

---

# CTF web 题型总结

## 第七课 CTF WEB 实战练习 (三)

CTF web 题型总结.....	1
入门第一部分 .....	2
bugku-ctf 第一题: 特殊的后门 .....	2
bugku-ctf 第二题: phpcmsV9 .....	6
bugku-ctf 第三题: bugku 导航.....	7
入门第二部分-社工篇 .....	9
bugku-ctf 社工篇: 密码 .....	9
bugku-ctf 社工篇: 信息查找 .....	9
bugku-ctf 社工篇: 简单个人信息收集 .....	10
bugku-ctf 社工篇: 社工进阶 .....	13
入门第三部分-高级篇 .....	16
第一题: fuzzing .....	16
第二题: pyscript.....	20

---

继上一篇总结：

CTF web 题型总结-第五课 CTF WEB 实战练习(二)

以下也是我在 bugku 练习的解题过程。

以下内容大多是我在 Bugku 自己操作练习，有部分来源于网络，我只是在前人的基础上，对 CET WEB 进行一个总结；

---

---

## 入门第一部分

### bugku-ctf 第一题：特殊的后门



下载压缩包，解压打开

(wireshark 流量包分析)

我们根据题目提示可以看到提示我们 flag 可能在这几个协议中我们打开 wireshark 分析下。

No.	Time	Source	Destination	Protocol	Length	Info
252	43.725732	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) request id=0x0001, seq=0/0, ttl=64 (n
253	43.726055	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) request id=0x0001, seq=0/0, ttl=64 (n
254	43.726210	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) request id=0x0001, seq=0/0, ttl=64 (n
255	43.726319	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) request id=0x0001, seq=0/0, ttl=64 (n
256	43.726458	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) request id=0x0001, seq=0/0, ttl=64 (n
257	43.726568	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) request id=0x0001, seq=0/0, ttl=64 (n
258	43.726756	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) request id=0x0001, seq=0/0, ttl=64 (n
259	43.726880	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) request id=0x0001, seq=0/0, ttl=64 (n
360	43.733136	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) request id=0x0001, seq=0/0, ttl=64 (n

> Frame 252: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)

> Ethernet II, Src: Vmware\_3b:39:9a (00:0c:29:3b:39:9a), Dst: Vmware\_f7:f5:6a (00:50:56:f7:f5:6a)

> Internet Protocol Version 4, Src: 192.168.238.138, Dst: 123.123.123.123

> Internet Control Message Protocol

```

0000  00 50 56 f7 f5 6a 00 0c 29 3b 39 9a 08 00 45 00  .PV..j.. );9...E.
0010  00 29 25 ab 40 00 40 01 6e ff c0 a8 ee 8a 7b 7b  .)%.@.@. n.....{{
0020  7b 7b 08 00 eb ec 00 01 00 00 66 00 00 00 00 00  {{.....f.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

微信号: lemon-sec

虽然我是直接一开始就搜的 icmp....

我们在往下看,

No.	Time	Source	Destination	Protocol	Length	Info
252	43.725732	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) rec
253	43.726055	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) rec
254	43.726210	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) rec
255	43.726319	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) rec
256	43.726458	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) rec
257	43.726568	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) rec
258	43.726756	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) rec
259	43.726880	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) rec
360	43.733136	192.168.238.138	123.123.123.123	ICMP	55	Echo (ping) rec

> Frame 253: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)

> Ethernet II, Src: Vmware\_3b:39:9a (00:0c:29:3b:39:9a), Dst: Vmware\_f7:f5:6a (00:50:56:f7:f5:6a)

> Internet Protocol Version 4, Src: 192.168.238.138, Dst: 123.123.123.123

> Internet Control Message Protocol

```

0000  00 50 56 f7 f5 6a 00 0c 29 3b 39 9a 08 00 45 00  .PV..j.. );9...E.
0010  00 29 25 ac 40 00 40 01 6e fe c0 a8 ee 8a 7b 7b  .)%.@.@. n.....{{
0020  7b 7b 08 00 91 fe 00 01 00 00 66 00 00 00 00 00  {{.....f.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

微信号: lemon-sec

252	43.725732	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping)
253	43.726055	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping)
254	43.726210	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping)
255	43.726319	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping)
256	43.726458	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping)
257	43.726568	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping)
258	43.726756	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping)
259	43.726880	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping)
260	43.727126	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping)

> Frame 254: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)

> Ethernet II, Src: Vmware\_3b:39:9a (00:0c:29:3b:39:9a), Dst: Vmware\_f7:f5:6a (00:50:56:f7:f5:6a)

> Internet Protocol Version 4, Src: 192.168.238.138, Dst: 123.123.123.123

> Internet Control Message Protocol

```

0000  00 50 56 f7 f5 6a 00 0c 29 3b 39 9a 08 00 45 00  .PV..j.. );9...E.
0010  00 29 25 ad 40 00 40 01 6e fd c0 a8 ee 8a 7b 7b  .)%.@. n.....{{
0020  7b 7b 08 00 8b fe 00 01 00 00 6c 00 00 00 00 00  {{..... ..l.....
0030  00 00 00 00 00 00 00 00  .....

