CSE370 CA4 CYBER SECURITY

PEN-TESTING A WEBSITE

Team Members:
Swaran S E0119015
Santosh Prasad D E0119050
Sakthi Murugan K E0119028

NEXT

INTRODUCTION ABOUT WEBSITE AND PEN-TESTING

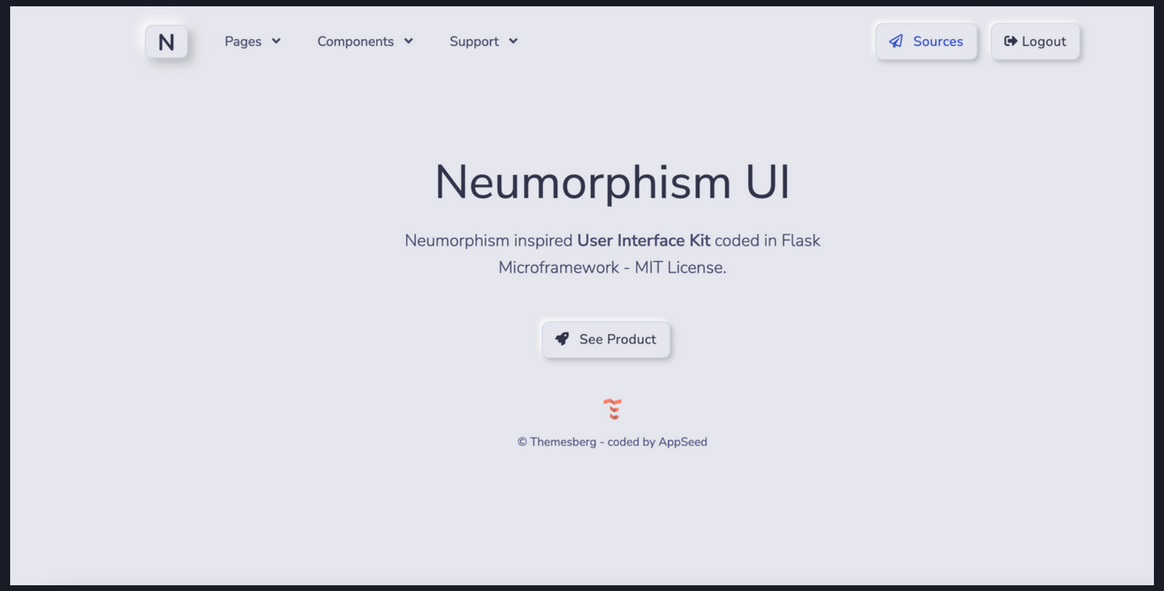
About the website

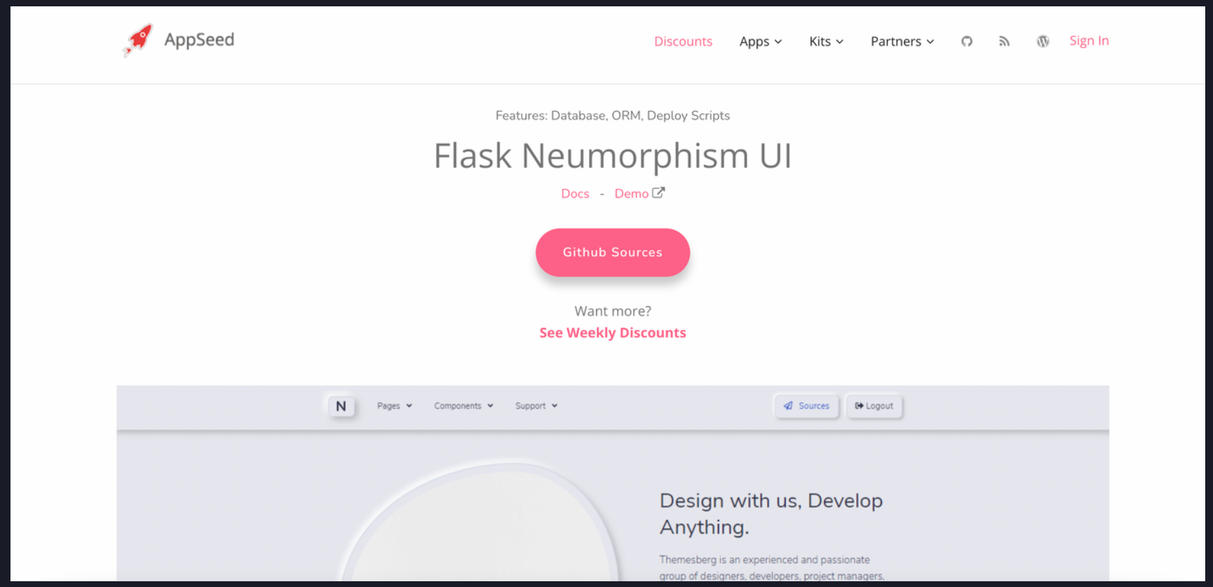
Appseed is a website that advertises a product called Flask Neumorphism U.
The product is used to develop websites using its UI based tools,

