**广州大学学生实验报告**

开课学院及实验室：计算机科学与工程实验室电子楼416A室 2023年6月13日

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 学院 | 网络空间安全学院 | | 年级、专业、班 |  | 姓名 |  | 学号 |  |
| 实验课程名称 | | 网络空间安全综合演练 | | | | | 成绩 |  |
| 实验项目名称 | | RCE漏洞利用实验指导 | | | | | 指导老师 | 鲁辉 |

**一、使用仪器、器材**

虚拟机：Vmware

操作系统：windows 系统

运行环境：phpstudy

**二、实验内容及原理**

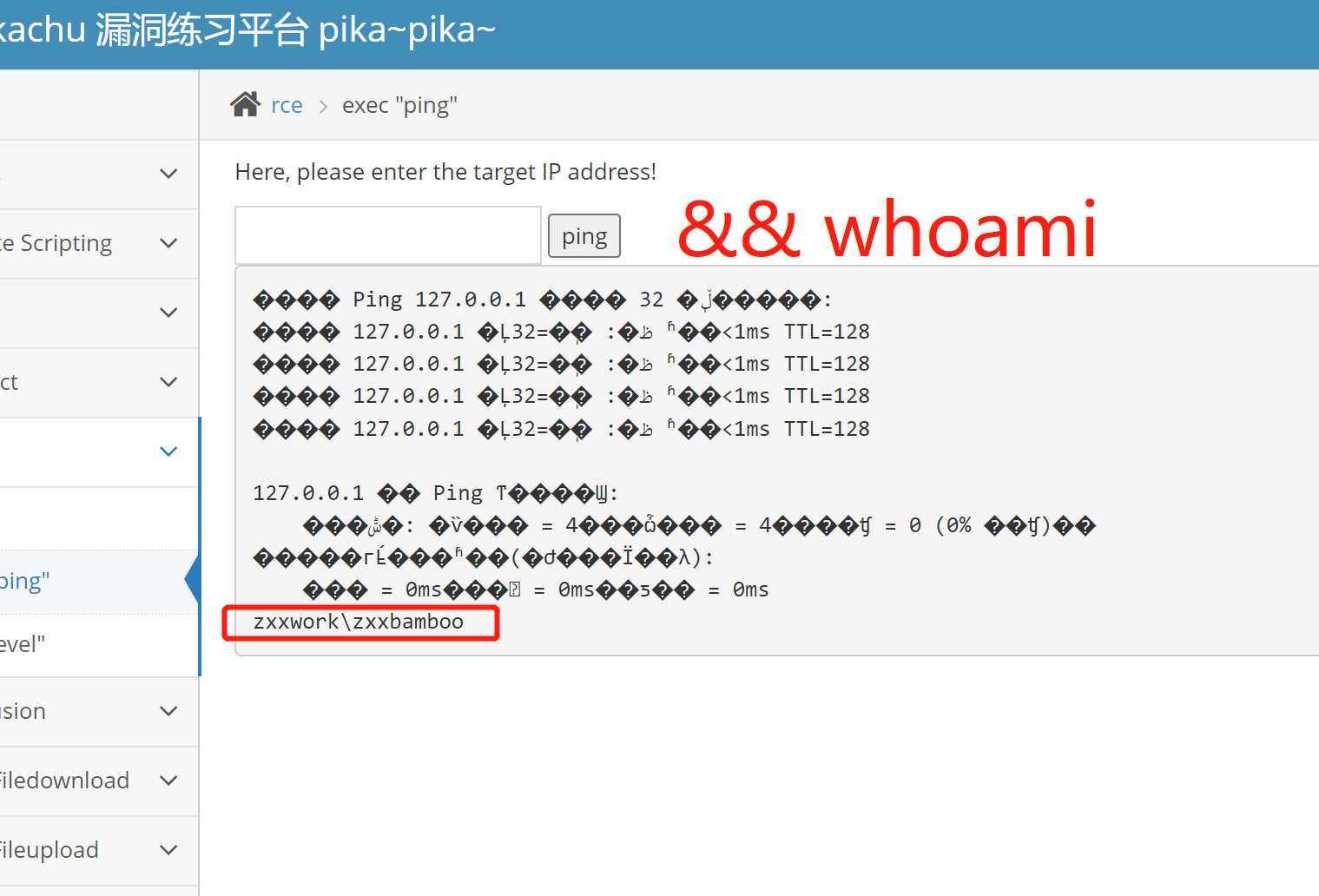
RCE，全称Remote Code/Command Execution，远程代码执行和远程命令执行漏洞。  
在很多Web应用中，开发人员会使用一些函数，这些函数以一些字符串作为输入，功能是将输入的字符串当作代码或者命令来进行执行。当用户可以控制这些函数的输入时，就产生了RCE漏洞。  
RCE漏洞是非常严重的安全漏洞，一旦出现，就意味着攻击者可以获取服务器的命令执行权限，从而对服务器安全造成极大的影响。

