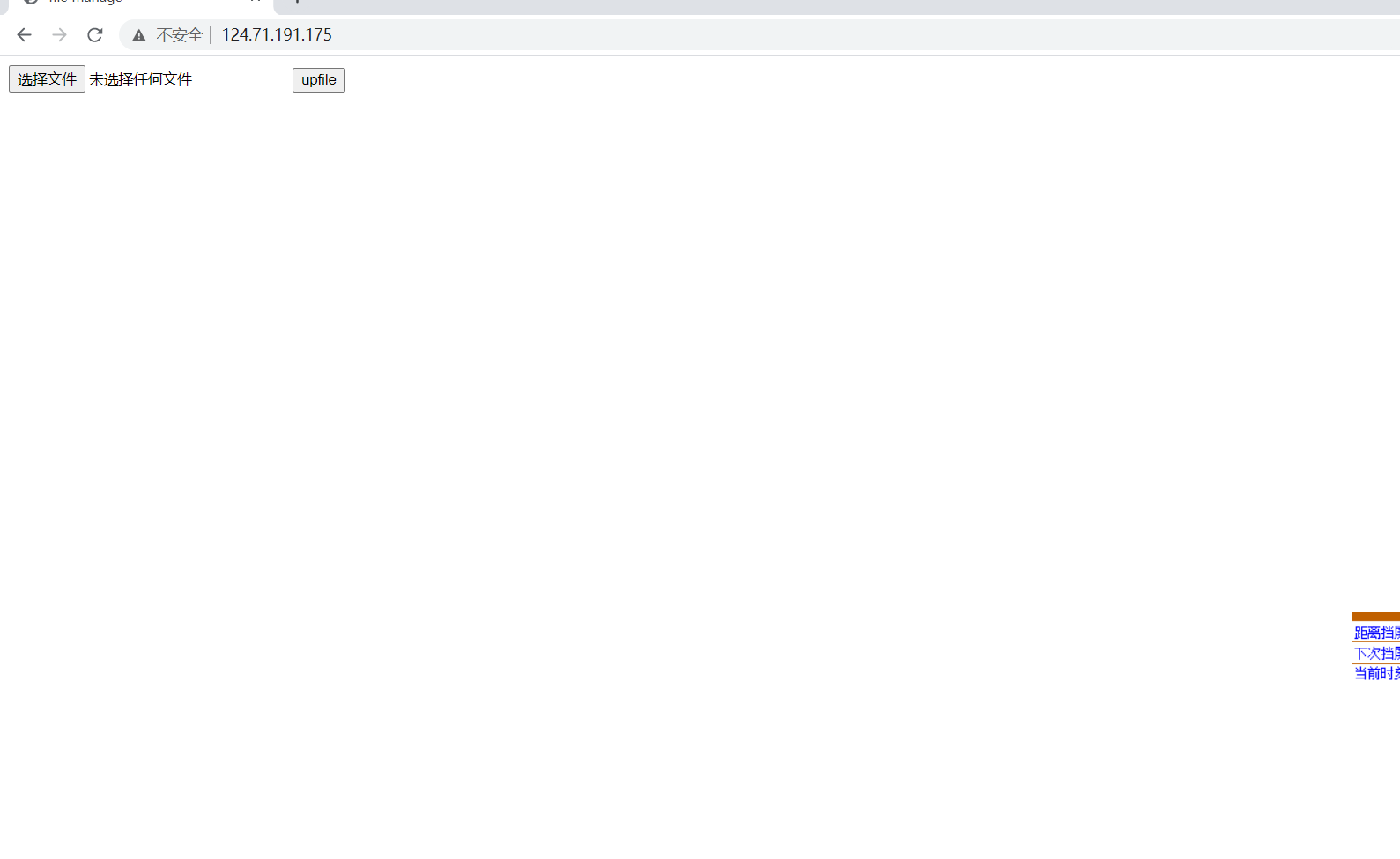
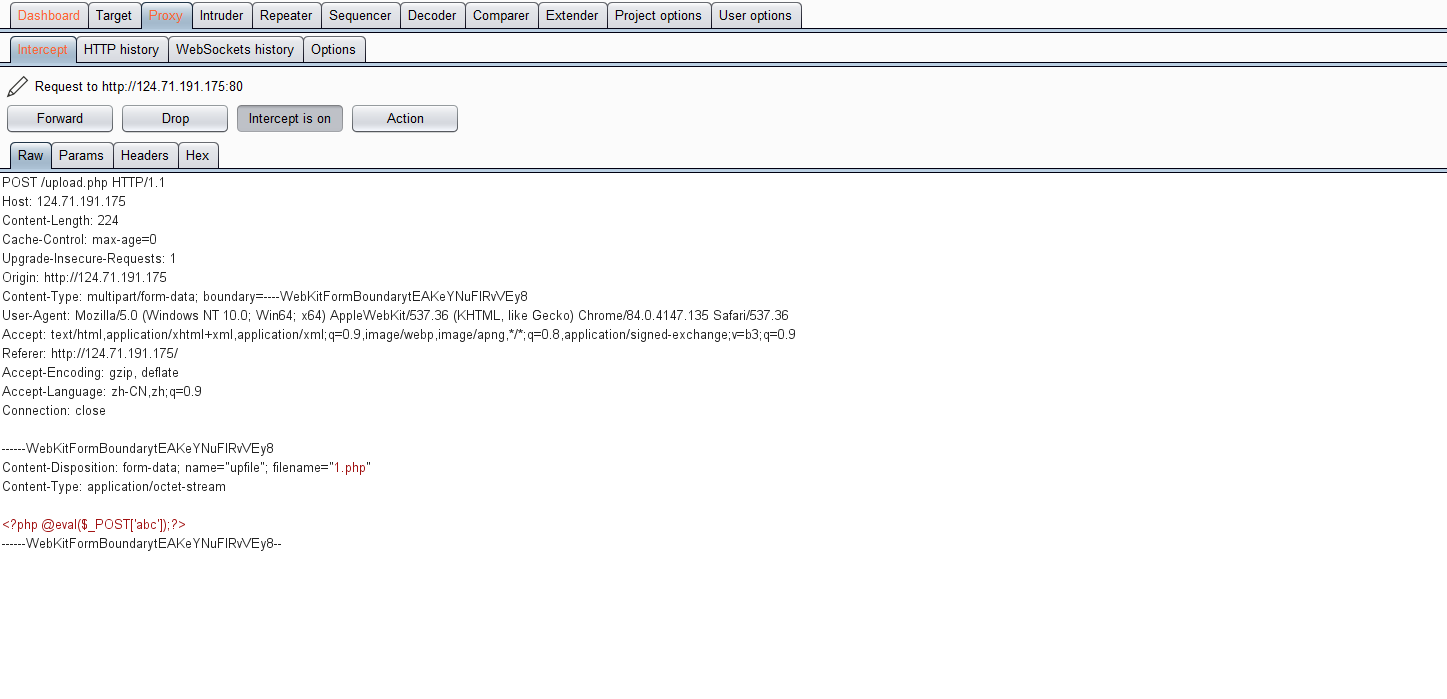
**首先，打开目标题目**