```

微信号: lemon-sec

252	43.725732	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping) r
253	43.726055	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping) r
254	43.726210	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping) r
255	43.726319	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping) r
256	43.726458	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping) r
257	43.726568	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping) r
258	43.726756	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping) r
259	43.726880	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping) r
260	43.727126	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping) r

> Frame 255: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)

> Ethernet II, Src: Vmware\_3b:39:9a (00:0c:29:3b:39:9a), Dst: Vmware\_f7:f5:6a (00:50:56:f7:f5:6a)

> Internet Protocol Version 4, Src: 192.168.238.138, Dst: 123.123.123.123

> Internet Control Message Protocol

```

0000  00 50 56 f7 f5 6a 00 0c 29 3b 39 9a 08 00 45 00  .PV..j.. );9...E.
0010  00 29 25 ae 40 00 40 01 6e fc c0 a8 ee 8a 7b 7b  .)%.@. n.....{{
0020  7b 7b 08 00 96 fe 00 01 00 00 61 00 00 00 00 00  {{..... ..a.....
0030  00 00 00 00 00 00 00 00  .....

```

微信号: lemon-sec

252	43.725732	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping
253	43.726055	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping
254	43.726210	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping
255	43.726319	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping
256	43.726458	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping
257	43.726568	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping
258	43.726756	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping
259	43.726880	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping
260	43.727126	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping

> Frame 256: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)

> Ethernet II, Src: Vmware\_3b:39:9a (00:0c:29:3b:39:9a), Dst: Vmware\_f7:f5:6a (00:50:56:f7:f5:6a)

> Internet Protocol Version 4, Src: 192.168.238.138, Dst: 123.123.123.123

> Internet Control Message Protocol

```

0000  00 50 56 f7 f5 6a 00 0c 29 3b 39 9a 08 00 45 00  .PV..j.. );9...E.
0010  00 29 25 af 40 00 40 01 6e fb c0 a8 ee 8a 7b 7b  .)%.@. n.....{{
0020  7b 7b 08 00 90 fe 00 01 00 00 67 00 00 00 00 00  {{.....}g.....
0030  00 00 00 00 00 00 00 00  ....

```

微信号: lemon-sec

257	43.726568	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping
258	43.726756	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping
259	43.726880	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping
260	43.727126	192.168.238.138	123.123.123.123	ICMP	55 Echo (ping

> Frame 257: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)

> Ethernet II, Src: Vmware\_3b:39:9a (00:0c:29:3b:39:9a), Dst: Vmware\_f7:f5:6a (00:50:56:f7:f5:6a)

> Internet Protocol Version 4, Src: 192.168.238.138, Dst: 123.123.123.123

> Internet Control Message Protocol

```

00  00 50 56 f7 f5 6a 00 0c 29 3b 39 9a 08 00 45 00  .PV..j.. );9...E.
10  00 29 25 b0 40 00 40 01 6e fa c0 a8 ee 8a 7b 7b  .)%.@. n.....{{
20  7b 7b 08 00 7c fe 00 01 00 00 7b 00 00 00 00 00  {{...}.....
30  00 00 00 00 00 00 00  ....

```

微信号: lemon-sec

252	43.725732	192.168.238.138	123.123.123.123	ICMP	55 Echo (
253	43.726055	192.168.238.138	123.123.123.123	ICMP	55 Echo (
254	43.726210	192.168.238.138	123.123.123.123	ICMP	55 Echo (
255	43.726319	192.168.238.138	123.123.123.123	ICMP	55 Echo (
256	43.726458	192.168.238.138	123.123.123.123	ICMP	55 Echo (
257	43.726568	192.168.238.138	123.123.123.123	ICMP	55 Echo (
258	43.726756	192.168.238.138	123.123.123.123	ICMP	55 Echo (
259	43.726880	192.168.238.138	123.123.123.123	ICMP	55 Echo (
260	43.727126	192.168.238.138	123.123.123.123	ICMP	55 Echo (

Frame 258: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)  
 Ethernet II, Src: Vmware\_3b:39:9a (00:0c:29:3b:39:9a), Dst: Vmware\_f7:f5:6a (00:50:  
 Internet Protocol Version 4, Src: 192.168.238.138, Dst: 123.123.123.123  
 Internet Control Message Protocol

000	00 50 56 f7 f5 6a 00 0c	29 3b 39 9a 08 00 45 00	.PV..j.. );9...E.
010	00 29 25 b1 40 00 40 01	6e f9 c0 a8 ee 8a 7b 7b	.)%.@. n.....{
020	7b 7b 08 00 ae fe 00 01	00 00 49 00 00 00 00 00	{{..... ..I.....
030	00 00 00 00 00 00 00 00		