1. 在漏洞测试平台 pikachu 上对基础漏洞进行复现和分析。

（2）在学会平台上复现vulhub上的RCE漏洞。

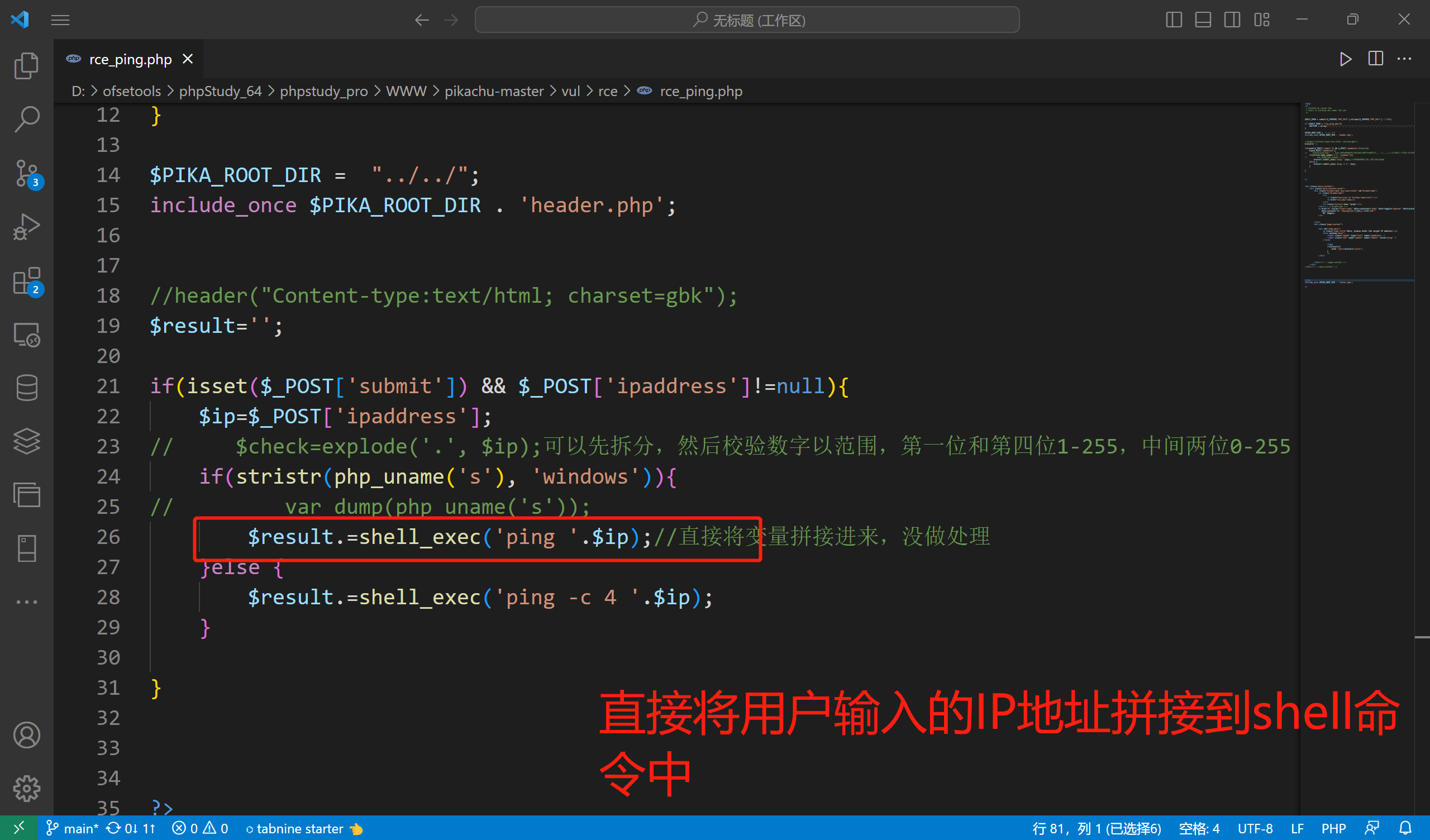


Window



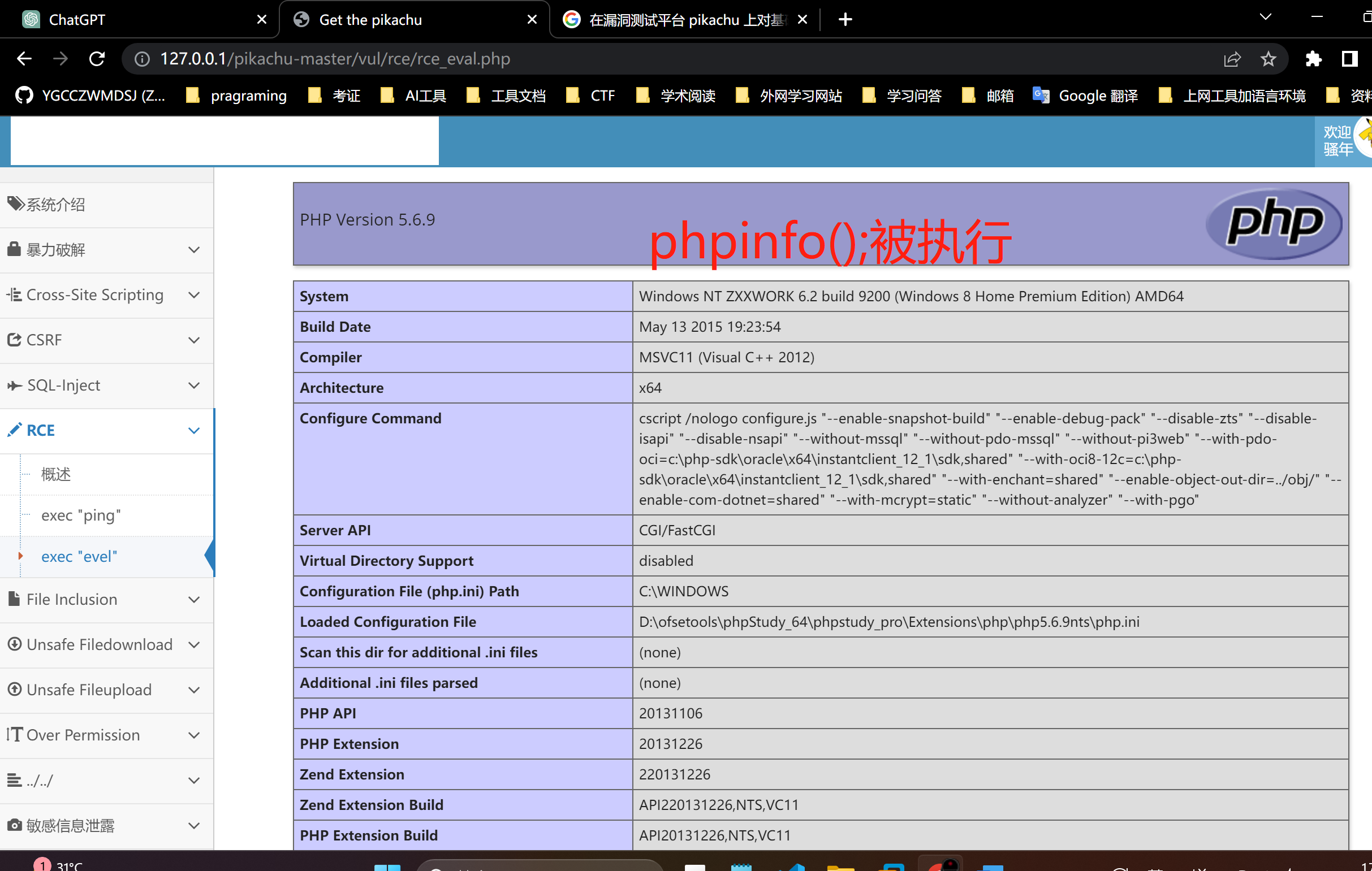