Pen-Test

Penetration testing, also known as pen testing, security pen testing, and security testing, is a form of ethical hacking. The pen test attempts to pierce the armour of an organisation's cyber defences, checking for exploitable vulnerabilities in networks, web apps, and user security.

Website Overview





List of Tools Used

INFORMATION GATHERING

Netcraft
Nmap
Whois, FTP

VULNERABILITY SCANNING

Nikto
Uniscan

EXPLOITATION TOOLS

UFONet

Information Gathering

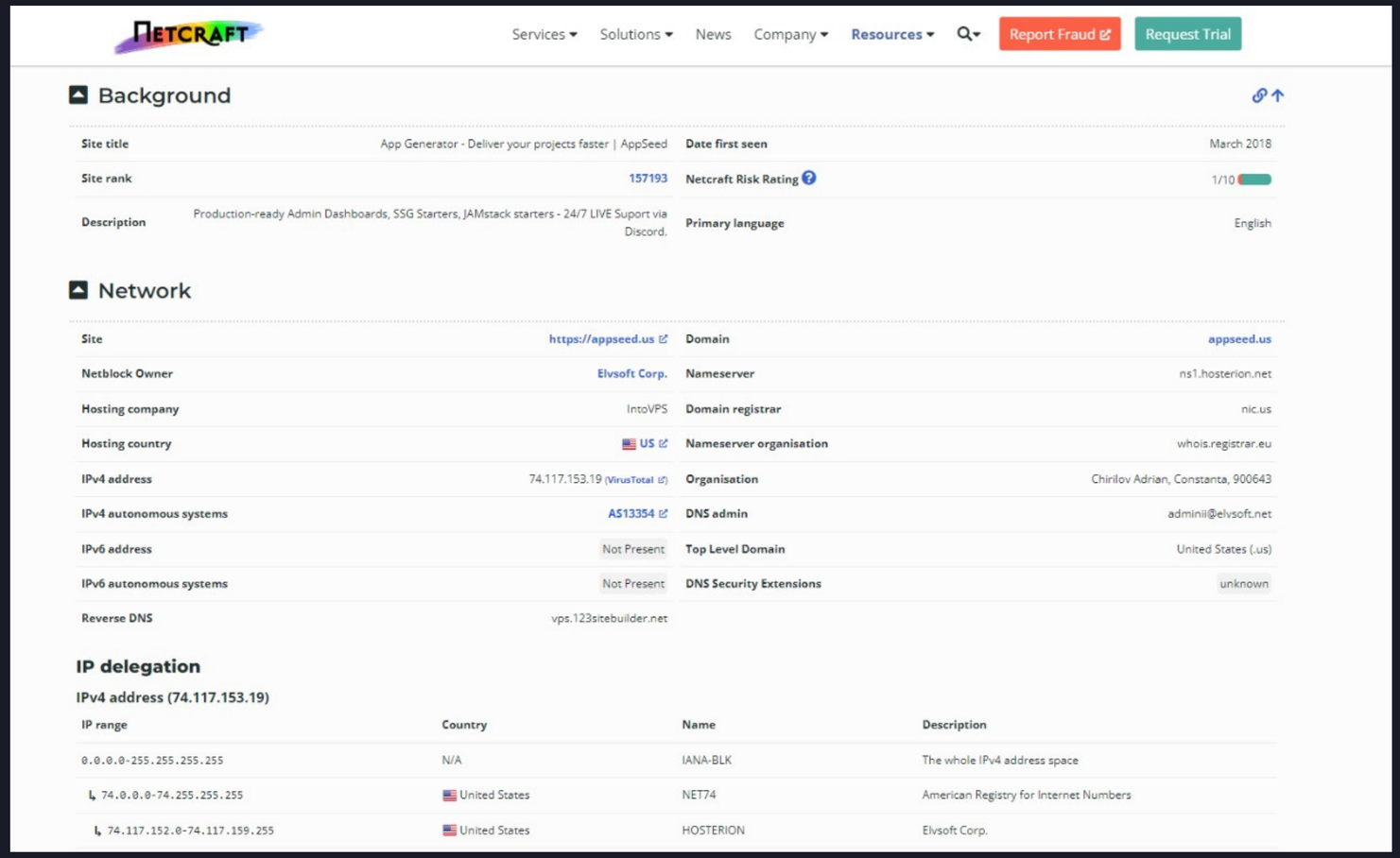
```
└─# nmap -sV 192.168.56.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-24 00:00 EST
Nmap scan report for 192.168.56.1
Host is up (0.0024s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2869/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.85 seconds

┌──(root💀kali)-[/home/kali]
└─#
```

```
┌──(root💀kali)-[/home/kali]
└─# nmap -p 1-200 www.appseed.us
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-24 00:31 EST
Nmap scan report for www.appseed.us (74.117.153.19)
Host is up (0.00069s latency).
All 200 scanned ports on www.appseed.us (74.117.153.19) are in ignored s
Not shown: 200 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 20.17 seconds
```

```
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# nmap www.appseed.us
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-24 00:27 EST
Nmap scan report for www.appseed.us (74.117.153.19)
Host is up (0.019s latency).
rDNS record for 74.117.153.19: vps.123sitebuilder.net
Not shown: 976 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
25/tcp    open   smtp
26/tcp    closed rsftp
53/tcp    open   domain
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
2222/tcp  closed EtherNetIP-1
3306/tcp  open   mysql
8888/tcp  open   sun-answerbook
30000/tcp closed ndmps
30718/tcp closed unknown
32770/tcp closed sometimes-rpc3
32771/tcp closed sometimes-rpc5
32777/tcp closed sometimes-rpc17
32779/tcp closed sometimes-rpc21
32782/tcp closed unknown
32784/tcp closed unknown
32785/tcp closed unknown
33899/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 46.68 seconds
```

