

ctf实战 封神台的靶场 第四关通关记录

转载

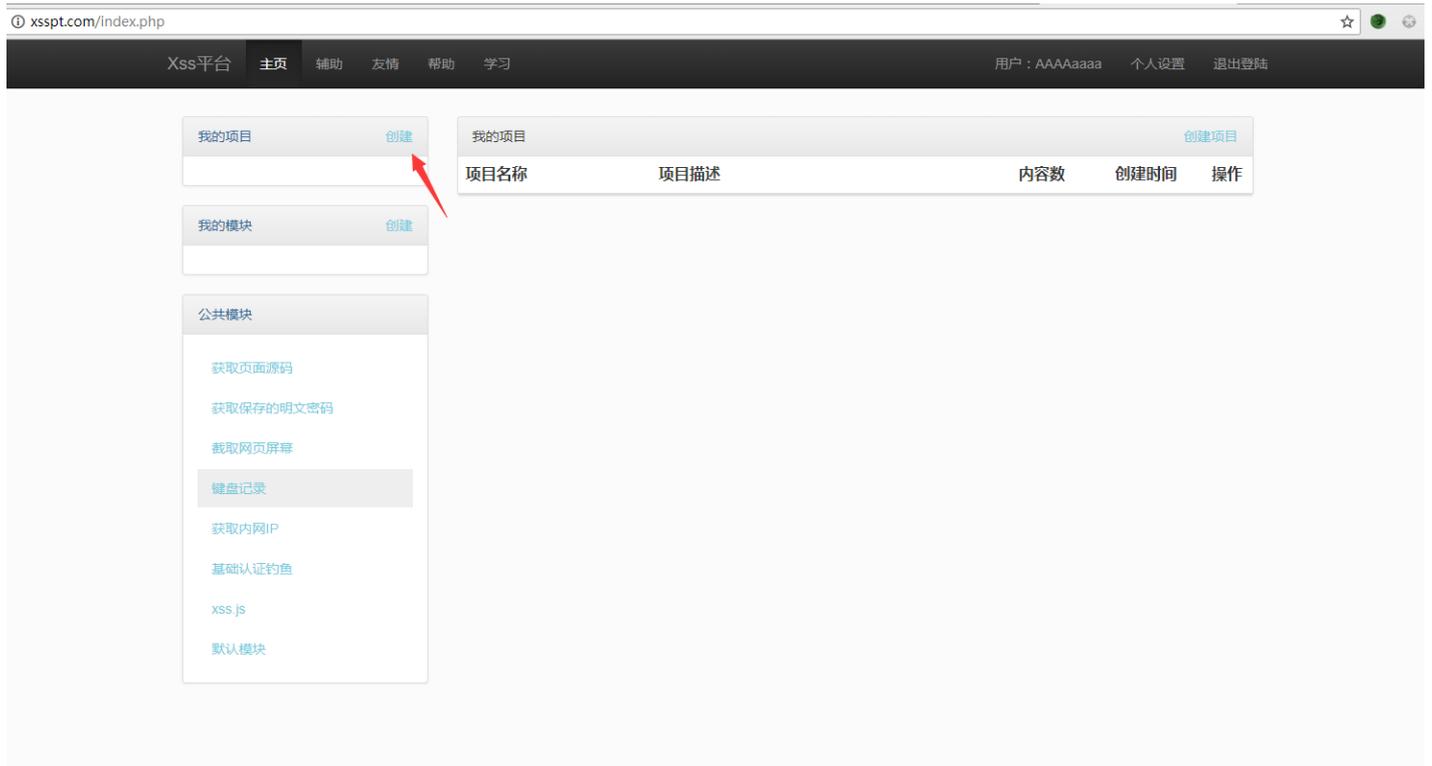
[weixin_30437847](#) 于 2019-05-28 01:33:00 发布 849 收藏

原文链接: <http://www.cnblogs.com/jackzz/p/10934779.html>

版权

发现留言板功能, 顺手试下反射型xss代码, 结果成功的弹窗了

网上的xss平台:<http://xsspt.com>,需要自己去注册和登录, 反正账号密码知道就行了, 邮箱反正不验证不建议写真实的。



我们先建立项目, 名称什么乱选都行, 就是选择模块的时候记得选取这两个



然后你可以看到一叠代码, 这个就是两个模块中的XSS Payload。把生成的存储型xss链接放入留言板提交成功后到xss平台等查收用户cookies ip信息 (cookie劫持盗用风险, 冒用用户登陆、支付等)。

我的项目
创建

jackzz安全

我的模块
创建

公共模块

js攻击

post指定页面源码读取

KillAdmin

QQ skey获取

项目内容
配置 查看代码

项目名称: jackzz安全
记录数: 2/200

Domain:

接口地址: <https://xsspt.com/do/auth/980d9e8dc1f70297f729142786666015> (加 /domain/xxx 可通过域名过滤内容)

+ 全部

	时间	接收的内容	Request Headers	操作
<input type="checkbox"/>	- 2019-05-28 01:15:54	<ul style="list-style-type: none"> • location : [REDACTED] • topolocation : [REDACTED] • cookie : ASPSESSIONIDQ QBBCBCR=IGIFPHNBMPH 	<ul style="list-style-type: none"> • HTTP_REFERER : [REDACTED] • HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/534.34 (KHTML, like Gecko) PhantomJS/1.9.7 Safari/534.3 	删除

转载于: <https://www.cnblogs.com/jackzz/p/10934779.html>