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

原创

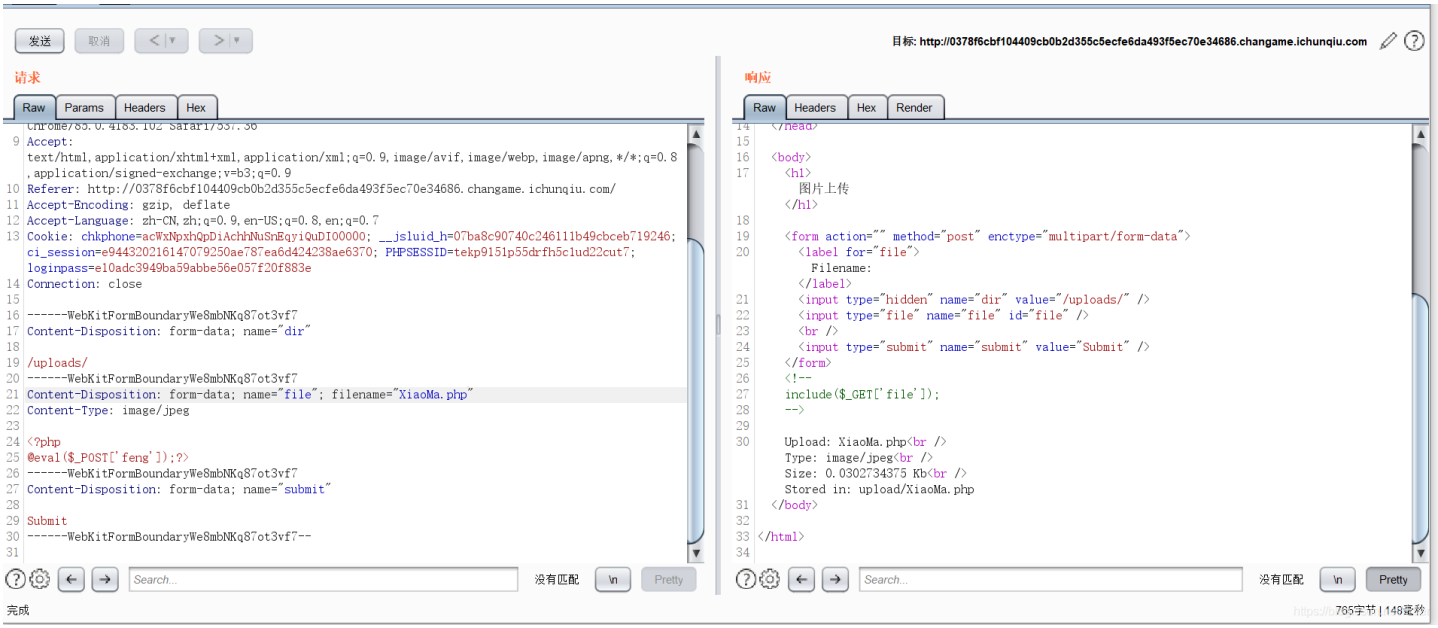
bfengj 于 2020-09-10 10:52:15 发布 372 收藏