微信号: lemon-sec

是不是看的有点眼熟接下来我们顺着一个一个看，便可以得到  
 flag{Icmp\_backdoor\_can\_transfer-some\_infomation}

## bugku-ctf 第二题：phpcmsV9

Challenge 1242 Solves

**phpcmsV9**

100

一个靶机而已，别搞破坏。  
 flag在根目录里txt文件里  
<http://123.206.87.240:8001/>

Flag  Submit

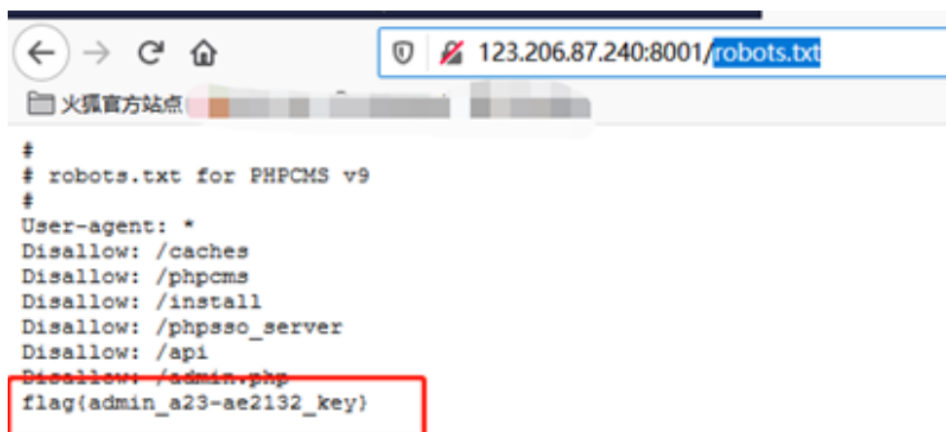
微信号: lemonsec

<http://123.206.87.240:8001/>

根据提示先想到了 robots.txt

访问得到 flag





微信号: lemon-sec

## bugku-ctf 第三题: bugku 导航



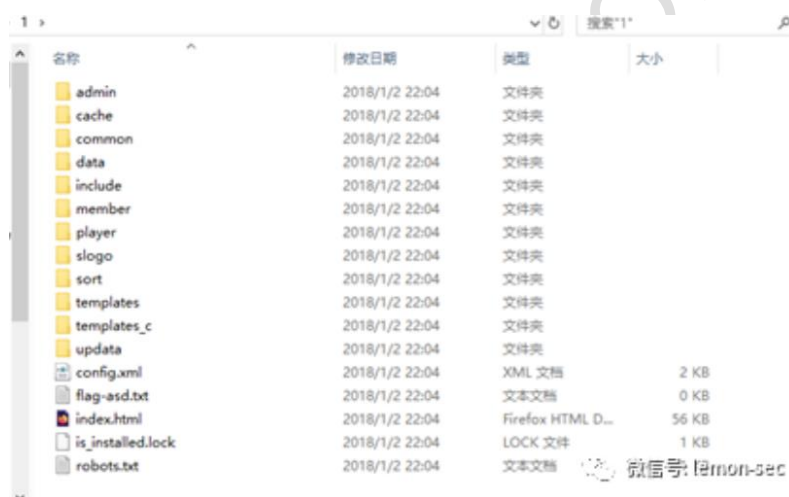
第一步，我们先用扫描器扫描该网站有没有什么敏感文件或资源



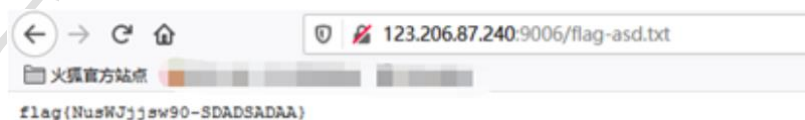
我们发现扫出了 1 个 admin、1.zip、robots.txt 等等敏感文件目录

然后我们访问 1.zip 把该文件下载过来，然后下载解压后发现这个是该网站的源代码

这个时候，我们在看一下上面的题目提示，flag 在根目录，是的，我们发现了这个东西。



在本地打开该文件是没有任何东西的，但是我们在浏览器上访问该文件，就显示出 flag 了。



flag{NusWJjsw90-SDADSADAA}



## 入门第二部分-社工篇

### bugku-ctf 社工篇: 密码

Challenge 5910 Solves

密码

50

姓名: 张三  
生日: 19970315

KEY格式KEY{xxxxxxxxxx}

Flag Submit

分析: 这个是典型的弱口令, 猜了一下, KEY 是姓名+生日, KEY{zs19970315}

### bugku-ctf 社工篇: 信息查找

Challenge 3043 Solves

信息查找

80

社会工程学基础题目 信息查找

听说bugku.cn在今日头条上能找到? ?

