.

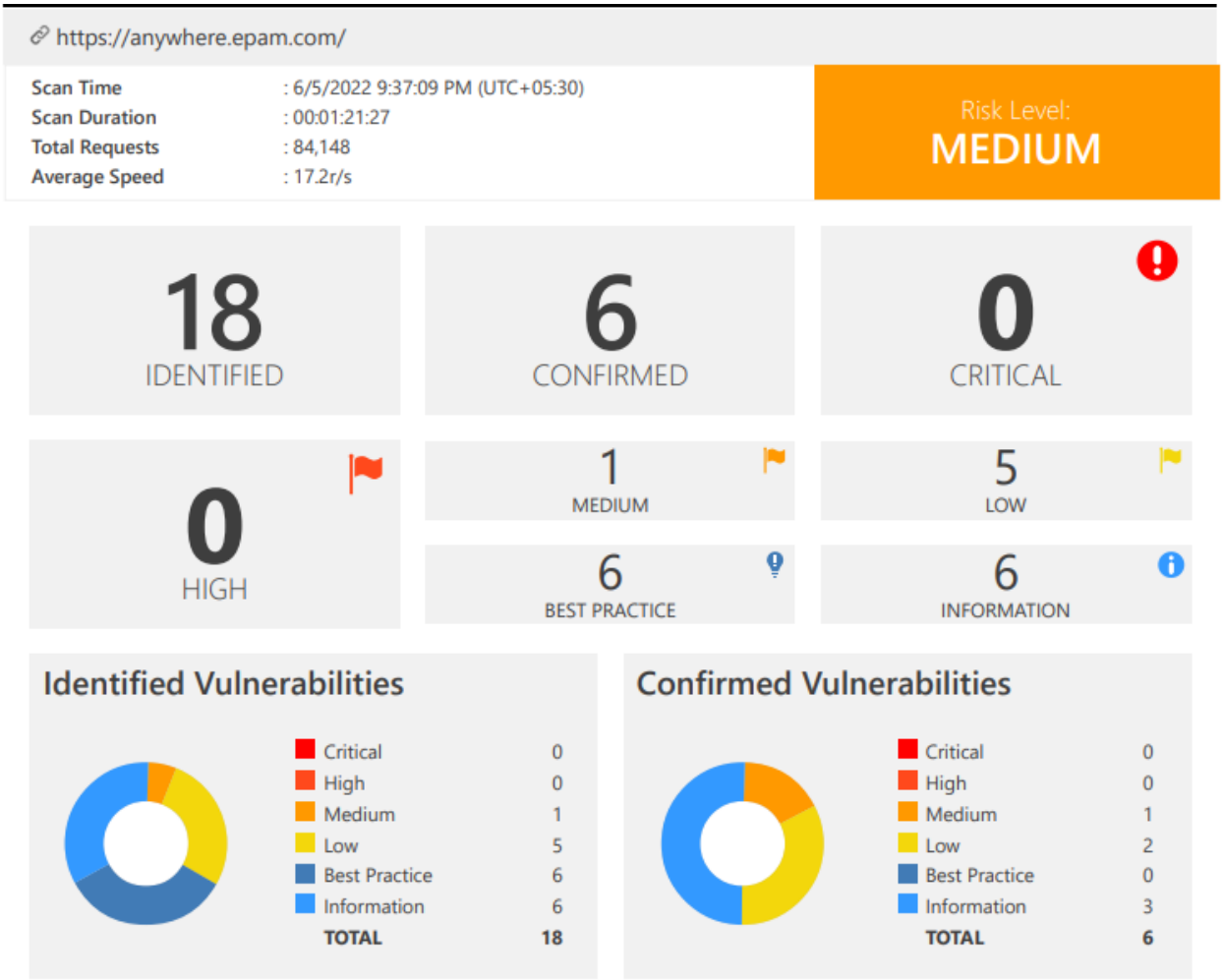
External References:

- HTTP Strict Transport Security (HSTS) HTTP Header
- Wikipedia - HTTP Strict Transport Security Implementation
- Check HSTS Preload status and eligibility

