CMR
GROUP OF INSTITUTIONS
EXPLORE TO INVENT

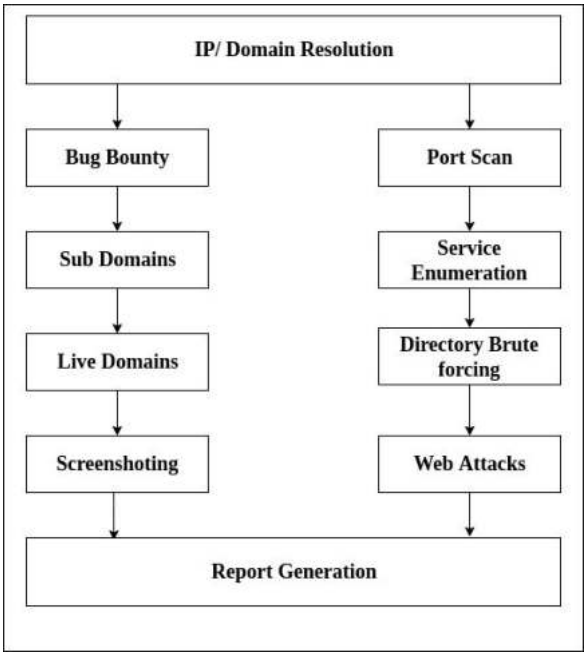
CMR
GROUP OF INSTITUTIONS
EXPLORE TO INVENT