提示: flag为群号码

格式KEY{xxxxxxxxxx}

Flag Submit

分析: 直接百度 bugku 群号码,



得出 KEY{462713425}

## bugku-ctf 社工篇：简单个人信息收集



下载压缩包

打开发现压缩包加密了

卡了很久，上网搜索才发现有可能存在伪加密

用 winhex 打开，然后修改 09 为 00



**17 00 00 00: 未压缩尺寸 (23)**

**07 00: 文件名长度**

**24 00: 扩展字段长度**

**00 00: 文件注释长度**

**00 00: 磁盘开始号**

**00 00: 内部文件属性**

**20 00 00 00: 外部文件属性**

**00 00 00 00: 局部头部偏移量**

**压缩源文件目录结束标志:**

**50 4B 05 06: 目录结束标记**

**00 00: 当前磁盘编号**

**00 00: 目录区开始磁盘编号**

**01 00: 本磁盘上纪录总数**

**01 00: 目录区中纪录总数**

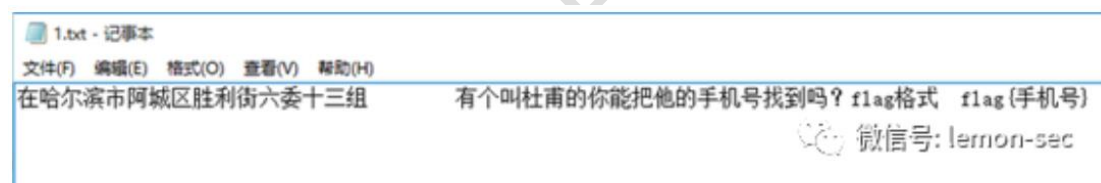
**59 00 00 00: 目录区尺寸大小**

**3E 00 00 00: 目录区对第一张磁盘的偏移量**

**00 00: ZIP 文件注释长度**

好了，修改后重新保存压缩包

打开得到



emmmmm

接下来要用社工库来查询了

但是本菜鸡没找到好用的在线查询网站，请好心的大佬赐教.....

遂 查看前辈们写的 wp，借大佬的查询结果图一用（侵权删）

龚明芳	420601195001287040	F	19500128	湖北省襄樊市樊城区建设路杜南巷6号附082号			胜利路六十三组 第1页, 共1
陶文殿	410124197307025064	F	19730702	河南省巩义市杜南路口号1号楼附20号			
常朝阳	410124197403105013	M	19740310	河南省巩义市杜南路14号1号楼附20号			这个地方搜索地名
张欢	410124196902105013	M	19690210	河南省巩义市杜南路64号职工宿舍			
曹志强	410181197508275032	M	19750827	河南省巩义市杜南路108号附6号			找到了手机号
李磊磊	410181198610025069	F	19861002	河南省巩义市杜南路10号			
魏宝莹	410181198309024521	F	19830807	河南省巩义市杜南办事处外沟村马家寨13排4号			
杜南	230119198405040313	M	19840504	湖北省荆门市钟祥市杜南镇杜南村王东组	15206164164		
杜南	410103198503100116	M	19850310	河南省濮阳县江家集镇杜南店村王东组			
何世英	413024197003285120	F	19700328	河南省濮阳县江家集镇杜南店村王东组			
袁秋红	41018119701106554X	F	19701106	河南省巩义市杜南路43号3号楼附19号			
宋福娟	410124196805055552	M	19680505	河南省巩义市杜南路43号3号楼附19号			
杜南金	412324197710186549	F	19771018	河南省宁陵县孔集乡前01楼村61号			微信号: lemon-sec

flag{15206164164}

## bugku-ctf 社工篇：社工进阶

Challenge
1587 Solves

社工进阶
100

name: 孤长离
提示: 弱口令

Flag
Submit

由于之前知道有 bugku 的百度吧 并且这个是一个社工题所以可以试一下这个百度吧

进入百度吧然后会见到



这句话的意思是要我们登录这个账号 但是我们只有账号没有密码 如果爆破的话很有可能爆破不开 所以我们再重新看一下 题目然后 我们看到了一个关键词“弱口令” 然后我们去百度弱口令 top100.

然后会发现弱口令

密码中包含有 148 数字的, 出现 11418 次  
 密码中包含有 520 数字的, 出现 4549 次  
 密码中包含有 1314 数字的, 出现 3113 次  
 密码中包含有 aini 的, 出现 877 次

密码	出现次数
123456	392
a123456	282
123456a	168
5201314	161
111111	157
woaini1314	140
qq123456	100
123123	98
000000	97
1qaz2wsx	95
1qaz3e4r	84
qwe123	80
7758521	76
123qwe	68
a123123	63
123456aa	56
woaini520	56
woaini	52
100200	52
1314520	52
woaini123	51
123321	50
q123456	49
123456789	49
123456789a	49