Classification

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

3. Targeted Domain: anywhere.epam.com

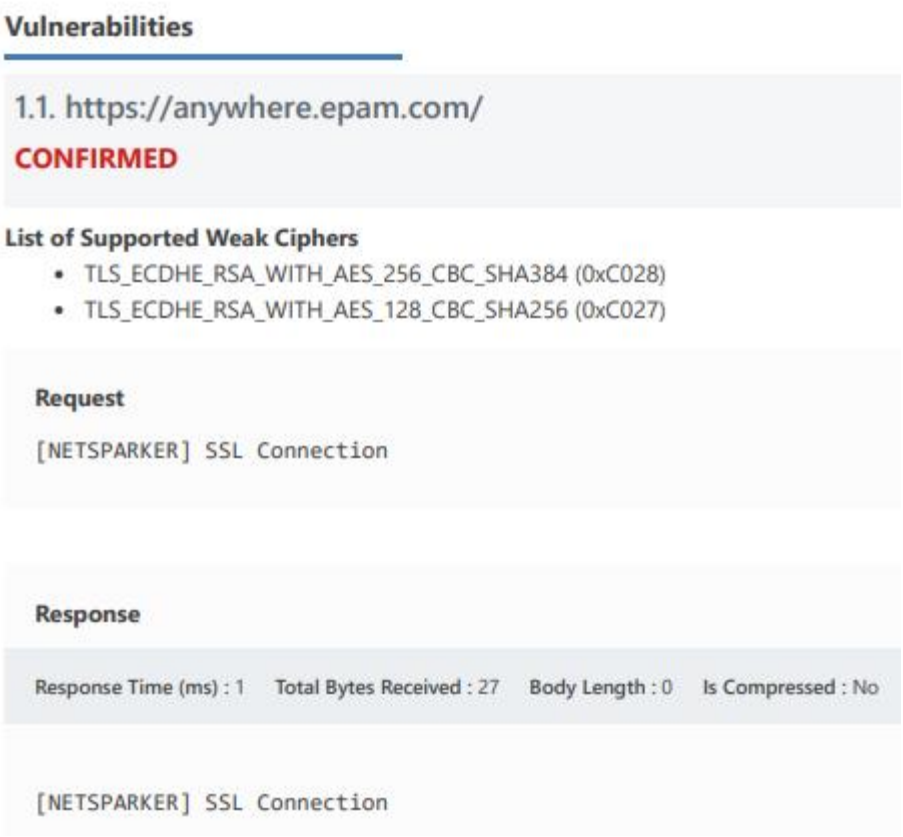


A. <u>Weak Cipher Enabled</u>

Severity : Medium
Method : GET
OWASP : No 02 type

Impact

Attackers may able to decrypt the SSL traffic between the server and your visitors.



Actions to take:

- In Apache, modify the SSLCipherSuite directive in the httpd.conf

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

- In Lighttpd

```
ssl.honor-cipher-order = "enable"
```

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

- For Microsoft ISS, should edit the registry as follows.

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

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

Remedy

Configure your web server to avoid 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