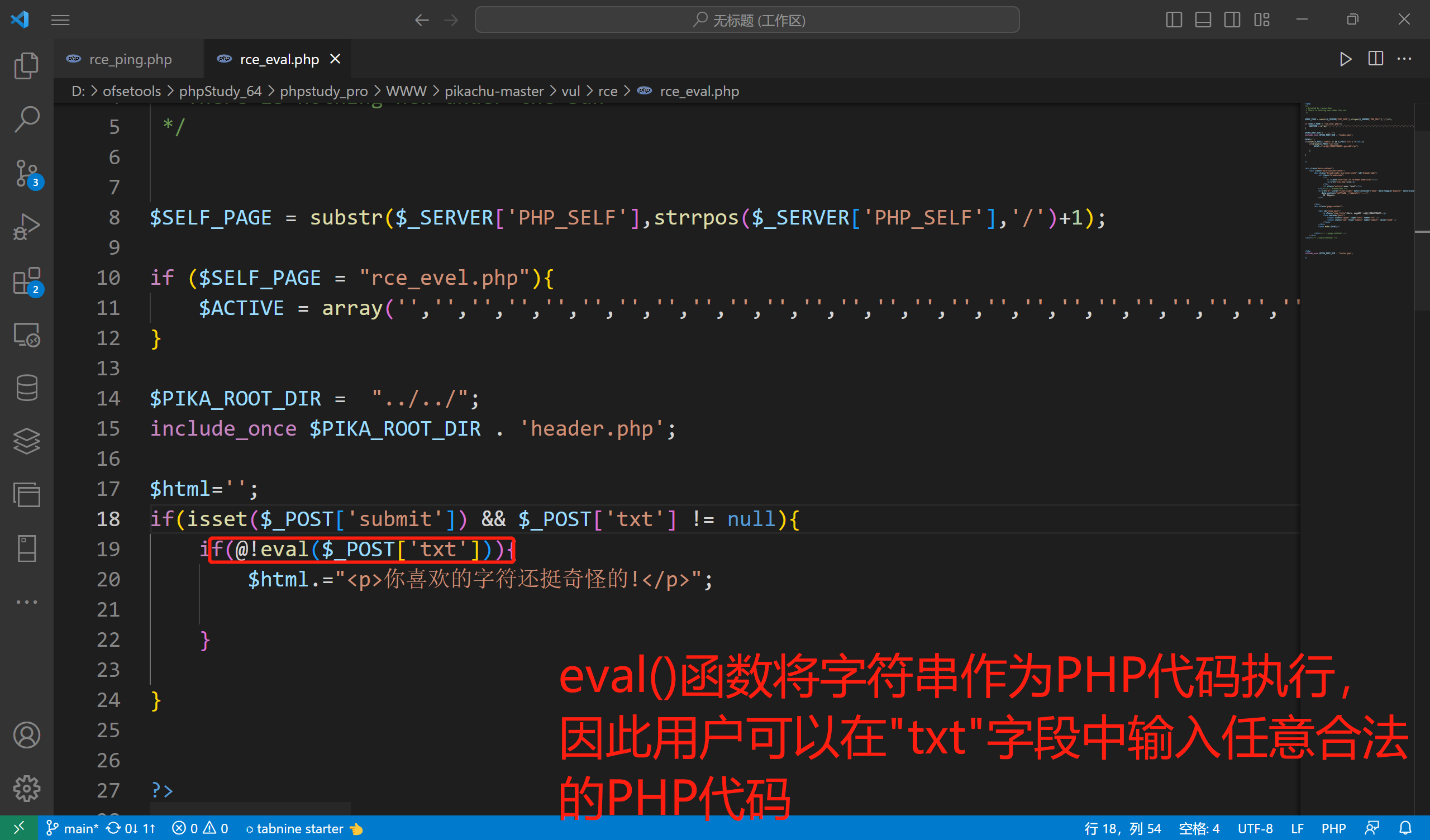