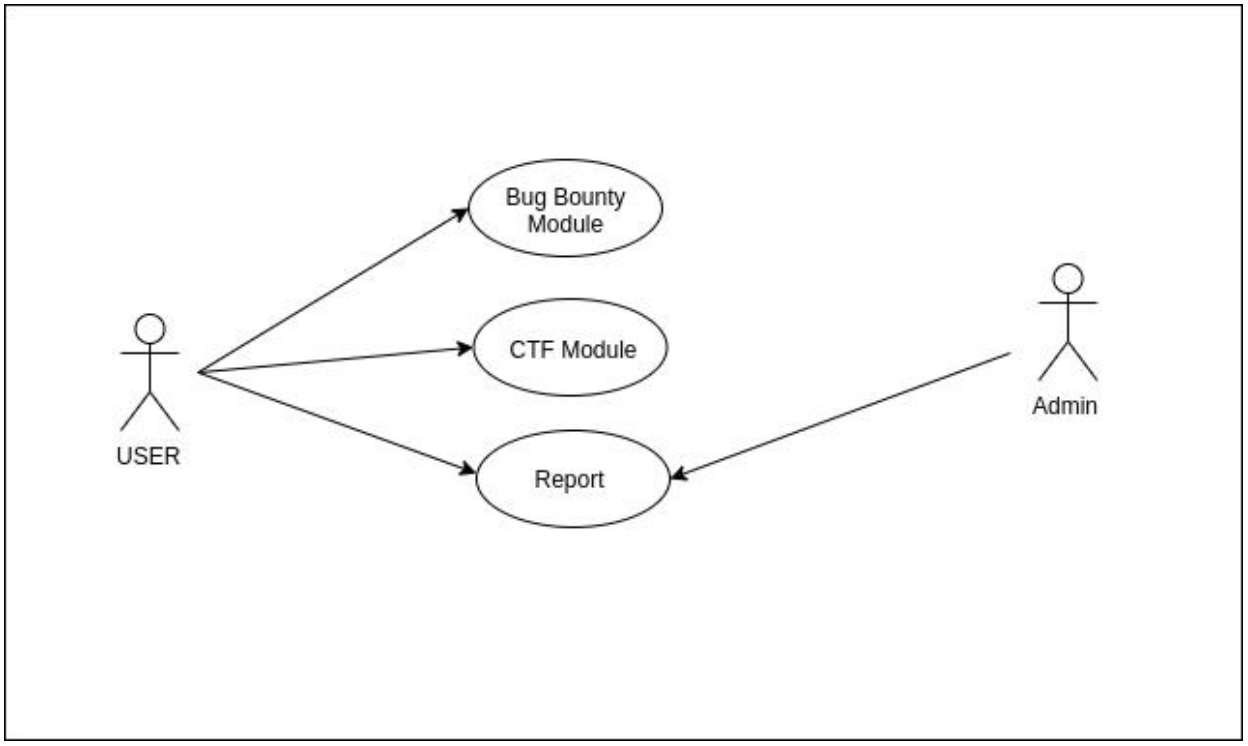
-
-
-
-
-

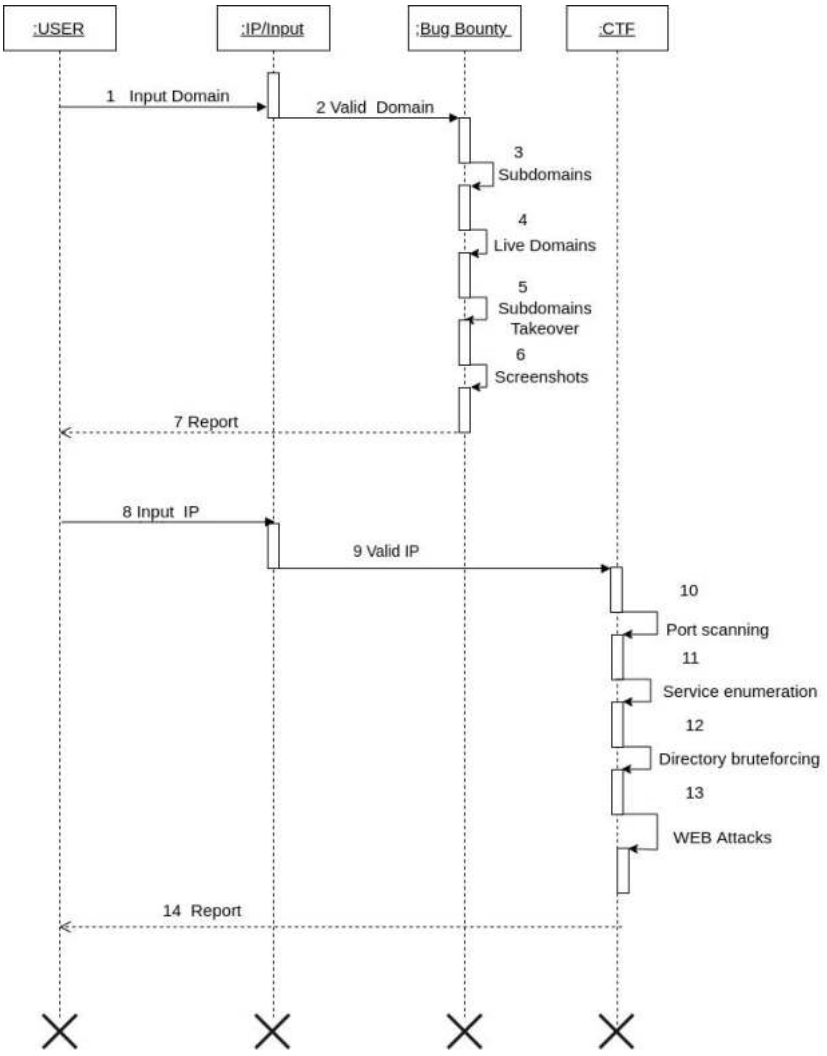
-
-
-
-

-
-
-
-

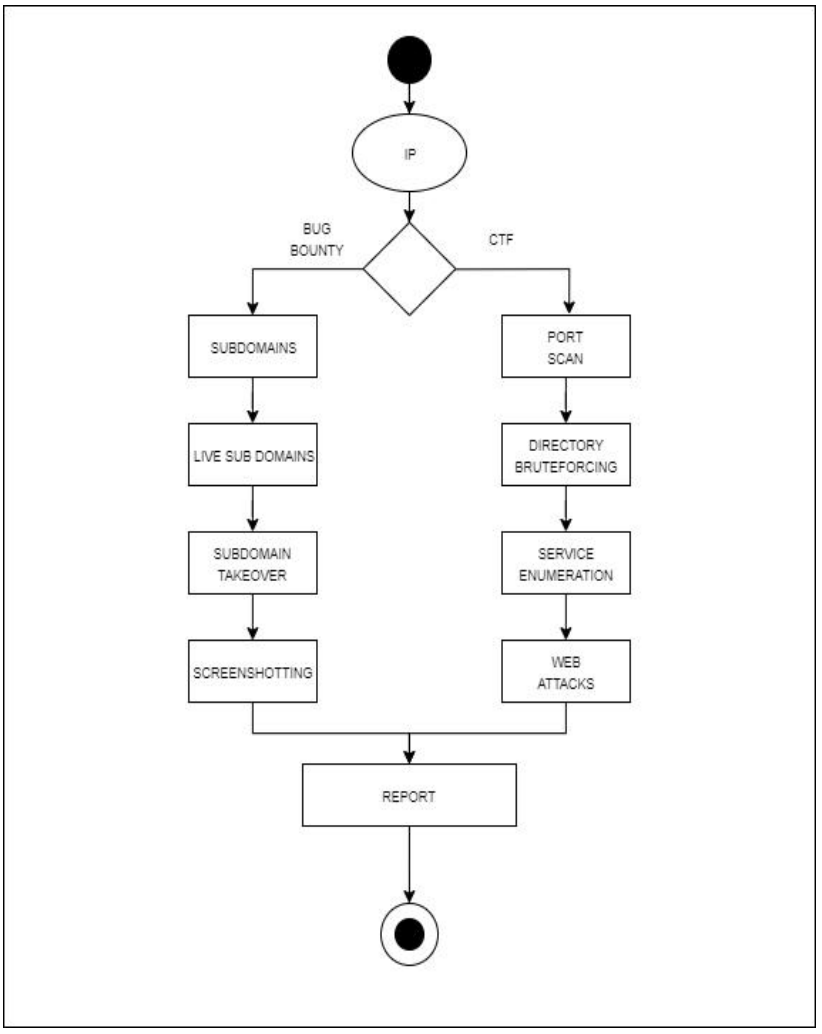
-
-
-


IP/ Domain Resolution
Bug Bounty
Port Scan
Sub Domains
Service Enumeration
Live Domains
Directory Brute forcing
Screenshoting
Web Attacks
Report Generation


Bug Bounty Module
CTF Module
Report
USER
Admin


:USER
:IP/Input
:Bug Bounty
:CTF
1 Input Domain
2 Valid Domain
3
Subdomains
4
Live Domains
5
Subdomains
Takeover
6
Screenshots
7 Report
8 Input IP
9 Valid IP
10
Port scanning
11
Service enumeration
12
Directory bruteforcing
13
WEB Attacks
14 Report

.


IP
BUG
BOUNTY
CTF
SUBDOMAINS
LIVE SUB DOMAINS
SUBDOMAIN
TAKEOVER
SCREENSHOTTING
PORT
SCAN
DIRECTORY
BRUTEFORCING
SERVICE
ENUMERATION
WEB
ATTACKS
REPORT

/home/agastya/Documents/MajorProject
python3 check_vuln.py -c -t 10.10.11.156
********** Nmap Scan Started**********
**********Nmap Scan Completed**********
**********Ports open**********
Ports
22
80
**********services and versions**********
services-versions
OpenSSH 7.6p1
nginx 1.14.0
seraching exploits for :OpenSSH 7.6p1
searchsploit OpenSSH 7.6p1
seraching exploits for :nginx 1.14.0
searchsploit nginx 1.14.0
**********Possible exploits**********
Exploit Title
Path
OpenSSH 2.3 < 7.7 - Username Enumeration
linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)
linux/remote/45210.py
OpenSSH < 7.7 - User Enumeration (2)
linux/remote/45939.py
Shellcodes: No Results
Exploits: No Results
Shellcodes: No Results

Scan date: 24-5-2022 11:43:25
| Domain: http://10.10.11.156/
| Server: nginx/1.14.0 (Ubuntu)
| IP: 10.10.11.156
| Crawler Started:
| Plugin name: E-mail Detection v.1.1 Loaded.
| Plugin name: FCKeditor upload test v.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| Plugin name: phpinfo() Disclosure v.1 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: Upload Form Detect v.1.1 Loaded.