Classification

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

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

B. Internal IP Address Disclosure

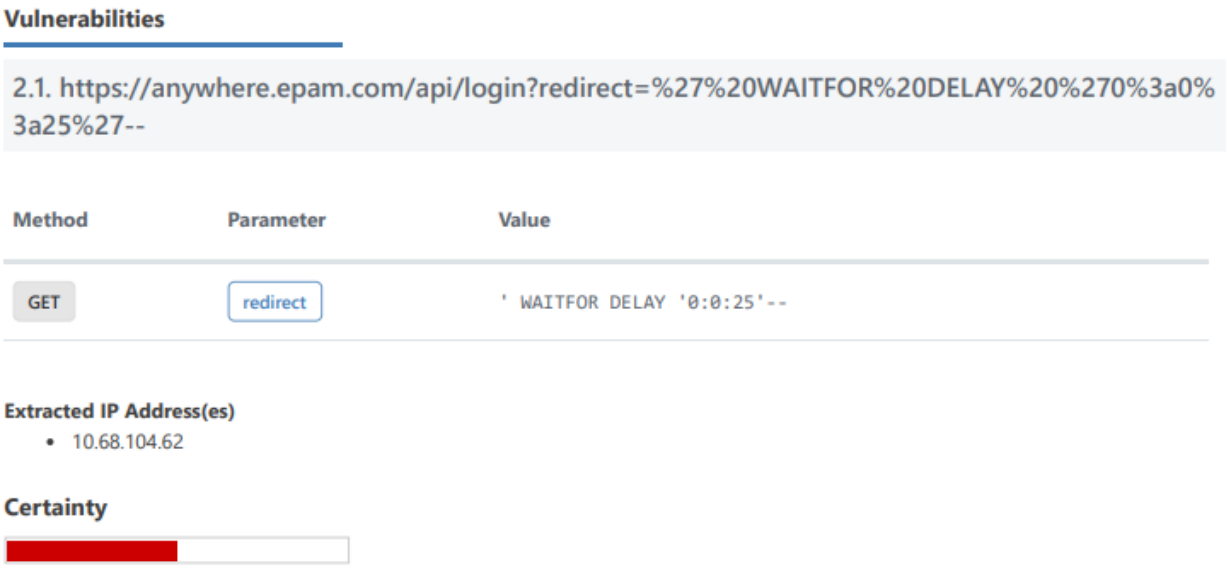
Severity : Low

Method : GET

OWASP : Type 03

Impact

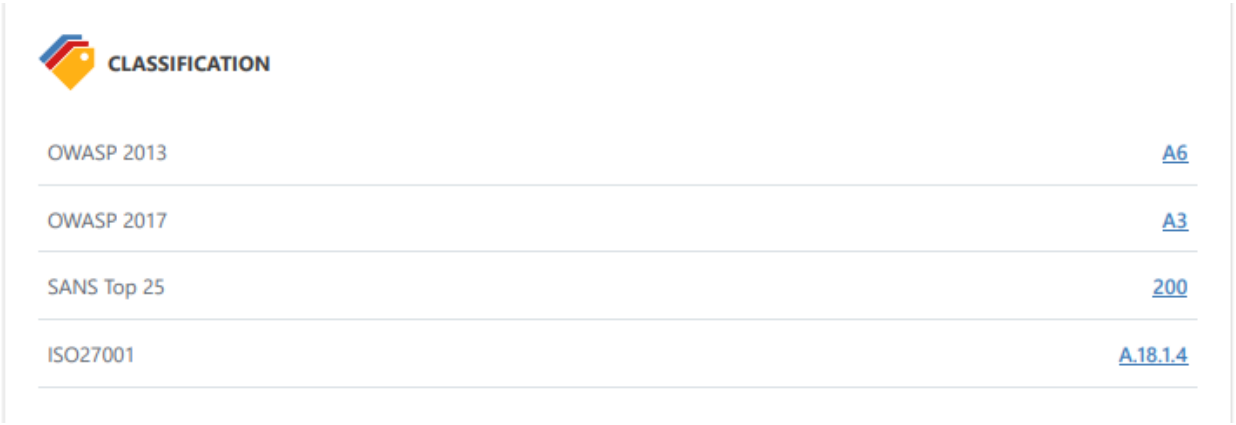
There is no immediate impact; nonetheless, this information can assist an attacker in identifying new vulnerabilities or exploitation of other vulnerabilities that have been identified.



