



PEN-TESTING A WEBSITE

Team Members:

Swaran S E0119015

Santosh Prasad D E0119050

Sakthi Murugan K E0119028

INTRODUCTION ABOUT WEBSITE AND PEN-TESTING

-
-
- :

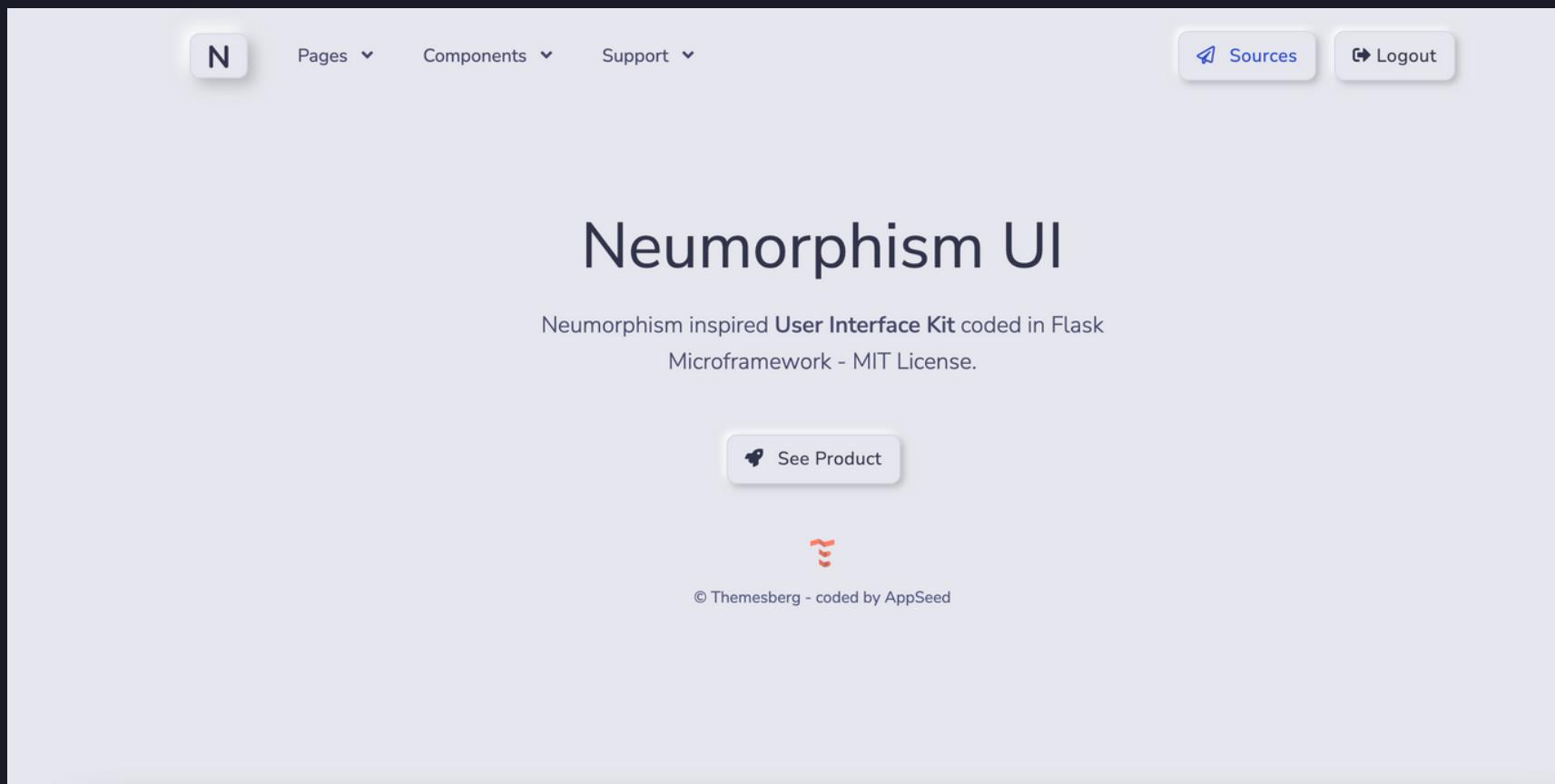
About the website

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



This screenshot displays a light-colored web page with a header featuring the 'AppSeed' logo and navigation links for 'Discounts', 'Apps ▾', 'Kits ▾', 'Partners ▾', and 'Sign In'. The main heading 'Flask Neumorphism UI' is centered above a 'Docs' and 'Demo' link. A prominent pink button labeled 'Github Sources' is visible. To the right, a call-to-action section includes 'Want more?' and 'See Weekly Discounts'. The bottom portion of the page contains a large circular placeholder image and the text 'Design with us, Develop Anything.' along with a note about Themesberg's team.

List of Tools Used

INFORMATION
GATHERING

VULNERABILITY
SCANNING

EXPLOITATION TOOLS

Netcraft
Nmap
Whois, FTP

Nikto
Uniscan

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]
# zsh: suspended sudo nikto -h https://appseed.us/apps/Flask-apps/Flask-neumorphism-UIKit
# (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 state
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]# 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; CPE: cpe:/o:microsoft:windows  
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 Support via Discord. | Primary language | English |

Network

| Site | Domain |
|-------------------------|----------------------------|
| https://appseed.us | appseed.us |
| Netblock Owner | Elvsoft Corp. |
| Hosting company | IntovPS |
| Hosting country | US |
| IPv4 address | 74.117.153.19 (VirusTotal) |
| IPv4 autonomous systems | AS13354 |
| IPv6 address | Not Present |
| IPv6 autonomous systems | Not Present |
| 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/tntfp_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 Scanning

```
(kali㉿kali)-[~] ~$ sudo nikto -h
Option host requires an argument
  -backdoor          Backdoor module
  -config+           Use this config file
  -Display+          Turn on/off display outputs