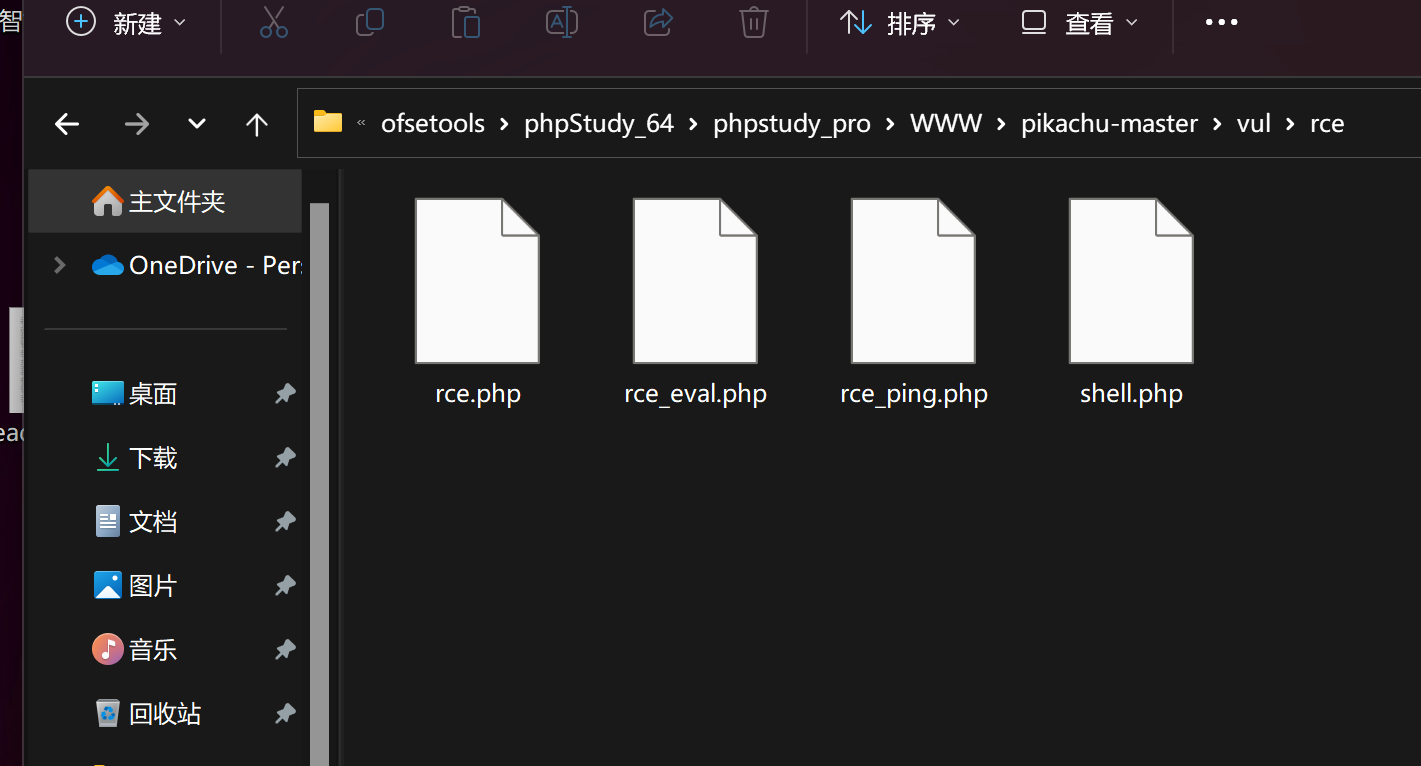
造成注入漏洞

后台将用户的输入作为代码的一部分进行执行，造成远程代码执行漏洞