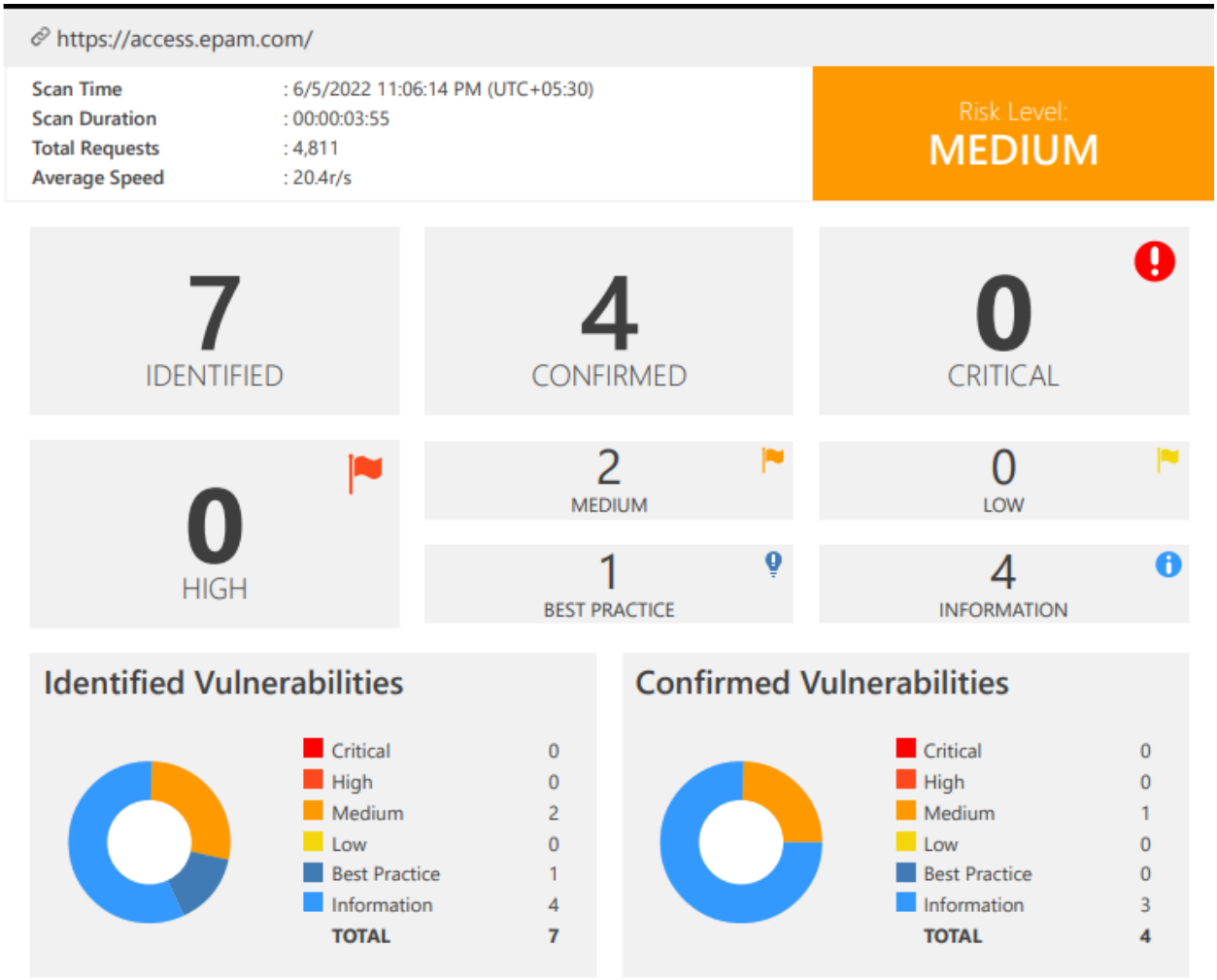
Remedy

To begin, double-check that this isn't a false positive. Netsparker was unable to establish that this IP address was the real internal IP address of the target web server or internal network due to the nature of the problem. If that's the case, consider removing it.