分类专栏： 文件上传 文章标签： 数据库 php mysql 安全 信息安全

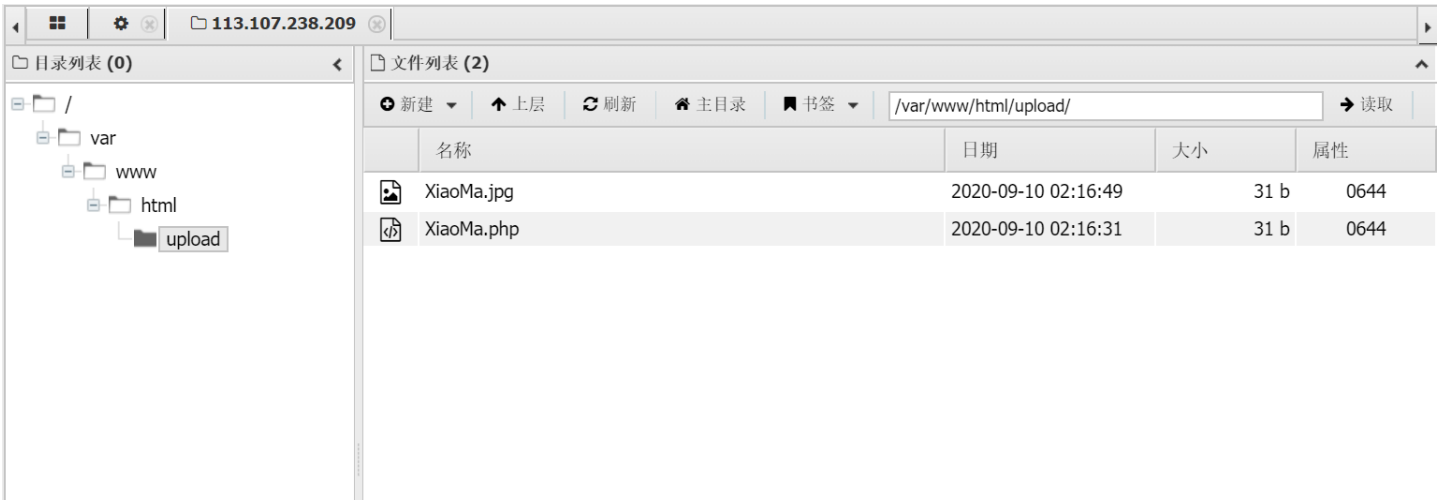
本文链接：https://blog.csdn.net/rfrder/article/details/108508537