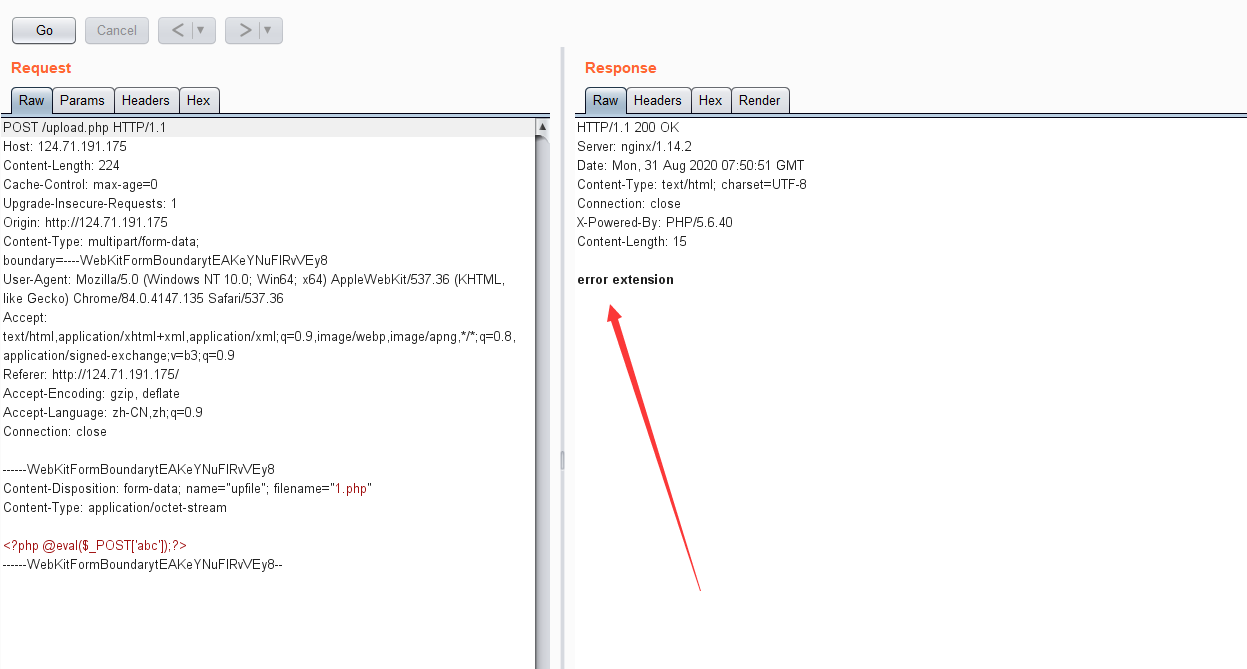


**第一反应，这是一道文件上传的题目**

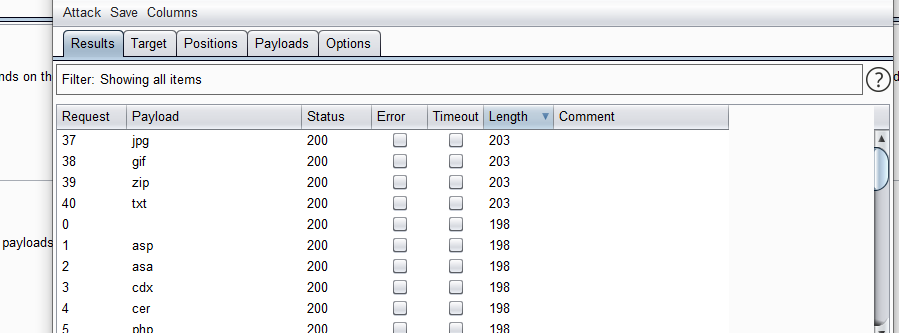
**尝试直接上传我们的webshell并抓包**



**发送到reapeter模块，尝试出waf**

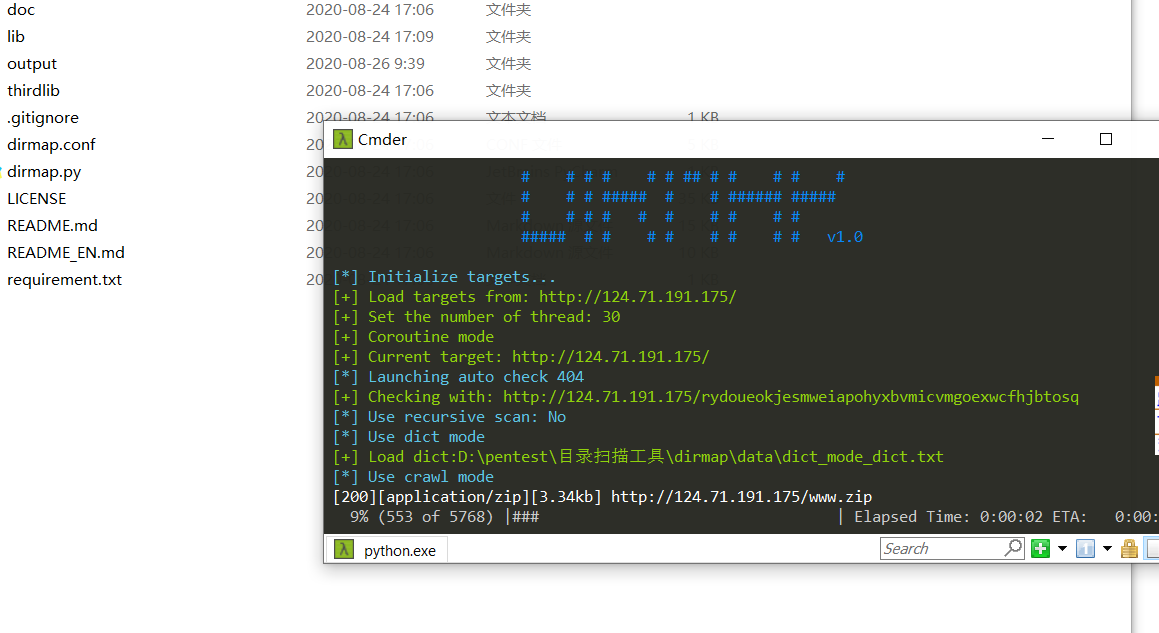