Classification



4. Targeted Domain: access.epam.com



A. HTTP Strict Transport Security (HSTS) Errors and Warnings

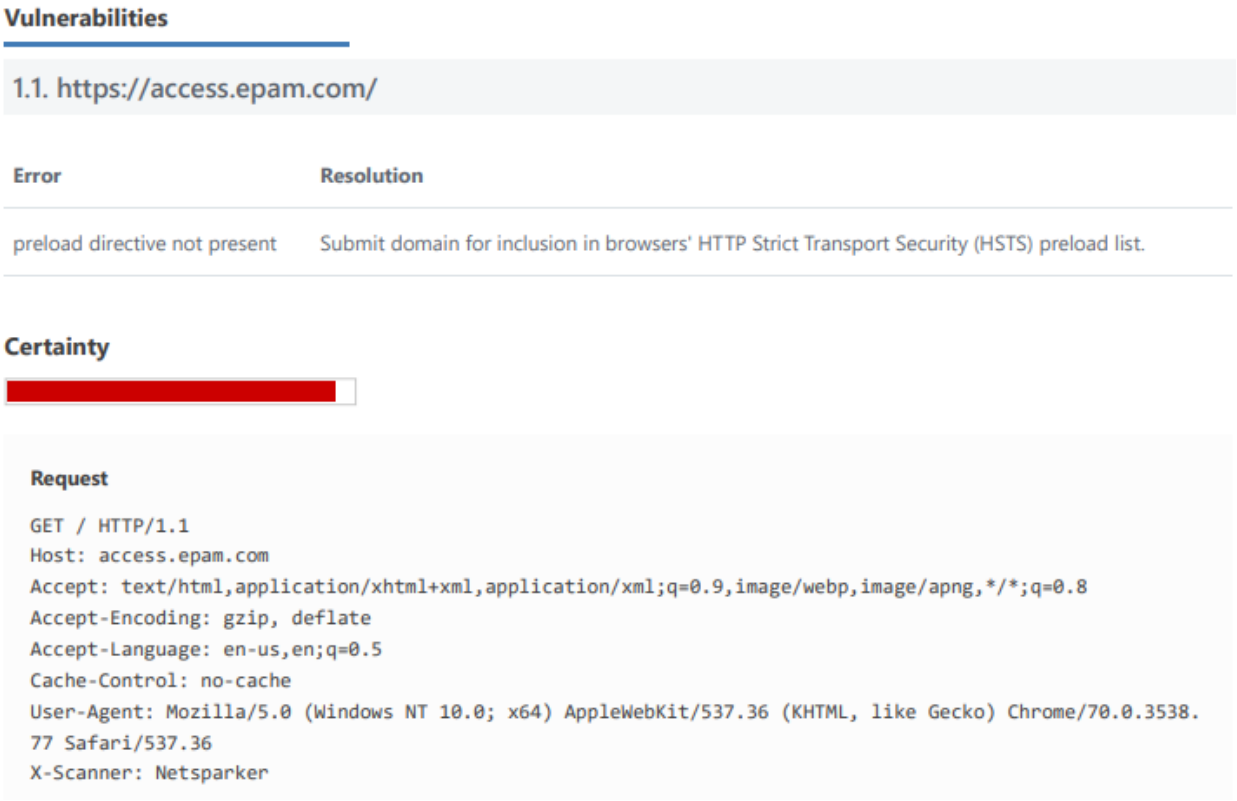
Severity : Medium

Method : GET

OWASP : No 06 type

Impact

The HSTS Warning and Error may allow attackers to circumvent HSTS, allowing them to view and change your website communications.



Vulnerabilities

1.1. https://access.epam.com/

Error	Resolution
preload directive not present	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