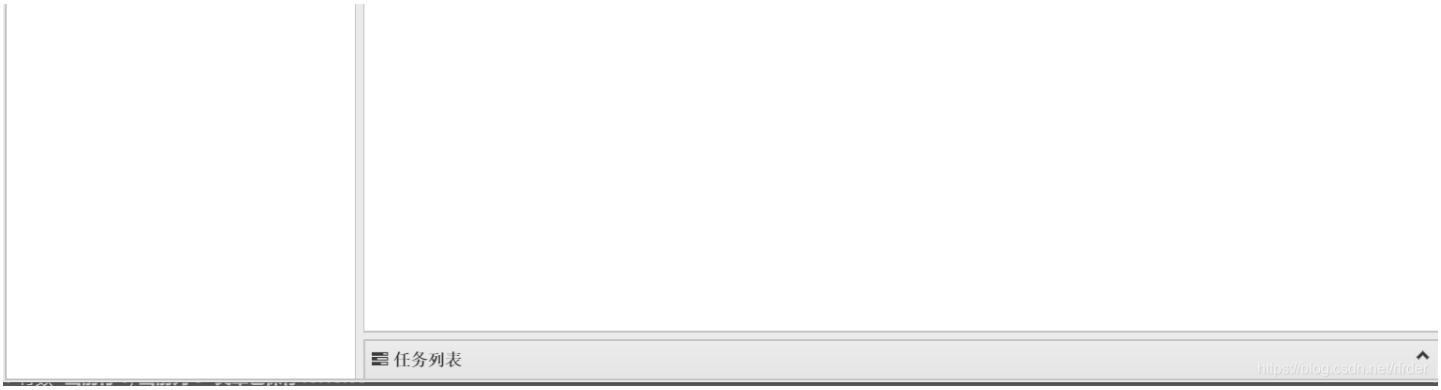
WP

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：



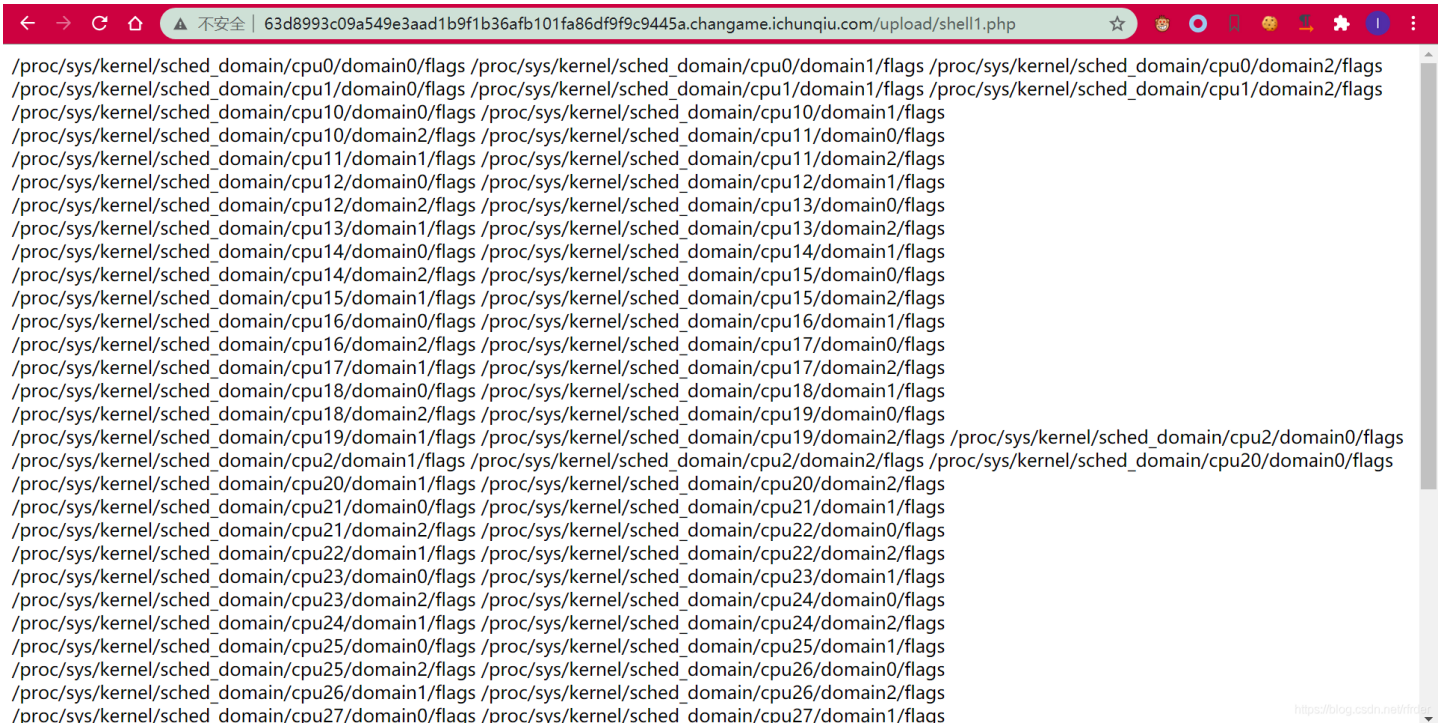
发现直接就上传成功了，当时还有点不可思议。然后我们用蚁剑连一下试试，发现连上去了：