  -dbcheck            check database and other key files for syntax errors
  -host+             target host/URL
  -id+               Host authentication to use, format is id:pass or id:realm
  -list-plugins      List all available plugins
  -output+           Write output to this file
  -nssl              Disables using SSL
  -no404             Disables 404 checks
  -Plugins+          List of plugins to run (default: ALL)
  -port+             Port to use (default 80)
  -root+             Prepend root value to all requests, format is /dir
  -ssl               Force ssl mode on port
  -Tuning+           Scan tuning
  -timeout+          Timeout for requests (default 10 seconds)
  -update             Update databases and plugins from CIRT.net
  -Version            Print plugin and database versions
  -vhost+            Virtual host (for Host header)
  + requires a value
Note: This is the short help output. Use -H for full help text.

(kali㉿kali)-[~] ~$ sudo nikto -h https://appseed.us/apps/flask-apps/flask-neumorphism-ukit
- Nikto v2.1.6

+ Target IP:        74.117.153.19
+ Target Hostname:  appseed.us
+ Target Port:      443
+ SSL Info:         Subject: /CN=webdisk.appseed.us
                     Ciphers: TLS_AES_256_GCM_SHA384
                     Issuer: /C=US/O=Let's Encrypt/CN=R3
+ Start Time:       2022-02-23 12:51:57 (GMT-5)

+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and the Content-Security-Policy header is not defined. This is a good thing.
+ The site uses SSL and the Expect-CT header is not present. concurrent threads (max one per connection).
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie csrf_cookie_appseed created without the secure flag
+ Cookie csrf_cookie_appseed created without the httponly flag
+ Cookie ci_session created without the secure flag
+ Cookie login_attempts created without the secure flag
+ Cookie login_attempts created without the httponly flag
+ Cookie login_attempts created without the httponly flag
```

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-uikit
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