NMap

NetCraft



NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Report Fraud Request Trial

Background

Site title	App Generator - Deliver your projects faster | AppSeed	**Date first seen**	March 2018
Site rank	157193	**Netcraft Risk Rating**	1/10
Description	Production-ready Admin Dashboards, SSG Starters, JAMstack starters - 24/7 LIVE Suport via Discord.	**Primary language**	English

Network

Site	https://appseed.us	**Domain**	appseed.us
Netblock Owner	Elvsoft Corp.	**Nameserver**	ns1.hosterion.net
Hosting company	IntoVPS	**Domain registrar**	nic.us
Hosting country	US	**Nameserver organisation**	whois.registrar.eu
IPv4 address	74.117.153.19 (VirusTotal)	**Organisation**	Chirilov Adrian, Constanta, 900643
IPv4 autonomous systems	AS13354	**DNS admin**	adminii@elvsoft.net
IPv6 address	Not Present	**Top Level Domain**	United States (.us)
IPv6 autonomous systems	Not Present	**DNS Security Extensions**	unknown
Reverse DNS	vps.123sitebuilder.net		

IP delegation

IPv4 address (74.117.153.19)

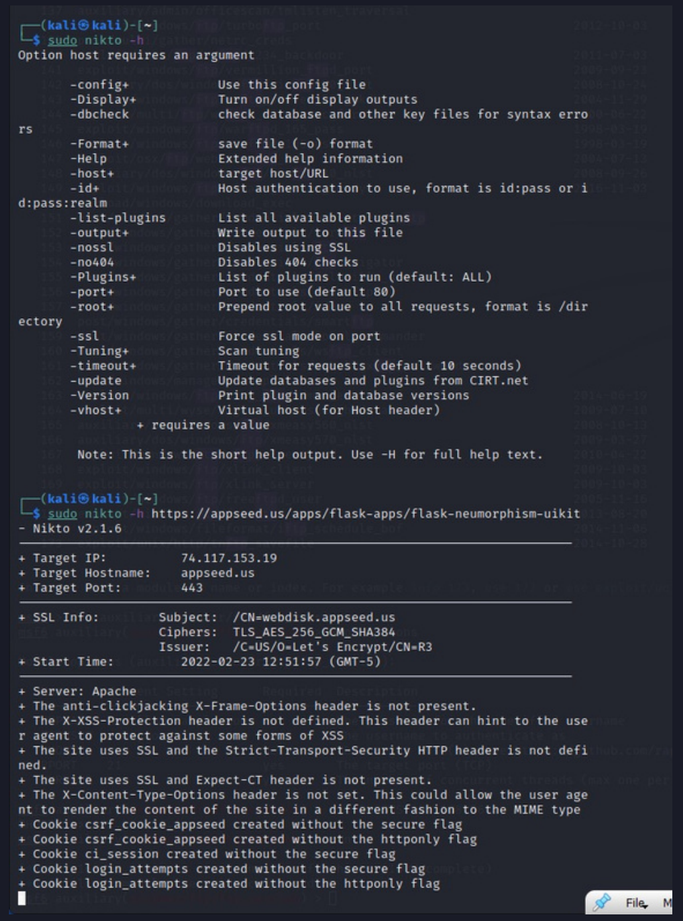
IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 74.0.0.0-74.255.255.255	United States	NET74	American Registry for Internet Numbers
↳ 74.117.152.0-74.117.159.255	United States	HOSTERION	Elvsoft Corp.

Whois & FTP

```
msf6 > whois www.appseed.us
[*] exec: whois www.appseed.us

No Data Found
>>> Last update of WHOIS database: 2022-02-23T17:40:49Z <<<

For more information on Whois status codes, please visit https://icann.org/ep
p

.US WHOIS Complaint Tool - http://www.whoiscomplaints.us
Advanced WHOIS Instructions - http://whois.us/help.html

Registry Services, LLC, the Registry Administrator for .US, has collected thi
s information for the WHOIS database through a .US-Accredited Registrar. This
 information is provided to you for informational purposes only and is design
ed to assist persons in determining contents of a domain name registration re
cord in the registry database.

Registry Services, LLC makes this information available to you "as is" and do
es not guarantee its accuracy. By submitting a WHOIS query, you agree that yo