<https://blog.51cto.com/10907603/2139653>

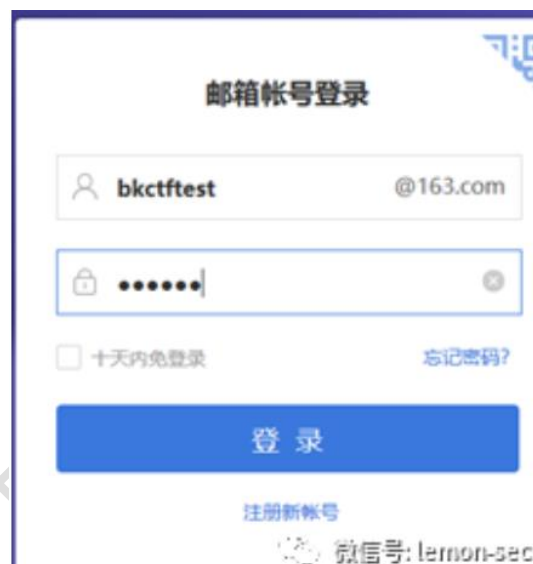
以下是在 12306 泄露的密码中，使用次数最多的密码排行，大家在修改密码时候，尽量避免使用类似的规则。

密码中包含有 123456 数字的，出现 3236 次  
密码中包含有 123 数字的，出现 11213 次  
密码中包含有 520 数字的，出现 4549 次  
密码中包含有 1314 数字的，出现 3113 次  
密码中包含有 aini 的，出现 877 次

密码	出现次数
123456	392
a123456	282
123456a	168
5201314	161
111111	157
woaini1314	140
qq123456	100
123123	98

微信号: lemon-sec

然后一个个试一下这些弱口令



然后发现第二个 就是密码 然后登录 进入邮箱



应该会发现一个邮件 邮箱那里面就有 flag



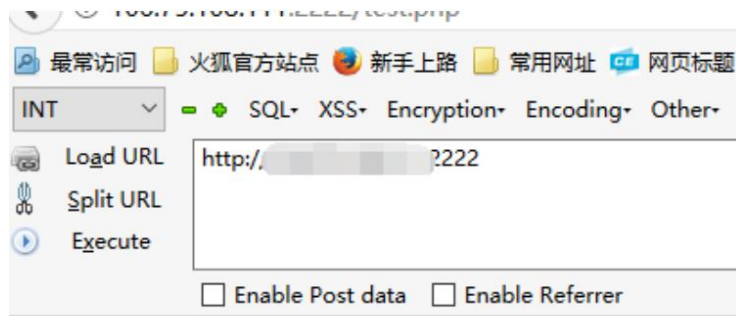
## 入门第三部分-高级篇



### 第一题：fuzzing

访问目标网址，“there is nothing”，小编心想，没东西是不是可以不做了？

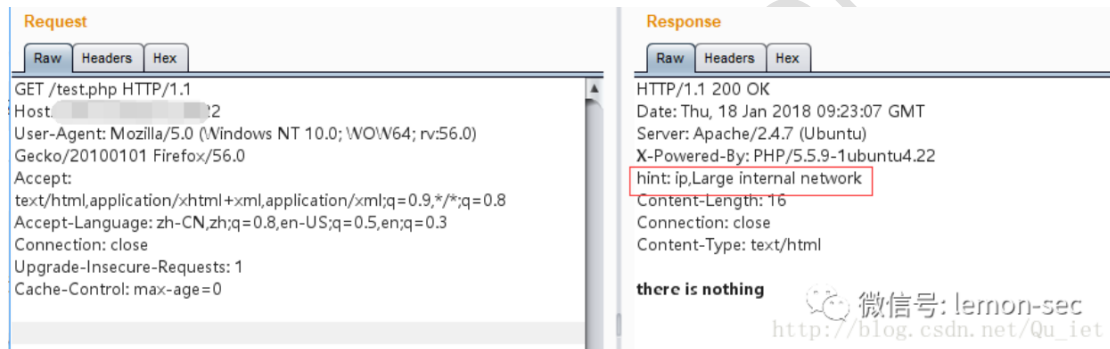
当然是不可能了，年轻人想想就好了，何必当真呢



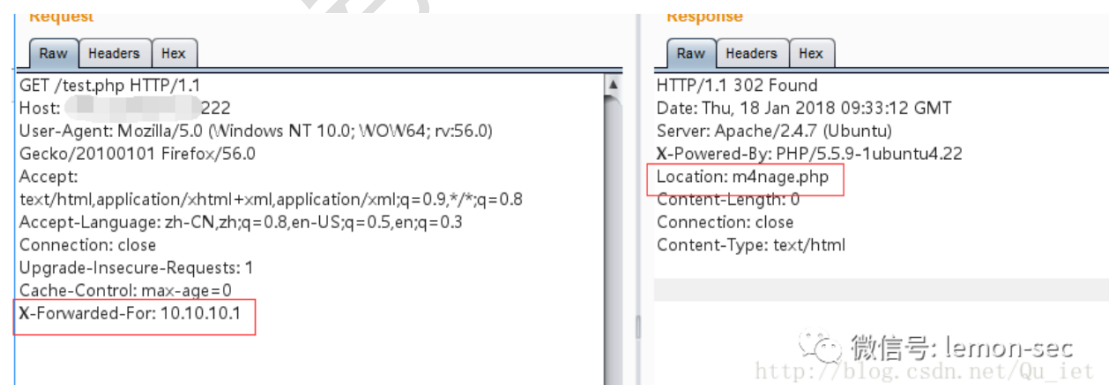
there is nothing

[http://blog.csdn.net/Qu\\_iet](http://blog.csdn.net/Qu_iet) (微信号: lemon-sec)