ATTACKER'S SECURITY
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
=====

Penetration Testing Distribution
=====
Scan end date: 23-2-2022 13:14:12
```

Exploitation Tools

```
[root@kali) [/home/kali/ufonet]# python3 ufonet
2869/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
888 888 888888888 .d88888b. 888b 888t:window888
888 888 888 d8PY888b 8888b 888 888
888 888 888 888 888 88888b 888 incorrec888
888 888 888888888888 888 888 888Y88b888 .d88b. 8888888
888 888 888 888 888 888 Y88b888 d8P Y8b 888
888 888 888 888 888 888 Y88888 888888888 888
Y88b. .d88P 888 Y88b. .d88P 888 Y8888 Y8b. Y88b.
'Y88888P' 888 'Y88888P' 888 Y888 'Y8888 'Y8888
{(D)eNial(OFF)ensive(S)ervice[ToolKit]}-{by_(io=psy+/03c8.net)}

▼ Version: 1.7 ▼ [dKR] /KRäK!eN/ ▼

→ _BOTNET [DDoS]: [ 00011683 ] ▼ Bots (Available)
  _> ZOMBIES [ 00000000 ] * HTTP GET (simple)
  _> DROIDS [ 00000000 ] * HTTP GET (complex)
  _> UCAVs [ 00000000 ] * WebAbuse (multiple)
  _> ALIENS [ 00000000 ] * HTTP POST
  _> X-RPCs [ 00000000 ] * XML-RPC
  _> DNSs [ 00011562 ] * DNS
  _> NTPs [ 00000111 ] * NTP
  _> SNMPs [ 00000010 ] * SNMP

→ _DORKS: [ 00000110 ] ▼ Open Redirect (CWE-601) patterns
  _> ENGINES [ 00000003 ] * Dorking providers (Working)

→ _TOOLS: [ 00000016 ] ▼ Extra Tools (Misc)
  _> ABDUCTOR * Defensive Shield Detector
  _> AI.BOTNET * Intelligent Attack System
  _> AI.BROWSER * Private Sandbox Browser
  _> AI.EVASIVE * Automatic Evasion System
  _> AI.GAMES * Fun & Games Center
  _> AI.GEO * Geomapping System
  _> AI.GLOBAL_NET * Global UFONET Network
  _> AI.LIBRARY * Public (data.Links) Library
  _> AI.STATS * Live Stats Reporter
  _> AI.STREAMING * Video (data.Streams) Player
  _> AI.WEB * Graphical User Web-Interface
  _> BLACKHOLE * Warper (p2p.Botnet) Generator
```

```
[root💀 kali]-[~/home/kali/ufonet]# python3 ufonet --download-zombies
# python3 ufonet --download-zombies
# =====#
# > Botnet [DDoS] # > Close Combat [DoS]
#   ↪ ZOMBIES #   ↪ LOIC
#   ↪ DROIDS #   ↪ LORIS
#   ↪ ALIENS #   ↪ UFSYN
#   ↪ UCAVs #   ↪ XMAS
#   ↪ X-RPCS #   ↪ NUKE
#   ↪ DBSTRESS #   ↪ UFOACK
#   ↪ SPRAY #   ↪ UFORST
#   ↪ SMURF #   ↪ DROPER
#   ↪ TACHYON #   ↪ OVERLAP
#   ↪ MONLIST #   ↪ PINGER
#   ↪ FRAGGLE #   ↪ UFOUDP
#   ↪ SNIPER #
# → [ UFNNet: https://ufonet.03c8.net ] ←
# =====#
# 
# Server: No banner retrieved
# =====#
# The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against
888 888 8888888888 .d88888b. 888b 888 security 888 header is not defined.
888 888 888 d88P Y888b 8888b 888 present 888
888 888 888 888 888 888888b 888 888 This 888 allow the user agent to render the content
888 888 88888888 888 888 8888Y88b 888 .d88b. 8888888
888 888 888 cookie 888 led 888 888 Y88b888 d8P Y8b 888
888 888 888 Session 888d 888 888 Y888888 8888888888 888
Y88b. .d88P 888 attempt Y88b. .d88P 888 Y8888 Y8b. Y88b.
'Y88888P' 888 'Y88888P' 888 Y888 'Y8888 'Y8888