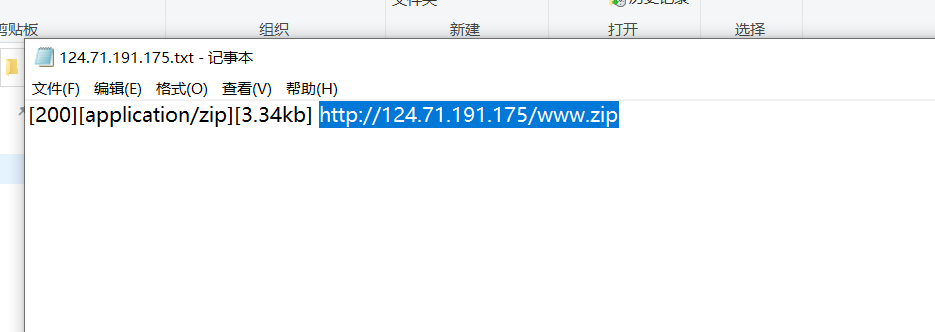
**果然，提示后缀名出错，说明检测了后缀名，拿出准备好的常用后缀名txt，进行爆破**



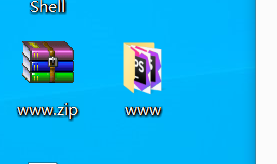
**白名单配置，要么现在尝试解析漏洞，ini文件，htpacess文件都不行，加点号，：也不行。**