Certainty

Request

```
GET / HTTP/1.1
Host: access.epam.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Remedy

After addressed the problems and warnings, you should think about adding your domain to the HSTS preload list. This will ensure that browsers connect to your website using HTTPS by default, actively preventing users from accessing it over HTTP. Because this list is hardcoded in users' browsers, HSTS will be enabled even before they visit your page for the first time, removing the requirement for Trust on First Use (TOFU) and its dangers and drawbacks. Your website will not meet the conditions required to enter the browser's preload list unless you fix the issues and warnings.

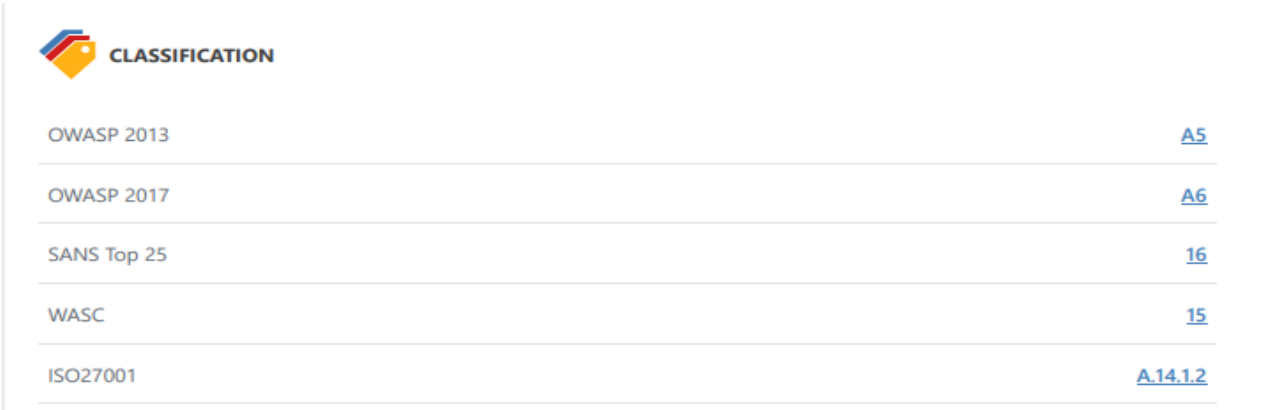
Browser vendors have declared,

- A valid certificate should be served.
- Redirect all domains from HTTP to HTTPS on the same host if you're listening on port 80. All subdomains should be served over HTTPS:
    - If a DNS record for the www subdomain exists, you must support HTTPS for that subdomain.
- For HTTPS requests, add a HSTS header to the base domain:
    - The maximum age must be 31536000 seconds (1 year)
    - The directive include Sub Domains must be provided.
    - It is necessary to specify the preload directive.
    - If you're delivering an additional redirect from your HTTPS site, that redirect (rather than the page it redirects to) must carry the HSTS header.

External References:

- HTTP Strict Transport Security (HSTS) HTTP Header
- Wikipedia - HTTP Strict Transport Security Implementation
- Check HSTS Preload status and eligibility

Classification

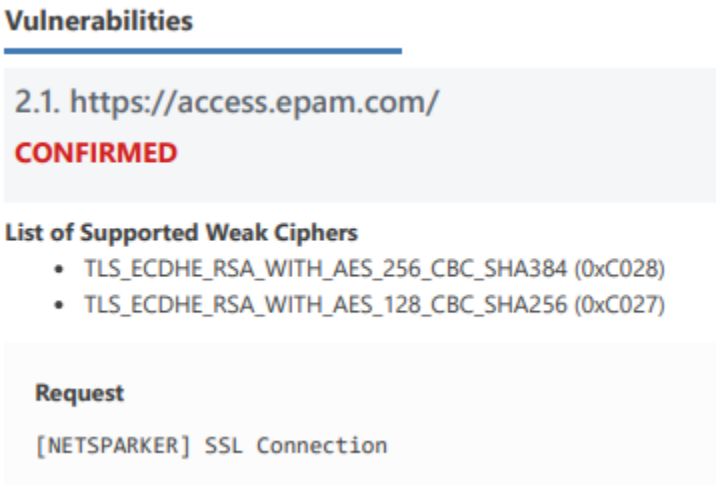


B. Weak Ciphers Enabled

Severity : Medium
Method : GET
OWASP : No 02 type

Impact

Attackers may able to decrypt the SSL traffic between the server and your visitors.



Actions to take:

- In Apache, modify the SSLCipherSuite directive in the httpd.conf

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

- In Lighttpd