| Plugin name: Timthumb ⩽ 1.32 vulnerability v.1 Loaded.
| [+] Crawling finished, 8 URL's found!
| E-mails:
| [+] E-mail Found: support@late.htb
| FCKeditor File Upload:
| Web Backdoors:
| PHPinfo() Disclosure:
| Source Code Disclosure:
| External hosts:
| [+] External Host Found: http://fonts.googleapis.com
| [+] External Host Found: http://images.late.htb
| [+] External Host Found: http://ajax.googleapis.com
| [+] External Host Found: http://netdna.bootstrapcdn.com

Scan report

Scan Date : May 24, 2022 Time : 11:35:46

General Info

Total Domains enumrated : 1212
Non Duplicate Domains enumrated : 519
Live Domains enumrated : 429

Domain : tesla.com

Live Domains are listed below

https://akamai-apigateway-deliveryopsapi.tesla.com
http://akamai-apigateway-deliveryopsapi.tesla.com
https://3.tesla.com
http://3.tesla.com
http://akamai-apigateway-dev-warptmsapiserver.tesla.com
http://akamai-apigateway-deliveryopsapi1.tesla.com
http://akamai-apigateway-captiveunderwriting.tesla.com
http://akamai-apigateway-automation-billing.tesla.com
http://akamai-apigateway-einvoicing.tesla.com
http://akamai-apigateway-automation.tesla.com
http://akamai-apigateway-bender.tesla.com
http://akamai-apigateway-finplateng-routeone.tesla.com
http://akamai-apigateway-finplateng.tesla.com
https://akamai-apigateway-inventorytxnextapi.tesla.com
http://akamai-apigateway-inventorytxnextapi.tesla.com
http://akamai-apigateway-finplat-prd.tesla.com
http://akamai-apigateway-logisticsratesapi.tesla.com
http://akamai-apigateway-mfs-supplier-uat.tesla.com
http://akamai-apigateway-fta.tesla.com
http://akamai-apigateway-materials.tesla.com
http://akamai-apigateway-mfs-supplier.tesla.com