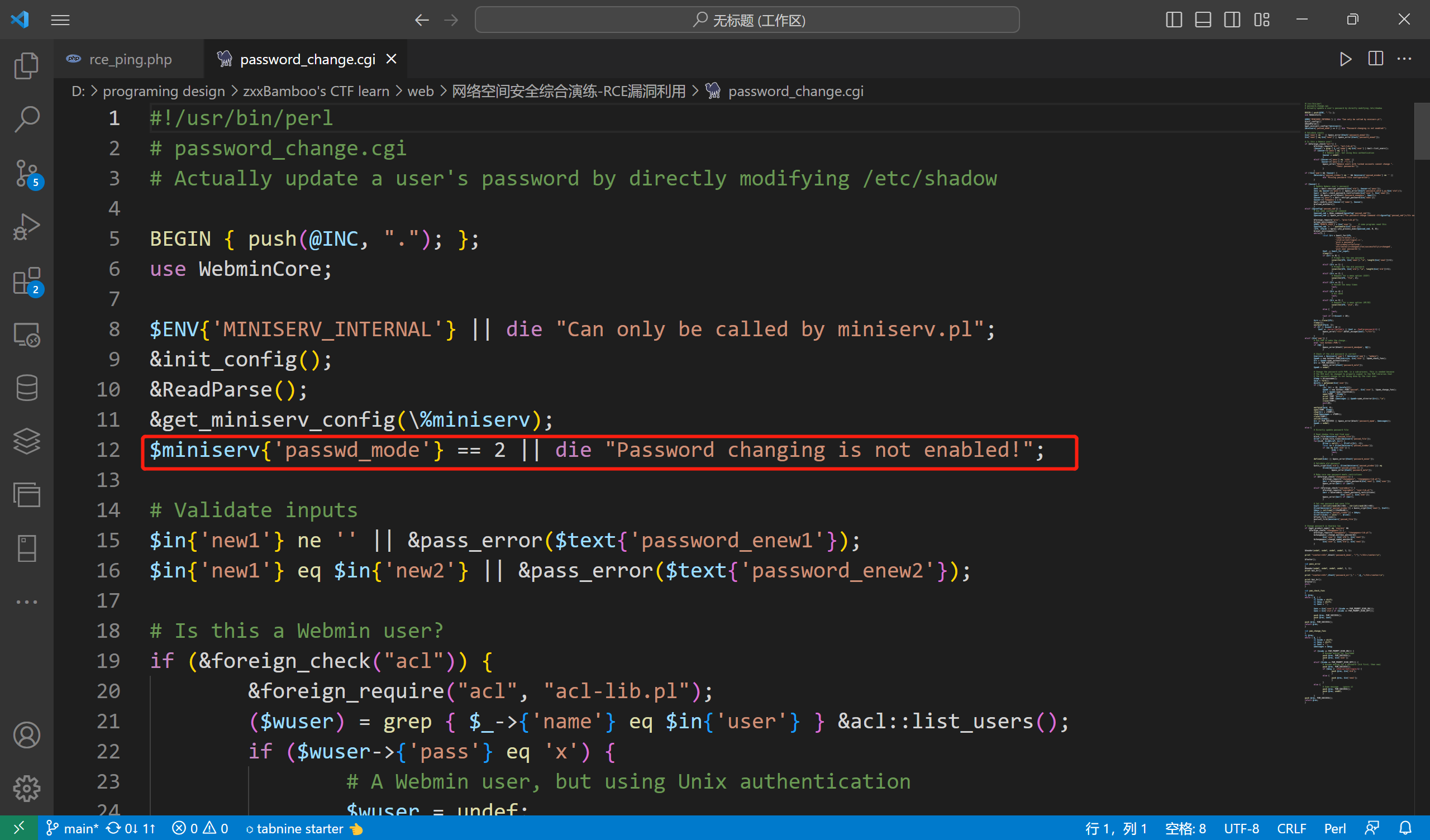


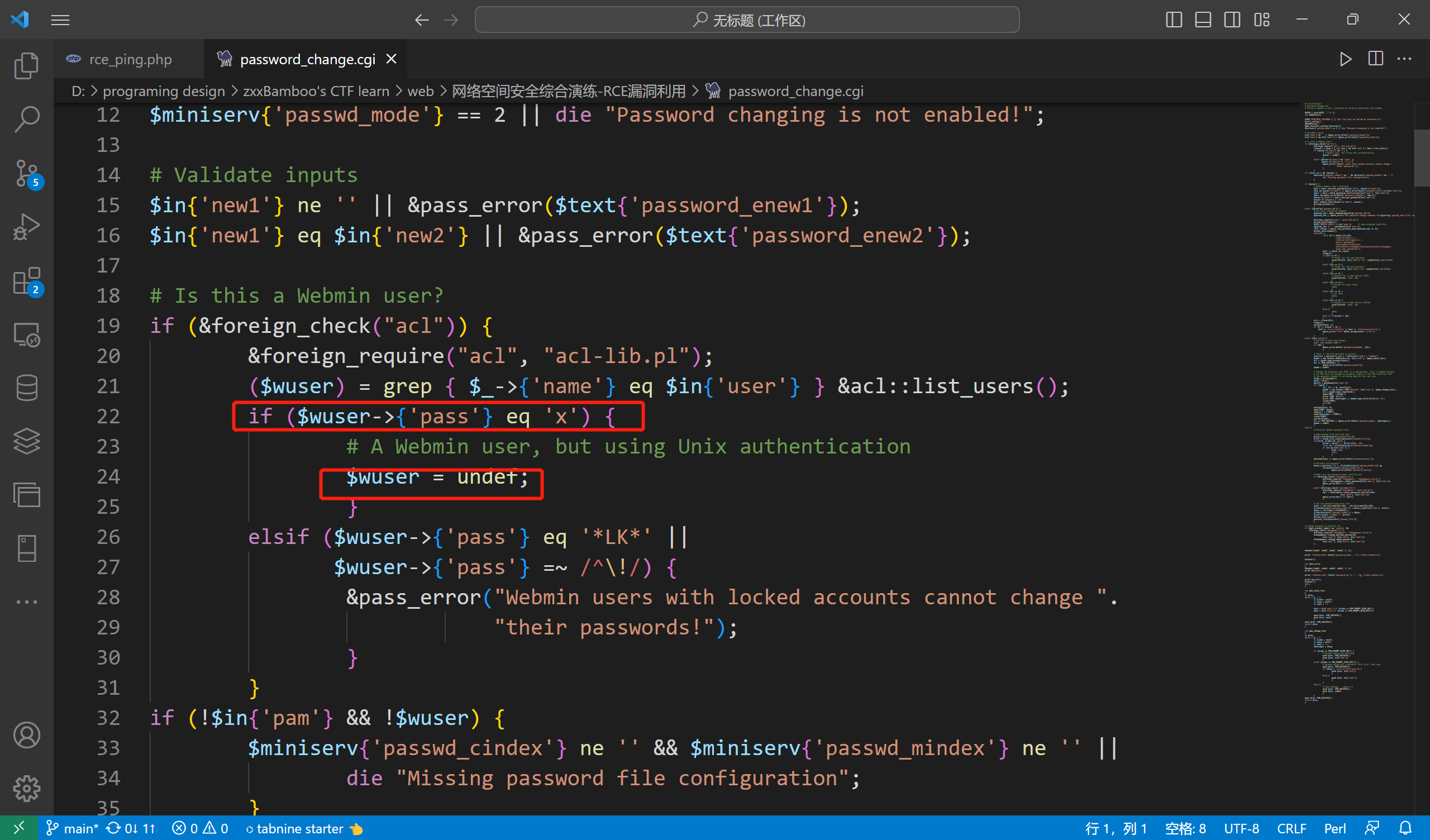