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：



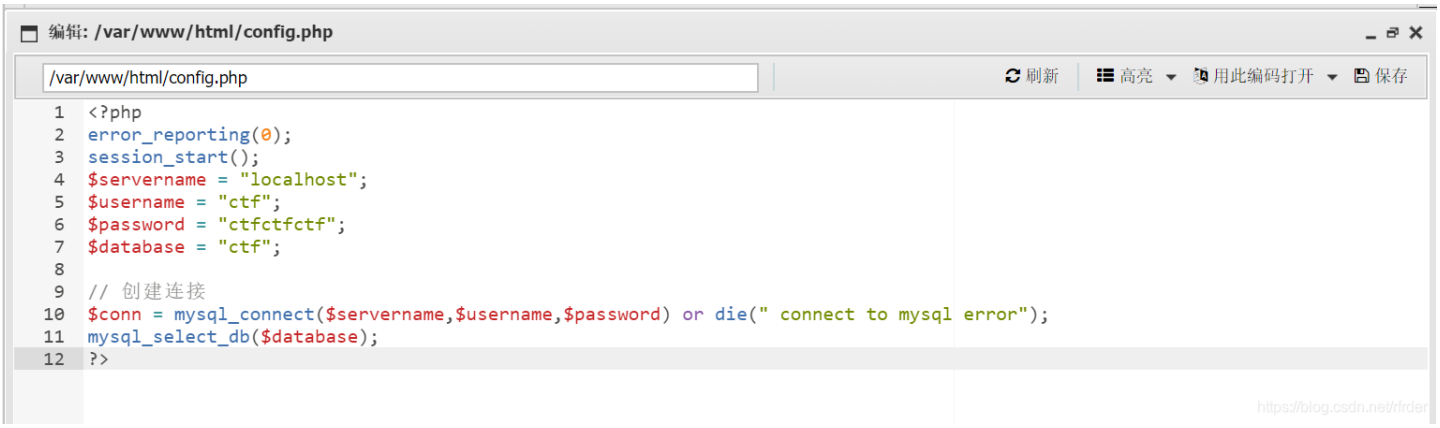
最后我也没找到flag。只能去看WP，知道了新的姿势：

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）