**尝试其他出路，扫描目录**





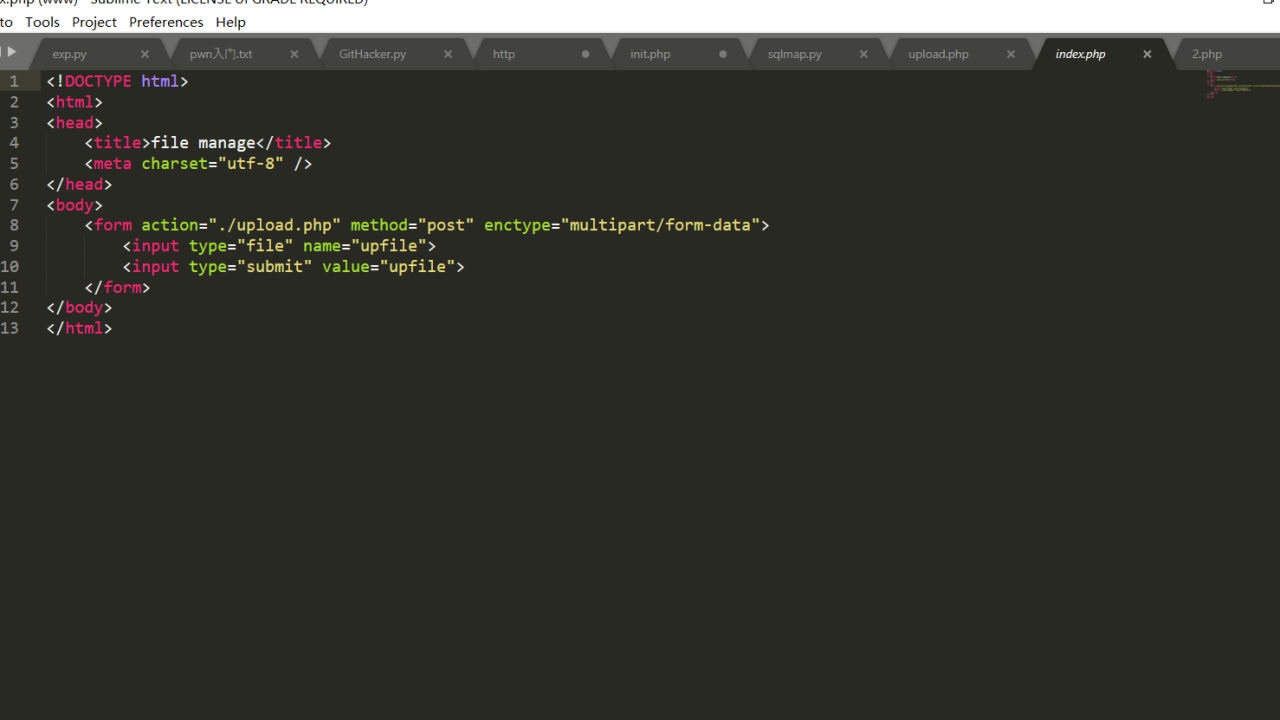
**网站备份源码泄漏。**



**下载，变成php代码审计**



**先看index**



**指向upload**



**发现与数据库的两个交互点，所以这个题考的不是文件上传**

一个是查询是否已经存在