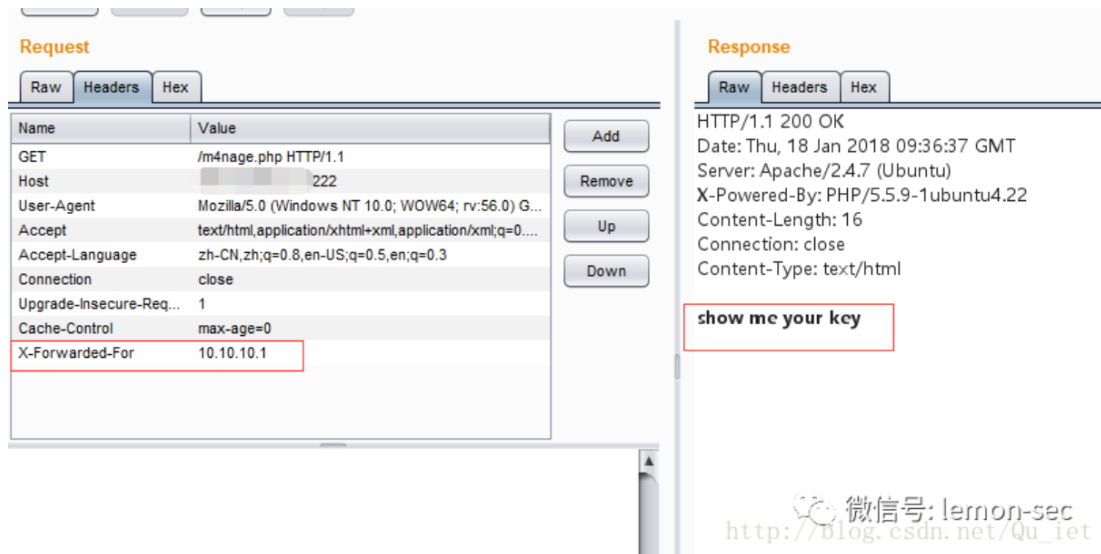
burp 抓包查看响应情况，初看好像没什么，这个时候拼什么呢，拼的是小编的这份细心了，看见小编圈起来的了嘛，很有用哦



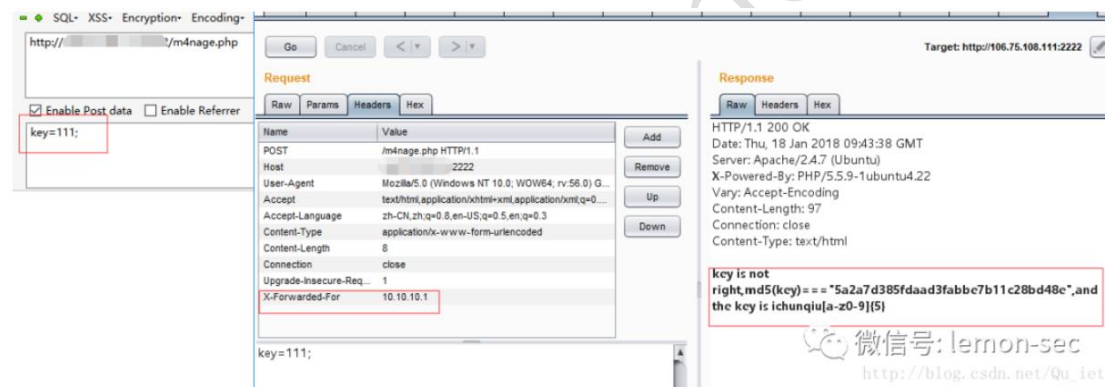
伪造一个 IP，查看响应，出现了一个“m4nage.php”，进行访问，继续抓包



继续伪造 IP，可以看到回显内容“show me you key”