u will use this data only for lawful purposes and that, under no circumstance
s will you use this data:

(1) to allow, enable, or otherwise support the transmission of mass unsolicit
ed, commercial advertising or solicitations via direct mail, electronic mail,
 or by telephone;
(2) in contravention of any applicable data and privacy protection laws; or
(3) to enable high volume, automated, electronic processes that apply to the
registry (or its systems).

Compilation, repackaging, dissemination, or other use of the WHOIS database i
n its entirety, or of a substantial portion thereof, is not allowed without o
ur prior written permission.

We reserve the right to modify or change these conditions at any time without
 prior or subsequent notification of any kind. By executing this query, in an
y manner whatsoever, you agree to abide by these terms. NOTE: FAILURE TO LOCA
TE A RECORD IN THE WHOIS DATABASE IS NOT INDICATIVE OF THE AVAILABILITY OF A
DOMAIN NAME. All domain names are subject to certain additional domain name r
egistration rules. For details, please visit our site at www.whois.us.
msf6 >
```

```
Interact with a module by name or index. For example info 173, use 173 or use exploit/unix/http/tnftp_savefile

msf6 > use auxiliary/scanner/ftp/ftp_version
msf6 auxiliary(scanner/ftp/ftp_version) > show options

Module options (auxiliary/scanner/ftp/ftp_version):

   Name     Current Setting      Required  Description
   ----     ---------------      --------  -----------
   FTPPASS  mozilla@example.com  no        The password for the specified username
   FTPUSER  anonymous            no        The username to authenticate as
   RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    21                   yes       The target port (TCP)
   THREADS  1                    yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/ftp/ftp_version) > set RHOSTS 192.168.56.1
RHOSTS => 192.168.56.1
msf6 auxiliary(scanner/ftp/ftp_version) > run

[*] 192.168.56.1:21       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_version) >
```