一个是插入一条数据

**但是都被“addslashes”**

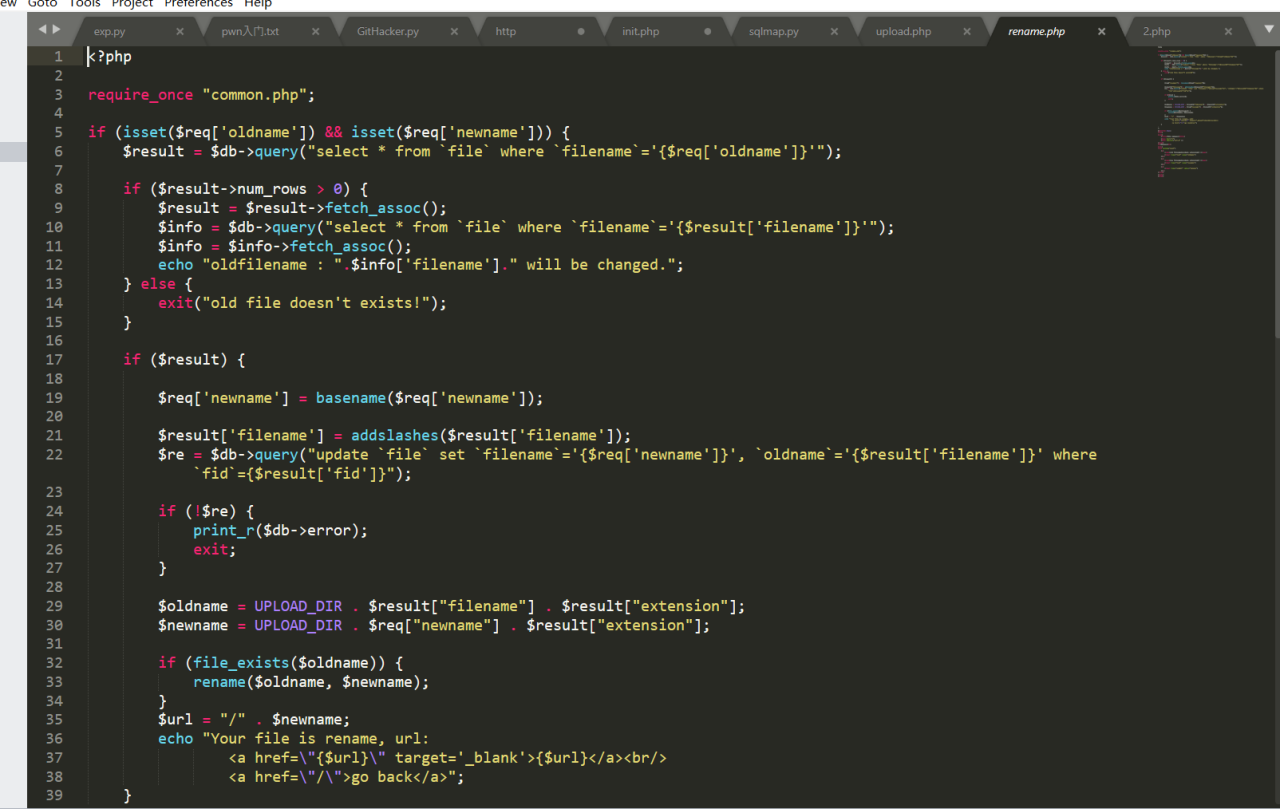
**这里可以尝试绕过，宽字节，url编码，均无效**

所以不能直接注入

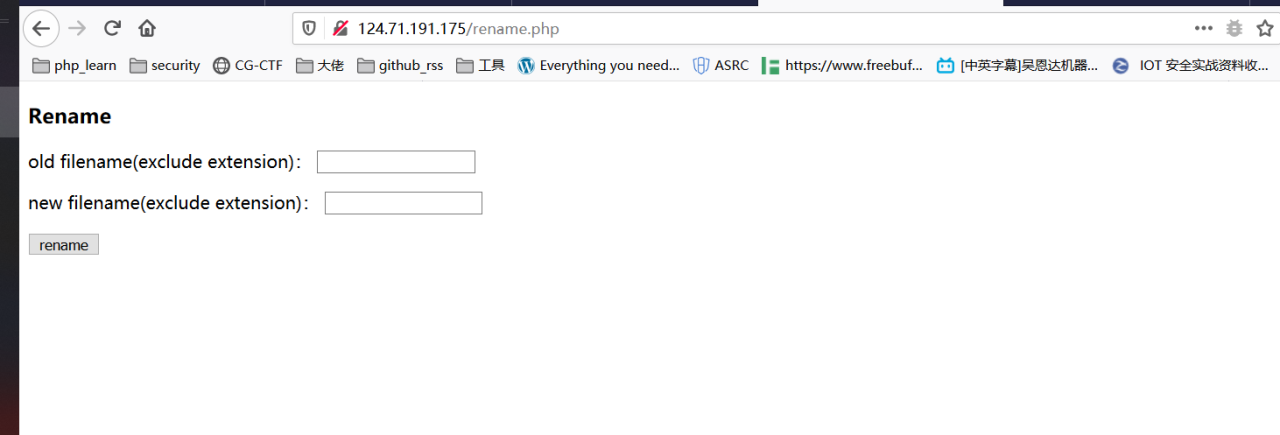