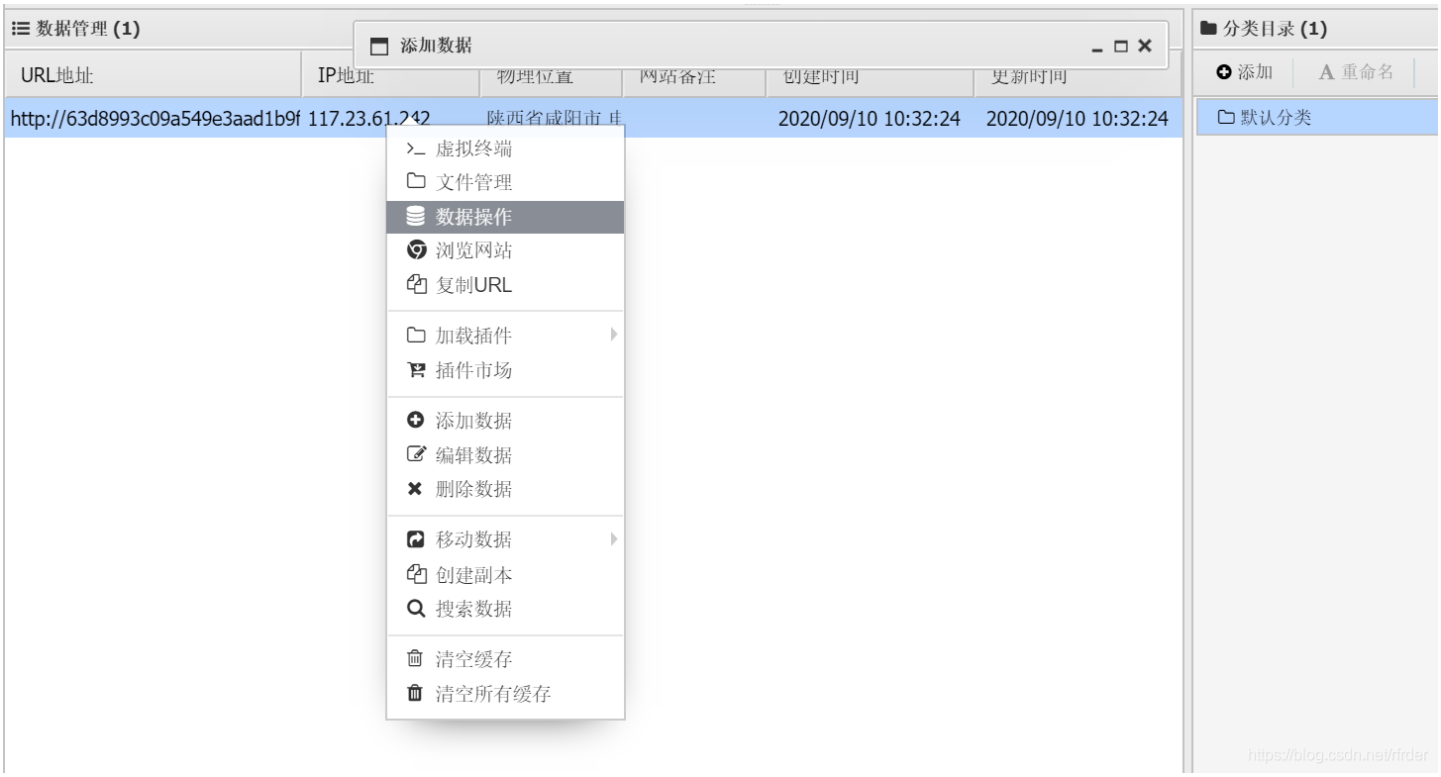
我们进入config.php就可以获得登进数据库的用户名和密码了：



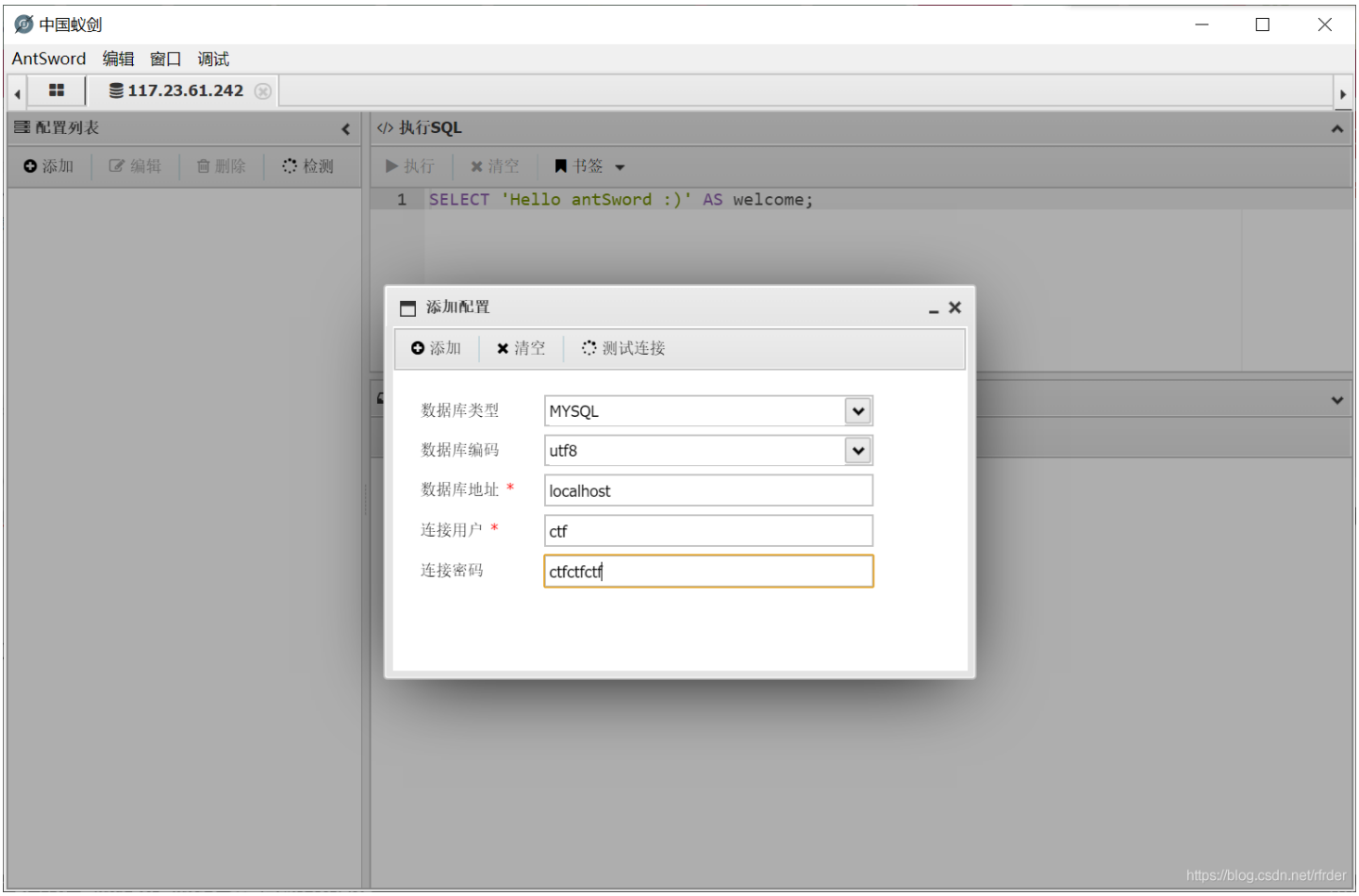
这时候我们有两种方法进入数据库：

方法一：使用蚁剑连接