Vulnerability Scaning



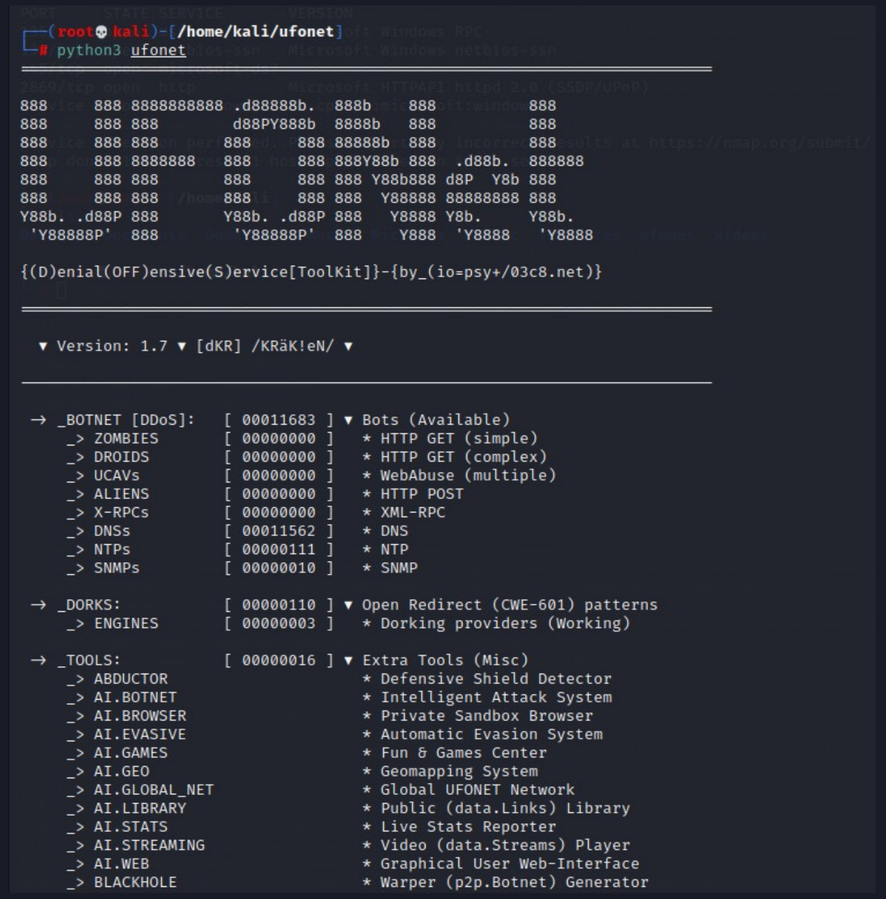
Nikto

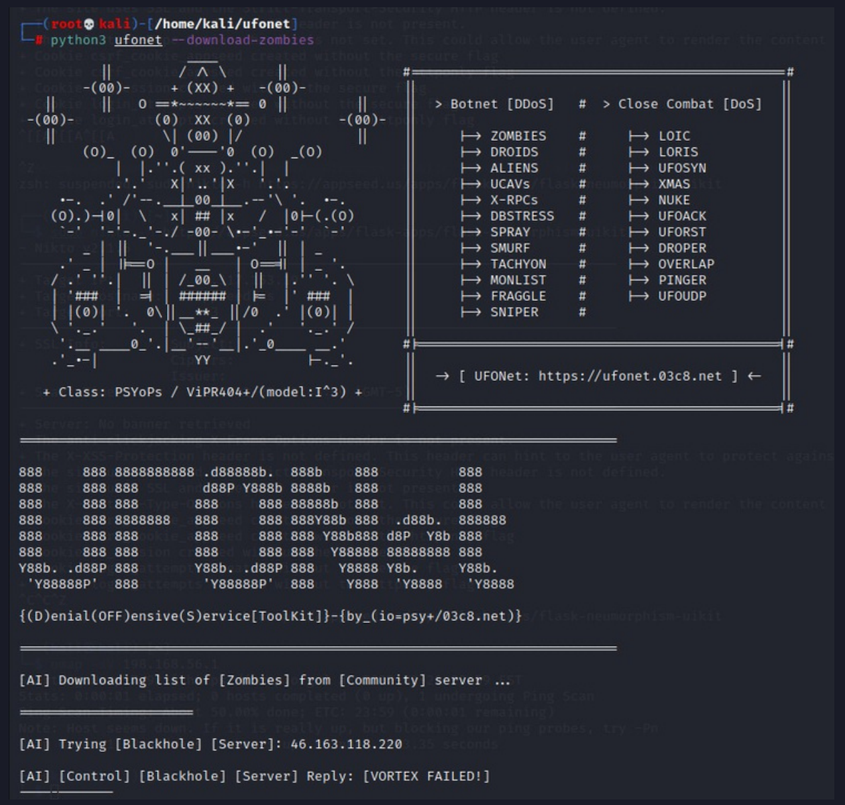
Uniscan

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install uniscan
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
uniscan is already the newest version (6.3-0kali2).
0 upgraded, 0 newly installed, 0 to remove and 810 not upgraded.

┌──(kali㉿kali)-[~]
└─$ sudo uniscan -h
###################################