任意构造一个 key 值，继续伪造 IP，发包访问，可以看到回显了找到正确的 key 的方法

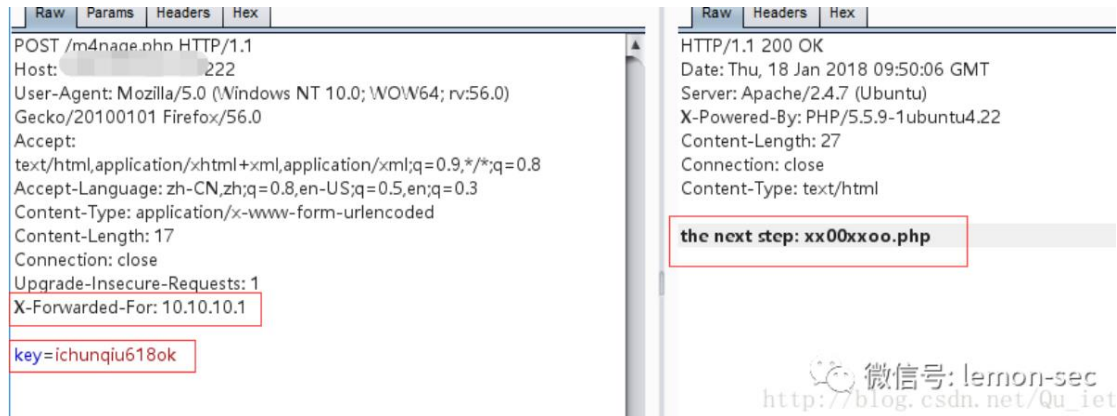


破解 key 值得 python 代码如下，破解出来的 key 值为“ichunqiu618ok”

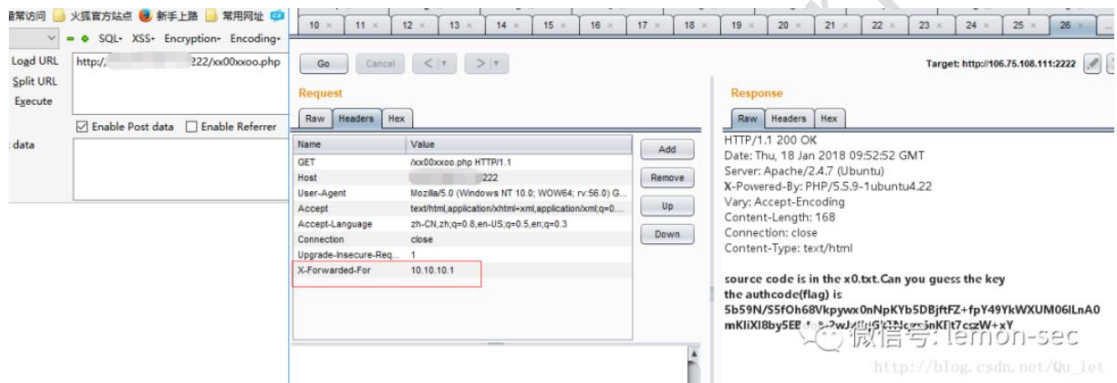
```
import hashlib
def md5(data):
    m = hashlib.md5()
    m.update(data)
    a = m.hexdigest()
    return a
a = 'ichunqiu'
b = 'abcdefghijklmnopqrstuvwxyz1234567890'
for i in b:
    for j in b:
        for k in b:
            for l in b:
                for m in b:
                    if md5(a+i+j+k+l+m)=='5a2a7d385fdaad3fabbe7b11c28bd48e':
```

```
print a+i+j+k+l+m
```

