封神台 第三章：为了更多的权限！留言板！【配套课时：cookie伪造目标权限 实战演练】

原创

E08640104 于 2021-06-14 22:59:15 发布 453 收藏
分类专栏： 渗透测试 文章标签： 安全

本文链接：https://blog.csdn.net/E08640104/article/details/117914227

题目

Tips:

1、存储型Xss
2、flag在cookie里，格式为zkz{..}，xss bot 每10秒访问一次页面
3、自建Xss平台源码：http://www.zkaq.org/?t/99.html

经过一番操作，尤里虽然进入到后台，窃窃自喜的他不满足于此，作为黑阔他要挑战曾经的自己，他要攻克之前失手的网站！
他重新浏览之前的网站，这时他突然发现了一个留言板功能。而留言板管理员是每天都会去查阅的。
尤里开始动手……

1.进入留言的页面，测试弹窗

发现弹框显示1，注入点为主题

二、输入注入命令

根据题目得知flag在cookie中，在主题中植入木马

```
<script>alert(document.cookie)</script>
```