**所以介绍一个“二次注入”** <https://www.cnblogs.com/cute-puli/p/11145758.html>。

**这里的二次注入讲解一下：**

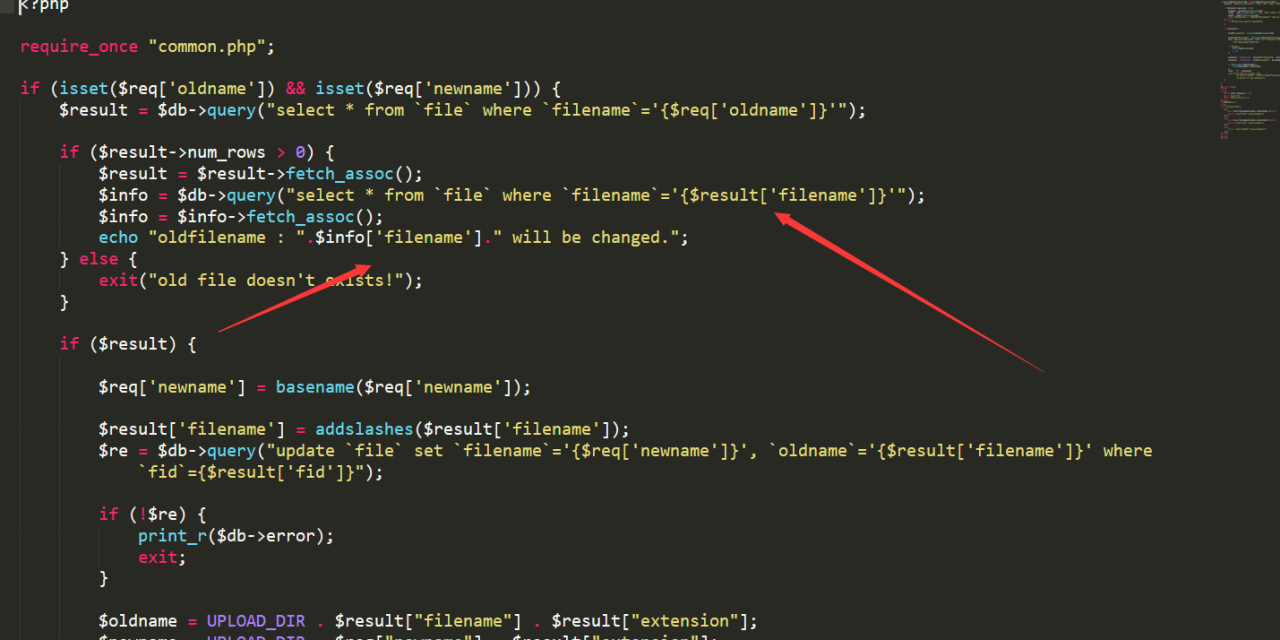
你的addslashes把像单引号‘这样的数据，变成\’，但是后面你取出来的时候他还是**‘**；