传入正确的 key 值后，回显了一个 php 文件



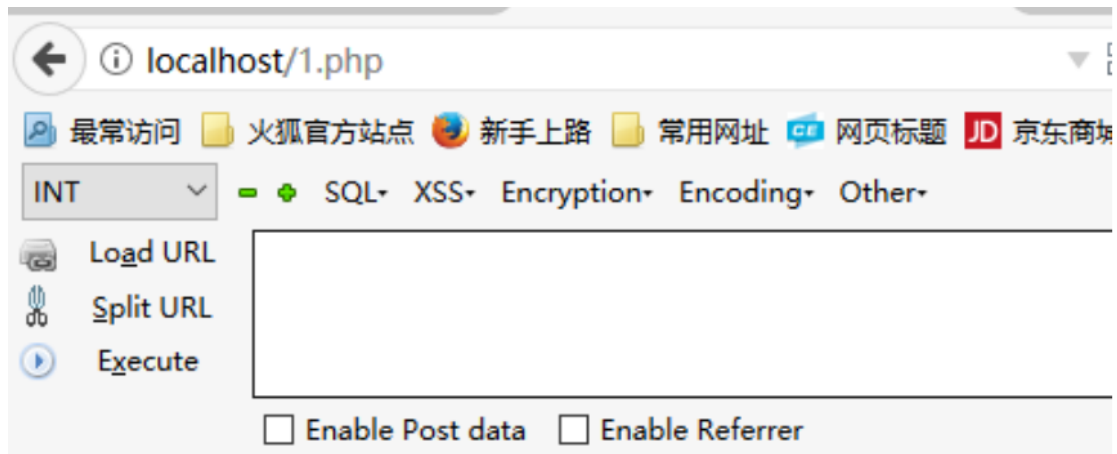
继续 burp 抓包，伪造 IP 访问，得到一个“x0.txt”文件



访问是一段 php 的源码函数，复制到本地，对代码进行修改，在最后对函数进行 echo 输出。



本地网页访问代码，即可得到 flag 信息



flag{bf9c71de-9852-93a0-9852-a23bc07dd12e}

<http://blog.csdn.net/lemonsec> 微信号: lemon-sec

## 第二题：pyscript

访问目标网址，很有趣的界面，“input your answer”，那么到底输入什么呢，小编也不知道，只有继续乱翻翻看了



查看网页源代码，小编发现了一个重要的线索（很重要哦），不过看完之后看来小编还是逃不了代码的命了



```

4  <meta charset="UTF-8" />
5  <title>Hello</title>
6  <link rel="stylesheet" href="css/style.css" media="screen" type="text/css" />
7  </head>
8
9  <body>
10 <!--ROUND ONE-->
11 <!--找出明文 -->
12 <!--sha1(三个数字+2TrGK06UwDdHXRwPmUONT1ASWKZpxw)==Ciphertext -->
13 <!--请于10s内提交答案 -->
14 <div class="panel">
15   <div class="wrap">
16     <form method="POST" action="#">
17       <input type="text" name="pass" placeholder=" here" />
18       <button onclick="form.submit();">Shhh!</button>
19     </form>
20   </div>
21 </div>
22 <div style="text-align:center;clear:both">
23 </div>
24 </body>

```

微信号: lemon-sec  
<http://blog.csdn.net/du1111>

破解代码 python, 如下

```

import urllib,urllib2,json
import hashlib
import re
import requests

url = 'http://106.75.108.111:1111'

def sha_1(data):
    sha_1 = hashlib.sha1()
    sha_1.update(data)
    sha = sha_1.hexdigest()
    return sha

def key(key1,key2):
    c='0123456789'
    str1 = key1
    cipher = key2
    for i in c:
        for j in c:
            for k in c:
                if sha_1(i+j+k+str1) == cipher:
                    # print (i+j+k)
                    return i+j+k

def get_info():
    r = requests.post("http://106.75.108.111:1111")
    key2 = r.headers['Ciphertext']

```

---

```
cookies = r.cookies
html = r.text
res = r'\+(.*?)\'
key1 = re.findall(res,html)[0]
print key1
return key1,key2,cookies

def postx(number,cookies):
    cookies = cookies
    values={'pass':number}
    response = requests.post("http://106.75.108.111:1111",cookies=cookies,data=values)
    return response.text

def sum(text):
    res = r'<!--.*?([\d\+\-\*]+).*?-->'
    key3 = re.findall(res,text)[0]
    result = eval(key3)
    return result

if __name__ == '__main__':
    (key1,key2,cookies)=get_info()
    number = key(key1,key2)
    result1 = postx(number,cookies)
    result2 = sum(result1)
    print result2
    print postx(result2,cookies)
```

直接运行，滴滴滴，flag 信息瞬间就出来了呢

```
LI1XYdiyjsK1bNHM3IkWQGB0hCZw9
-5428003978279
<!DOCTYPE html>
<html>
<head>
  <meta charset="UTF-8">
  <title>Hello</title>
  <link rel="stylesheet" href="css/style.css" media="screen" type="text/css" />
</head>
<body>
<!--找出明文 -->
<!--flag {895e7500-ba10-bcc4-84fd-548db6b34f0f} -->
<!--请于10s内提交答案 -->
  <div class="panel">
    <div class="wrap">
      <form method="POST" action="#">
        <input type="text" name="pass" placeholder=" here"/>
        <button onclick="form.submit();">Shhh!</button>
      </form>
    </div>
  </div>
<div style="text-align:center;clear:both">
</div>
</body>
```

微信号: lemon-sec  
[http://blog.csdn.net/qu\\_iet](http://blog.csdn.net/qu_iet)

原文链接: [https://blog.csdn.net/qu\\_iet/java/article/details/79099218](https://blog.csdn.net/qu_iet/java/article/details/79099218)

所有需要资料均是我个人学习笔记, 根据在 bugku 平台的练习以及参考了互联网上各位大佬的思路经验进行总结。

互联网上的思路过于零散, 很少有资料是系统的从理论到实践的总结。本着共享的经身, 这几天关于 CTF-WEB 的学习笔记进行了整理, 可分享。

有需要的可以私聊我公众号, 回复“CTF 学习资料”获取。

CTF web 方面和渗透测试涉及的知识点基本一样, 但是思路又完全不一样。渗透测试基本是整个站漏洞挖掘的思路, CTF 基本是单个点的思路。相同点即是他们所涉及的漏洞点、知识点、利用方式是一样的。对于有渗透基础的大佬来说, 学习 CTF 只是学习一个解题思路;

以上仅是我个人见解, 整理的笔记中涉及的点并不全, 大多漏洞点其实并没有涉及到,

后续如进行深度学会 CTF web 方面的话, 我会继续进行整理分享。