```
ssl.honor-cipher-order = "enable"
```

[redacted]

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

- For Microsoft ISS, should edit the registry as follows.

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

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

Remedy

Configure your web server to avoid 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

Classification

CLASSIFICATION

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

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

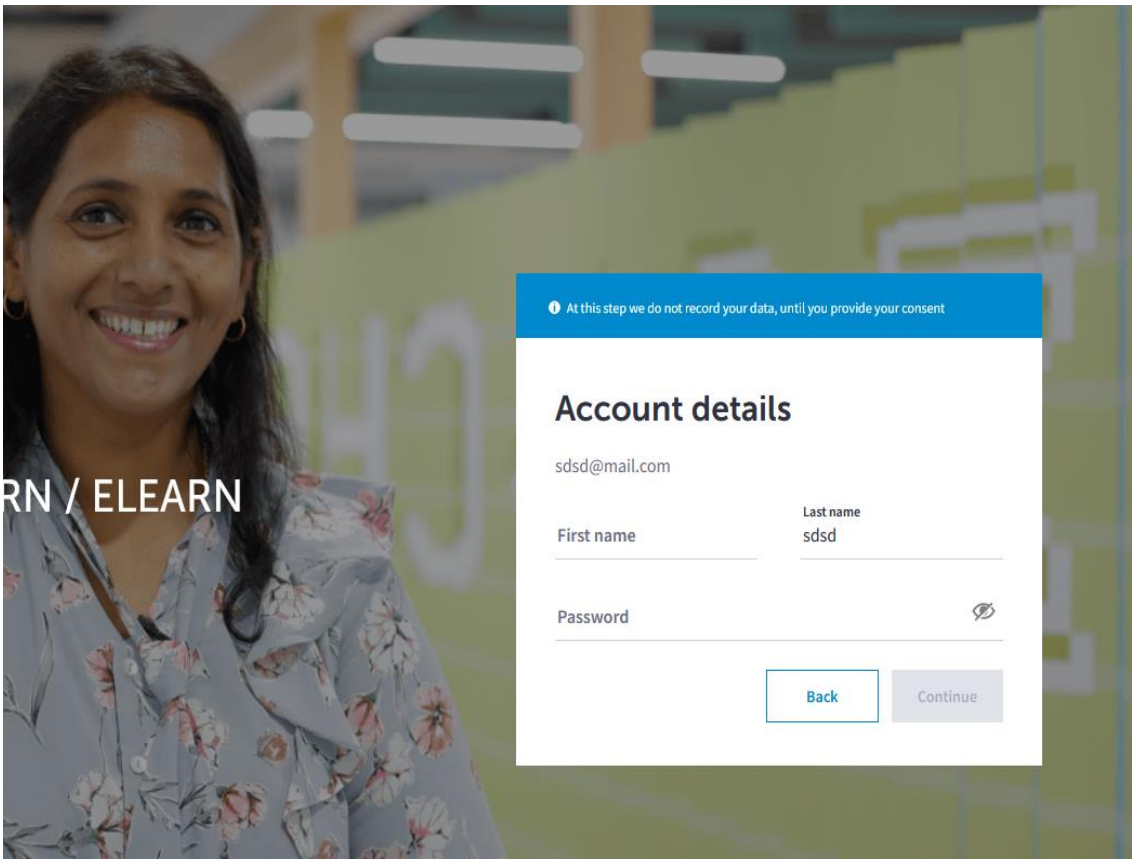
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

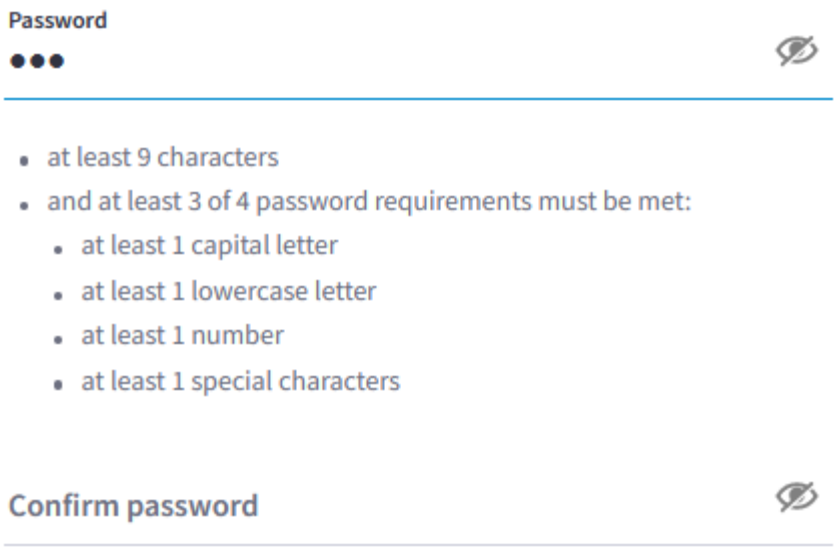
Base	6.8 (Medium)

Manual Testing

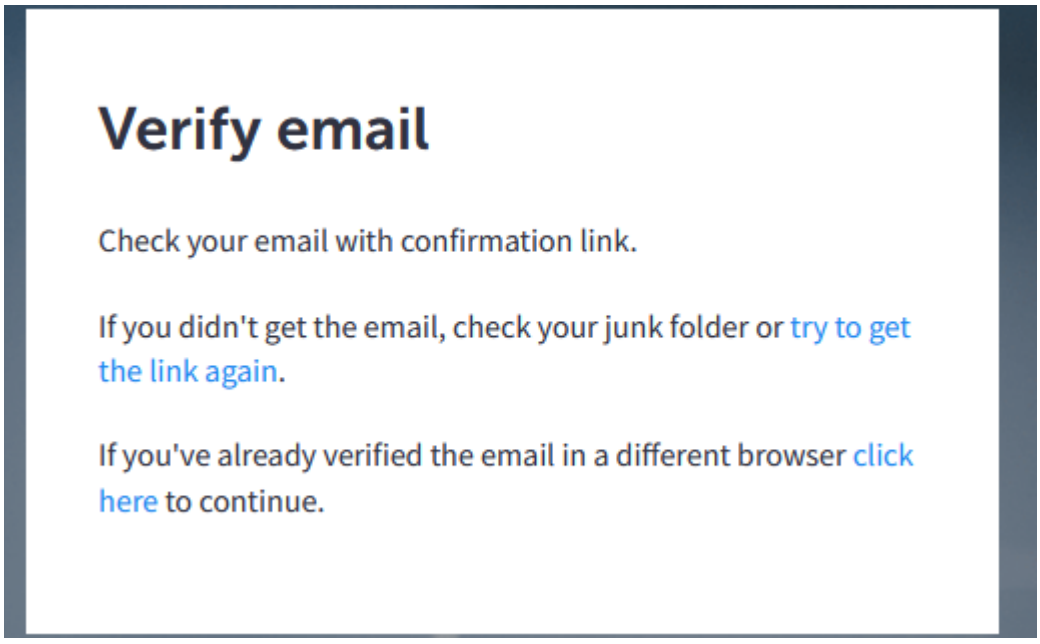
To check the selected domains manually, Initially I have created the user account on https://access.epam.com.



When creating a account as usually the form asks for a password and that password has a policy there and also it does not allow to bypass the policy when creating a password which is a good sign of initial security.



The site has a step to verify the email used to create the account and it is mandatory. The verification can be done only via the link in email. Vice versa site does not allow to go forward without verifying.



When clicking on the link saying to click if we have already verified will not goanna bypass the step before verifying the email and I have tried that.

Cross-site Scripting (XSS)

Cross-site scripting (XSS) is a sort of client-side attack. Attackers insert malicious payloads/scripts into webpages via input fields such as forms, comment sections, and so on, and the malicious script is executed when a genuine user renders the webpage. The legitimate user's cookies, session IDs, and other sensitive information will be sent to the attacker after the script is successfully executed.

XSS attacks can be classified into three categories. Based on the final impact, each of them is unique.

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

I attempted to include the basic script into the website, but no actions were reflected. When I do the same thing over and over, the system recognizes me as an invader.

Conclusion

In order to assess the security of web applications, a web audit is required. During this study, several faults were uncovered, which must be corrected as soon as possible. Corrective actions must be prioritized based on the severity of the found faults.

The selected domains contain all of the severity level vulnerabilities after all of the information collecting, scanning, and testing.

- Medium severity Vulnerabilities – 5
- Low severity vulnerabilities – 5
- Other – 19

As a leading world-class platform Epam has done their security assessments so good so far. Although, they should take care of these above flaws in their system and address them in order to being protected and protect their clients from attackers.