**我们继续看下一个知识点，**

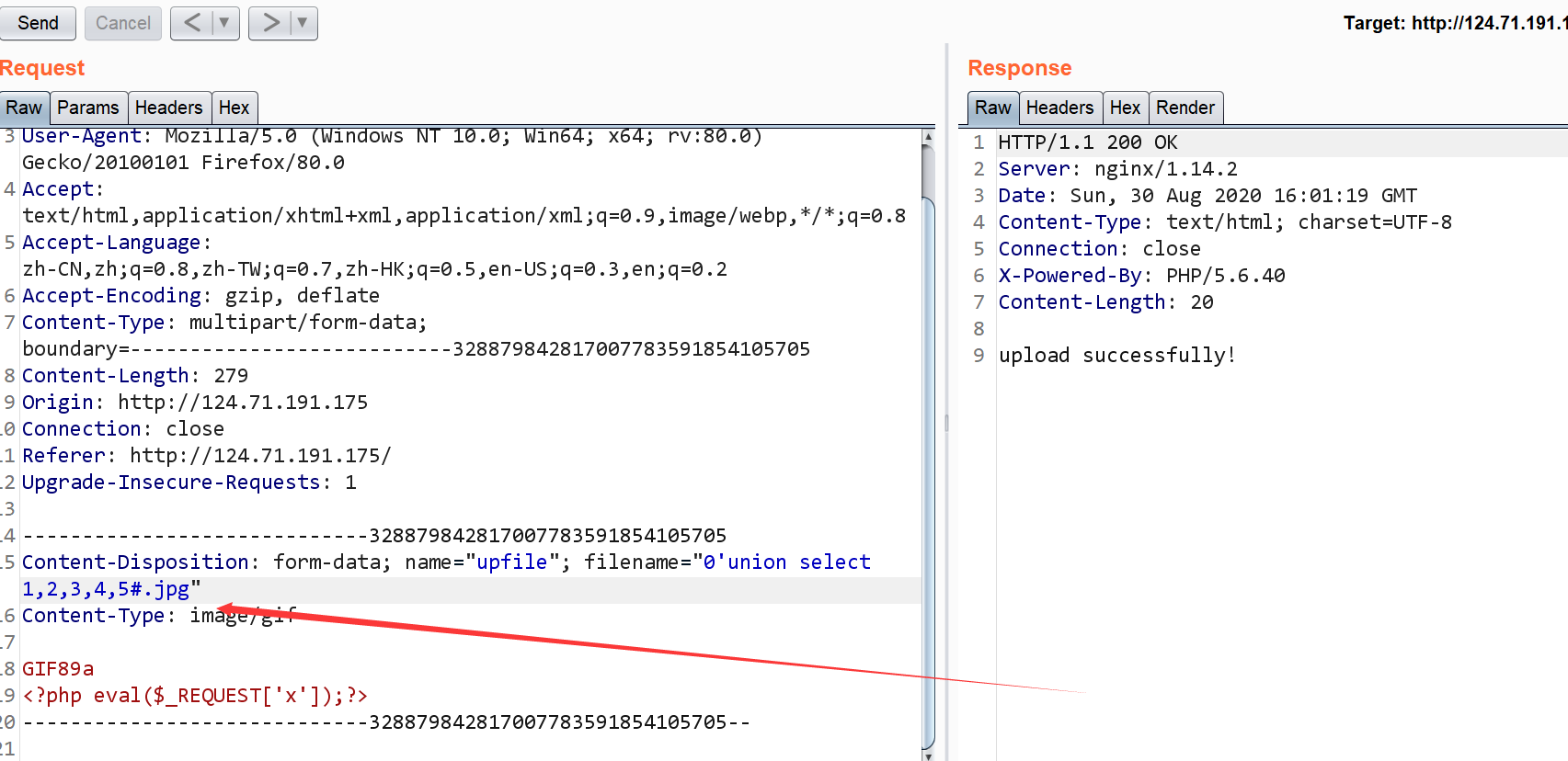


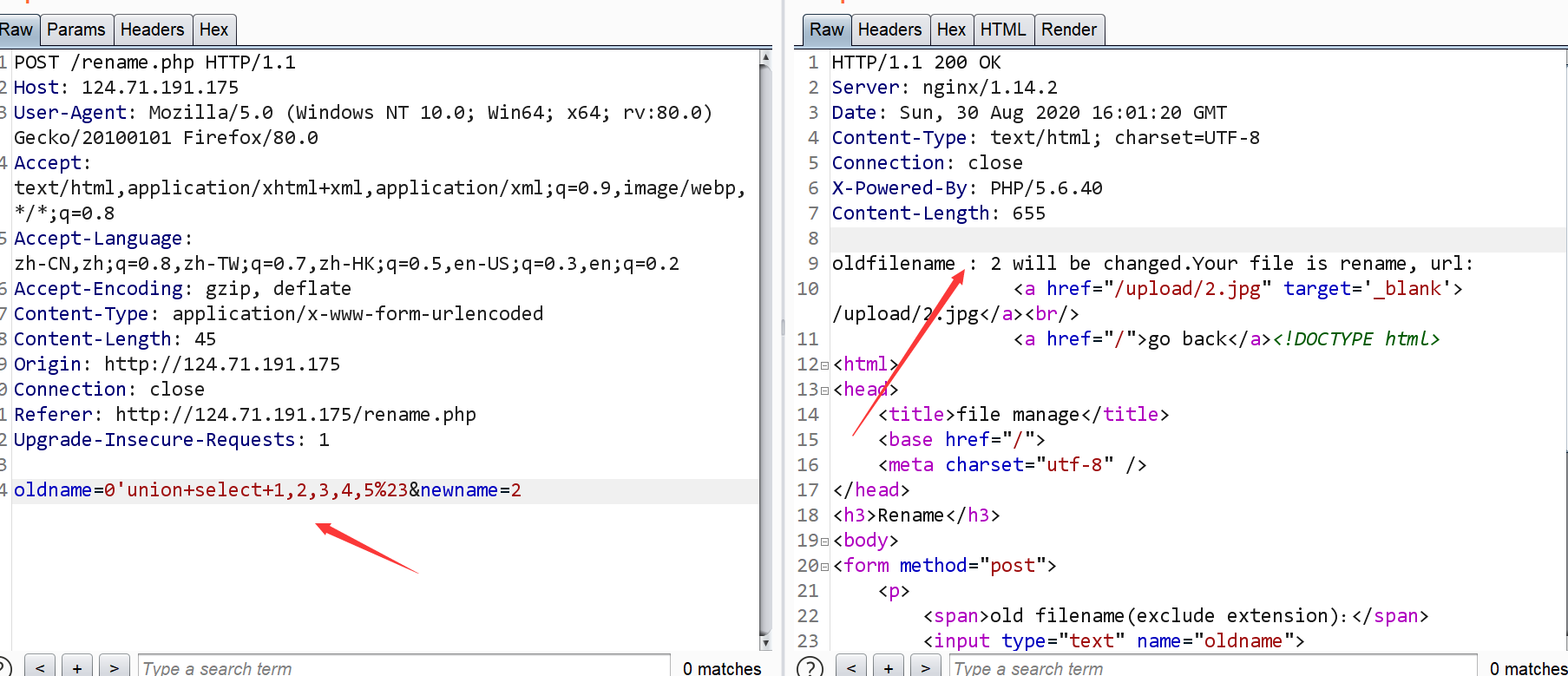
这里可以把文件名发生修改



在取出来时，他没有了“\“。

**所以就可以干坏事了嘿嘿**





**后面就是常规操作了，这道题只需要爆破出用户名和密码。**

**练习：sql-liabs第24关**