# Uniscan project                 #
# http://uniscan.sourceforge.net/ #
###################################
V. 6.3


OPTIONS:
        -h      help
        -u      <url> example: https://www.example.com/
        -f      <file> list of url's
```

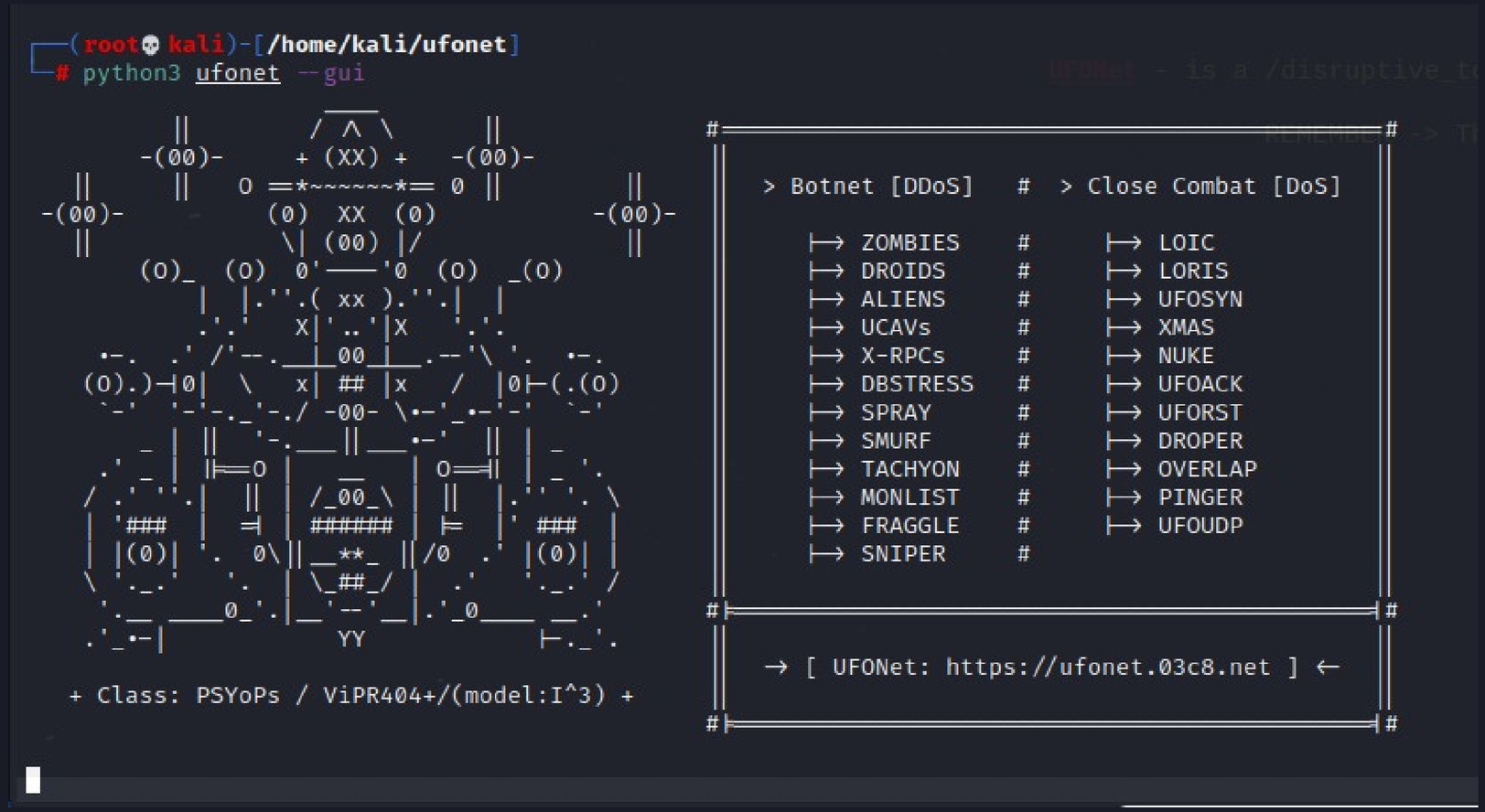
```
┌──(kali㉿kali)-[~]
└─$ sudo uniscan -u https://appseed.us/apps/flask-apps/flask-neumorphism-uik
it
###################################
# Uniscan project                 #
# http://uniscan.sourceforge.net/ #
###################################
V. 6.3