{(D)enial(OFF)ensive(S)ervice[ToolKit]}-{by_(io=psy+/03c8.net)}{flask-neumorphism-uikit}
# =====#
# [AI] Downloading list of [Zombies] from [Community] server ...
# Stats: 0:00:01 elapsed, 0 hosts completed (0 up), 1 undergoing Ping Scan
# Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
# [AI] Trying [Blackhole] [Server]: 46.163.118.220
# [AI] [Control] [Blackhole] [Server] Reply: [VORTEX FAILED!]
```

UFOnet

```
(root㉿kali)-[/home/kali/ufonet]
# python3 ufonet --gui

  _||_ - (00) - + (XX) + - (00) -
  ||| 0 =*~~~~~*= 0 ||| -(00)-
  ||| (0) XX (0) ||| -(00)-
  ||| \ | (00) | / |||
  ||| (0) (0) 0' ____ '0 (0) (0) |||
  ||| | . ' . ( xx ) . ' . | | |
  ||| X | .. ' | X | .. ' | |
  ||| .. . ' / -- . 00 . -- ' \ . ' .. |
  ||| (0) . ) - 0 | \ x | # # | x | / | 0 | - (0) |
  ||| ` - - - - - / - 00 - \ - - - - - ' - - - - |
  ||| . - | | | | | | | | | | | | | | | | | | | |
  ||| / | | | | | | | | | | | | | | | | | | | | |
  ||| { | | | | | | | | | | | | | | | | | | | | |
  ||| | (0) | | | 0 \ | | | * * | | | / 0 | . | | (0) | |
  ||| \ | | | | | | | | | | | | | | | | | | | | |
  ||| . - | | | | | | | | | | | | | | | | | | | |
  ||| . - | | | | | | | | | | | | | | | | | | | |
  ||| YY | | | | | | | | | | | | | | | | | | | |
  ||| H . . | | | | | | | | | | | | | | | | | | |

#=====
> Botnet [DDoS] # > Close Combat [DoS]
    ↗ ZOMBIES # ↗ LOIC
    ↗ DROIDS # ↗ LORIS
    ↗ ALIENS # ↗ UFOSYN
    ↗ UCAVs # ↗ XMAS
    ↗ X-RPCs # ↗ NUKE
    ↗ DBSTRESS # ↗ UFOACK
    ↗ SPRAY # ↗ UFORST
    ↗ SMURF # ↗ DROPER
    ↗ TACHYON # ↗ OVERLAP
    ↗ MONLIST # ↗ PINGER
    ↗ FRAGGLE # ↗ UFOUDP
    ↗ SNIPER # ↗

#=====
→ [ UFONet: https://ufonet.03c8.net ] ←
```

UFOnet GUI

DDos Attack



UFONet - is a /disruptive_toolkit/ that allows to perform **DDoS** and **DoS** attacks ...

REMEMBER -> This code is NOT for

START MOTHERSHIP!

- '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'

Attack

Set your target:

Set place to attack:

Number of rounds:

Configure requests | Generate map! | Extra(s)

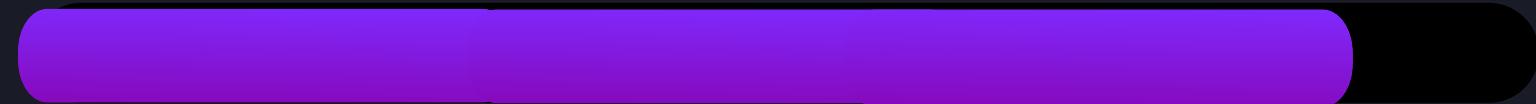
ATTACK! | Total Botnet = **11683**

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!