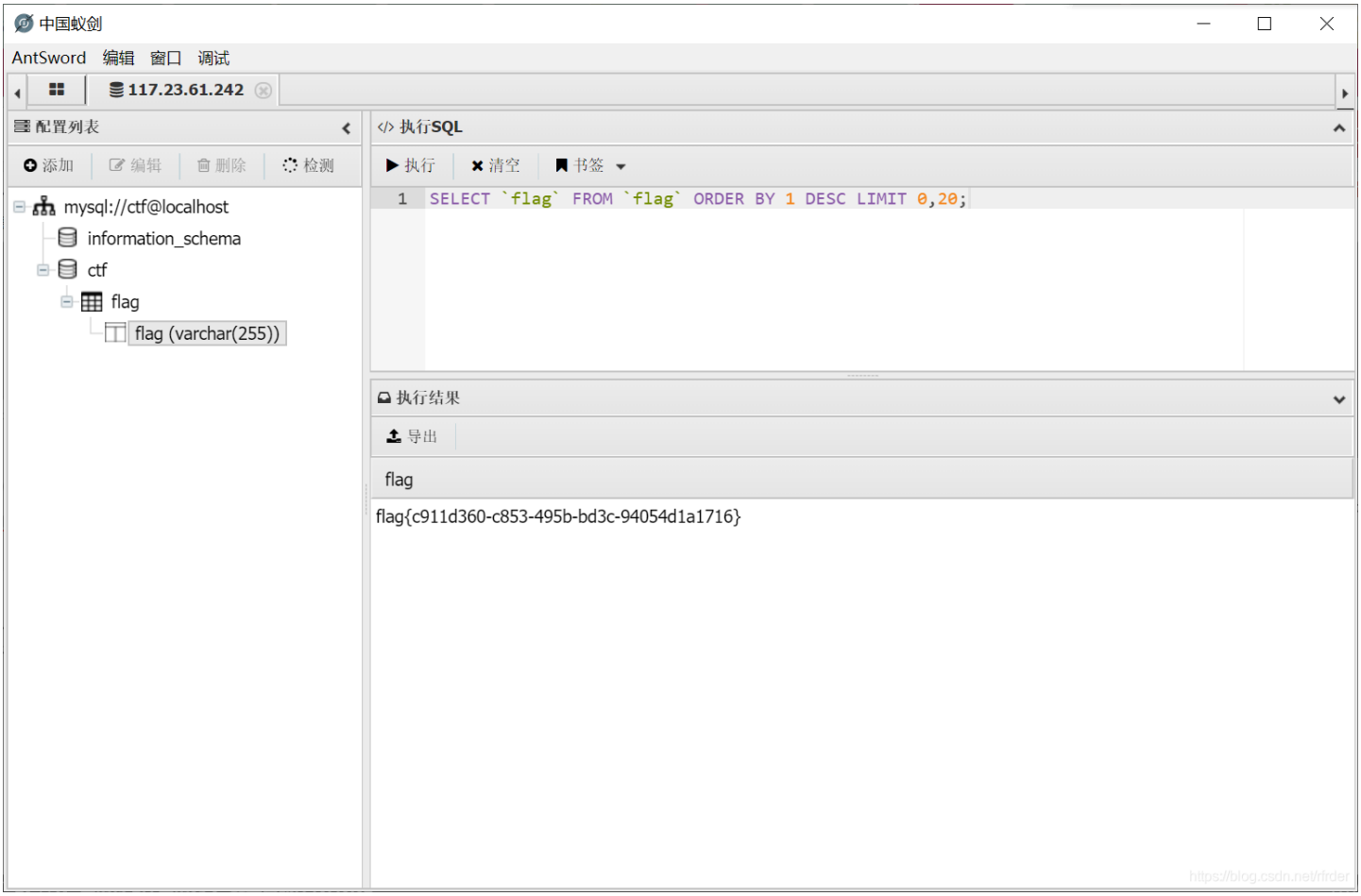
我以前真不知道蚁剑还能连数据库，我找了好久才发现原来在这里：



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：

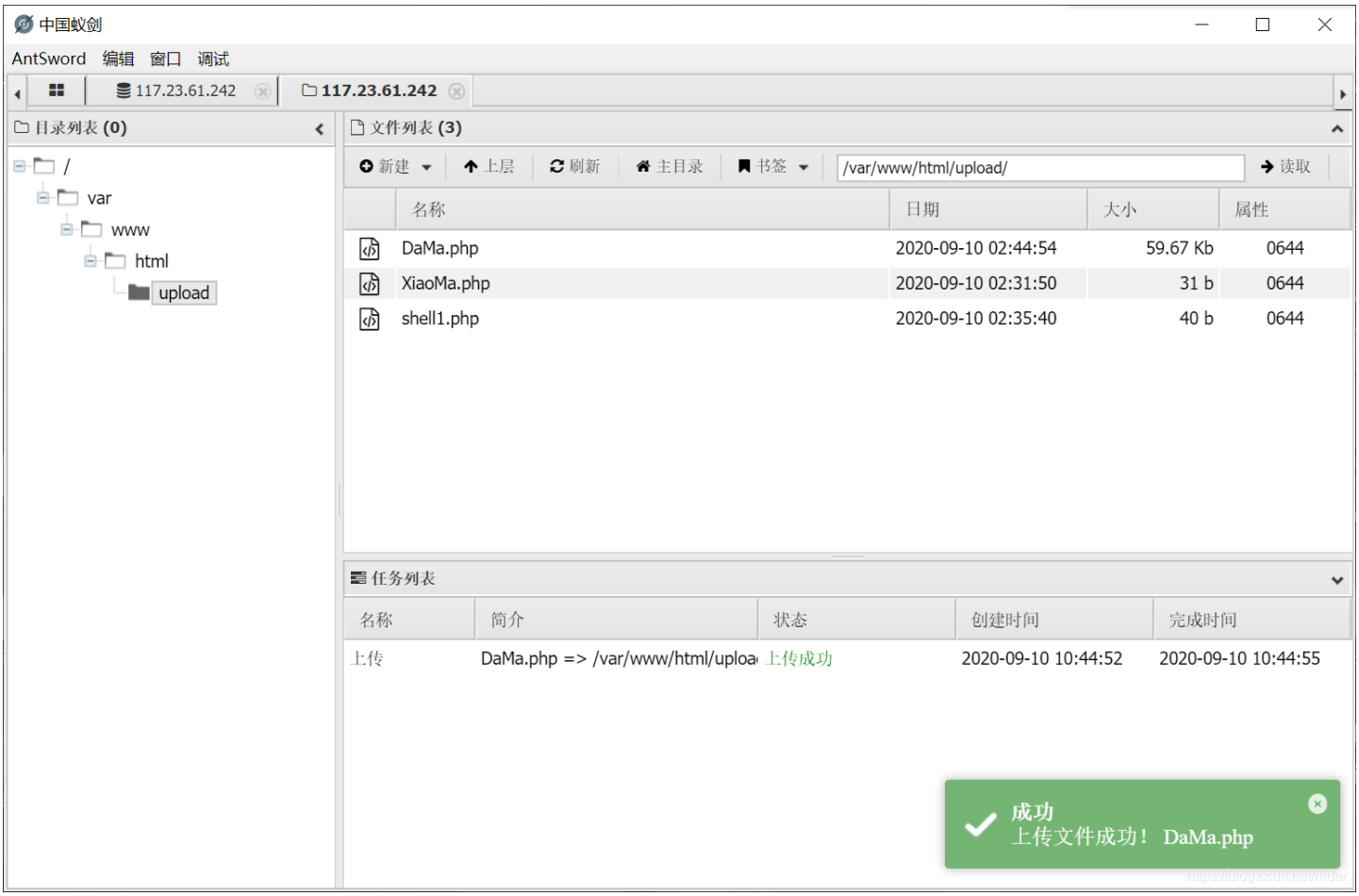