Scan date: 23-2-2022 13:14:5
═══════════════════════════════════════════════════════════════════════════
═══════════════════════════
| Domain: https://appseed.us/apps/flask-apps/flask-neumorphism-uikit/
| Server: Apache
| IP: 74.117.153.19
═══════════════════════════════════════════════════════════════════════════
═══════════════════════════
═══════════════════════════════════════════════════════════════════════════
═══════════════════════════
Scan end date: 23-2-2022 13:14:12
```

Exploitation Tools





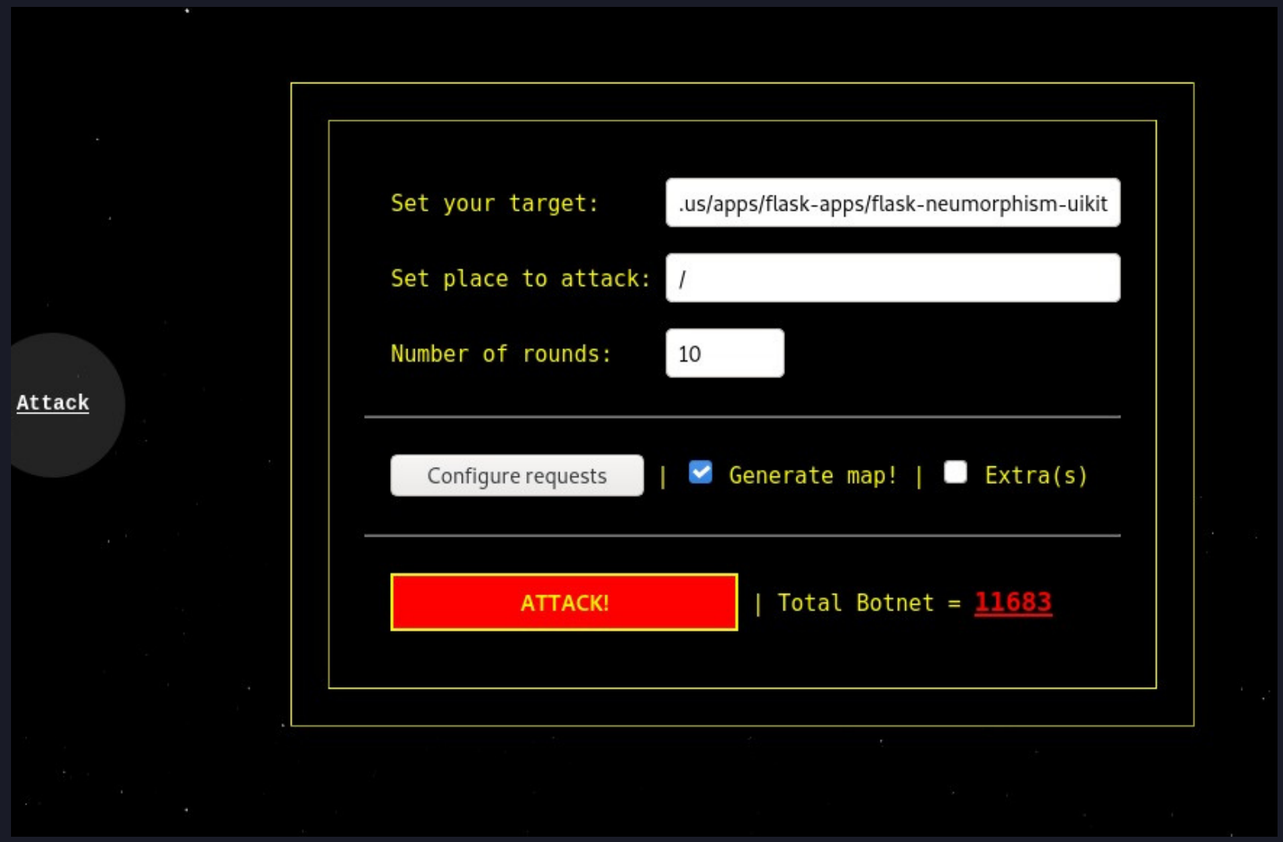
UFOnet


(root kali)-[/home/kali/ufonet]
python3 ufonet --gui
+ Class: PSYoPs / ViPR404+/(model:I^3) +
> Botnet [DDoS]
├→ ZOMBIES
├→ DROIDS
├→ ALIENS
├→ UCAVs
├→ X-RPCs
├→ DBSTRESS
├→ SPRAY
├→ SMURF
├→ TACHYON
├→ MONLIST
├→ FRAGGLE
├→ SNIPER
> Close Combat [DoS]
├→ LOIC
├→ LORIS
├→ UFOSYN
├→ XMAS
├→ NUKE
├→ UFOACK
├→ UFORST
├→ DROPER
├→ OVERLAP
├→ PINGER
├→ UFOUDP
→ [UFONet: https://ufonet.03c8.net] ←

UFOnet GUI

DDos Attack


'oderint dum metuant'
'ad susceptum perficiendum'
'chao ab ordo'
'obscuris vera involvens'
'omnia mutantur, nihil interit'
'orbis unum'
'si vis pacem, para bellum'
'homo homini lupus'
'causa de timendi est nescire'
'adhuc tempus'
'iniqua nunquam regna perpetuo manent'