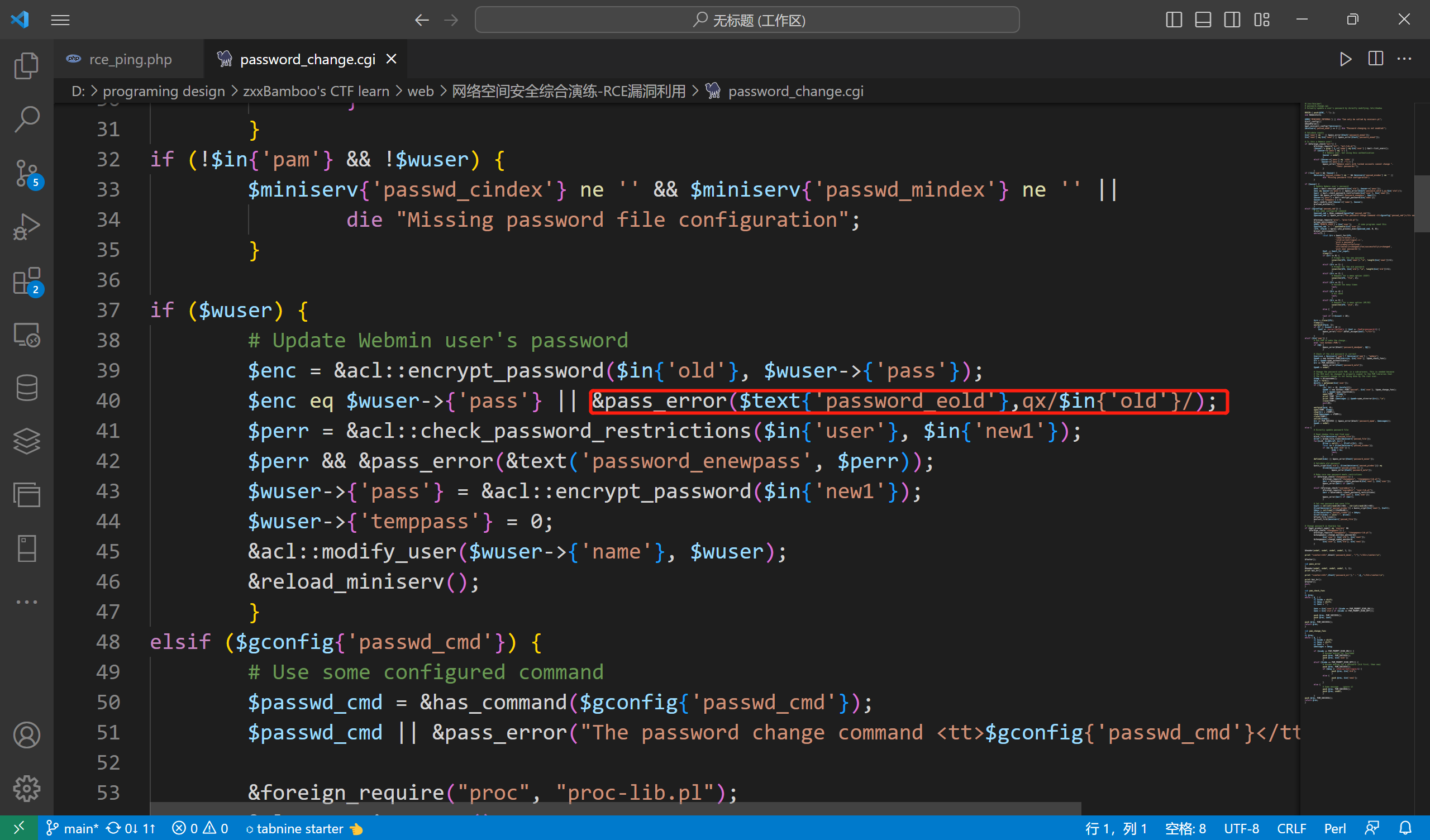


本地目录木马上传成功

1. 使用虚拟机搭建vulnhub的靶机并利用rce漏洞getshell。（选做）







**三、实验总结**

1、成功用漏洞平台和源代码审计发现并利用RCE漏洞

2、