连接成功后进入数据库，我们最后找到flag那里。注意的是，点那个flag没有用，你还要点右边执行SQL中的执行就可以获得flag了：

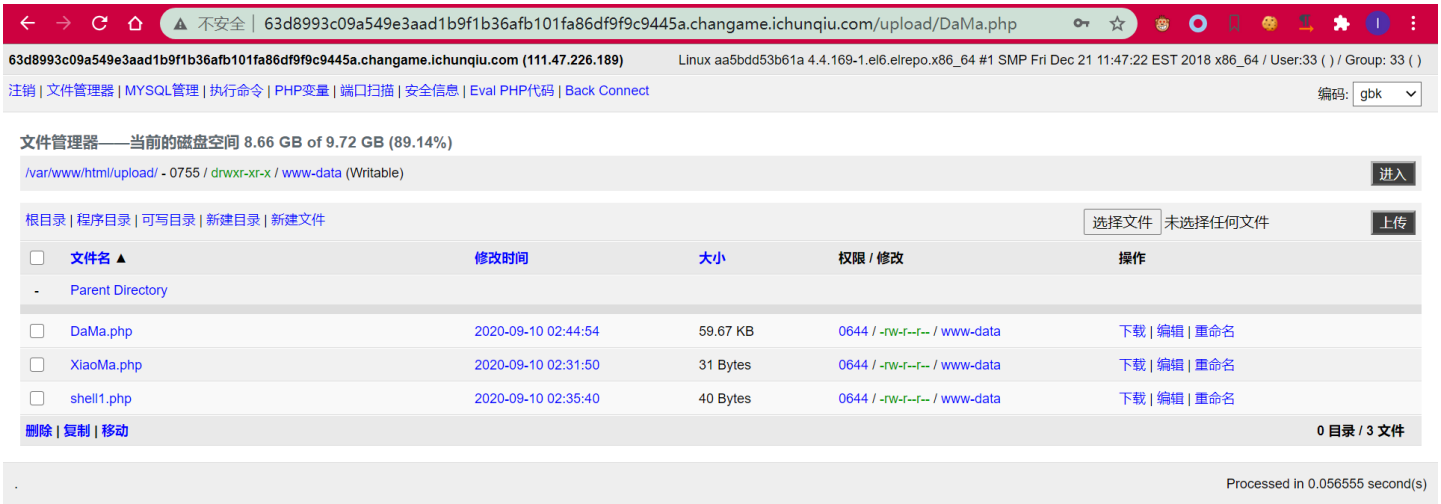


方法二：使用大马

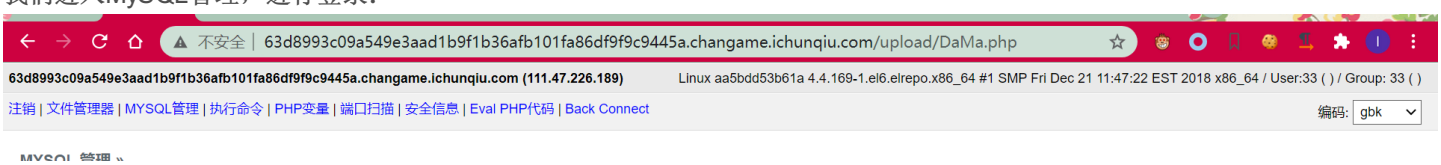
一般来说都是用小马来上传大马。我们这里就直接上传大马了。

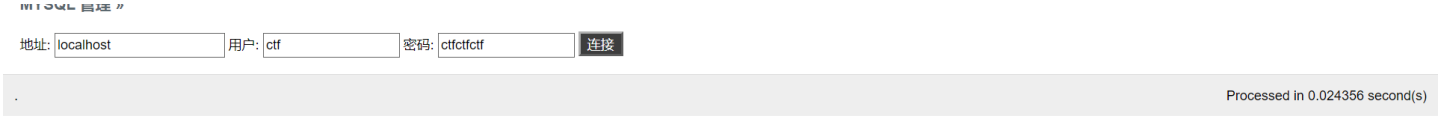


上传成功后在网页中进入大马：



我们进入MySQL管理，进行登录：





进入之后找到flag就可以了：

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。