'ab uno disce omnes'
'unus pro omnibus, omnes pro uno'
'age quod agis'
'fac et excusa'
'divide et impera'
'si fecisti nega'
'necessitas caret lege'
'fiat iustitia, et pereat mundus'
UFONet - is a /disruptive_toolkit/ that allows to perform DDoS and DoS attacks ...
REMEMBER -> This code is NOT for
START MOTHERSHIP!

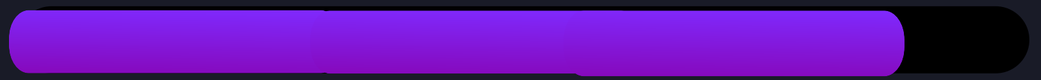

Attack
Set your target:
.us/apps/flask-apps/flask-neumorphism-uikit
Set place to attack:
/
Number of rounds:
10
Configure requests
| Generate map! | Extra(s)
ATTACK!
| Total Botnet = 11683

Security Patches for Update

- A security patch is a set of changes that quickly resolves a bug or security vulnerability.
- By using Nikto and Uniscan, we haven't found any vulnerabilities in the website.

Overall Security Score

The website has fewer/zero vulnerabilities and hence the overall security score for this application is 9.



9/10

Conclusion

Information gathering using different tools, vulnerability scanning, Exploits such as DDoS attacks have been implemented to update the security of the application. By performing the Pen-test vulnerabilities that are exploitable by an attacker were identifiable to ensure the security of the application .

Thank you!