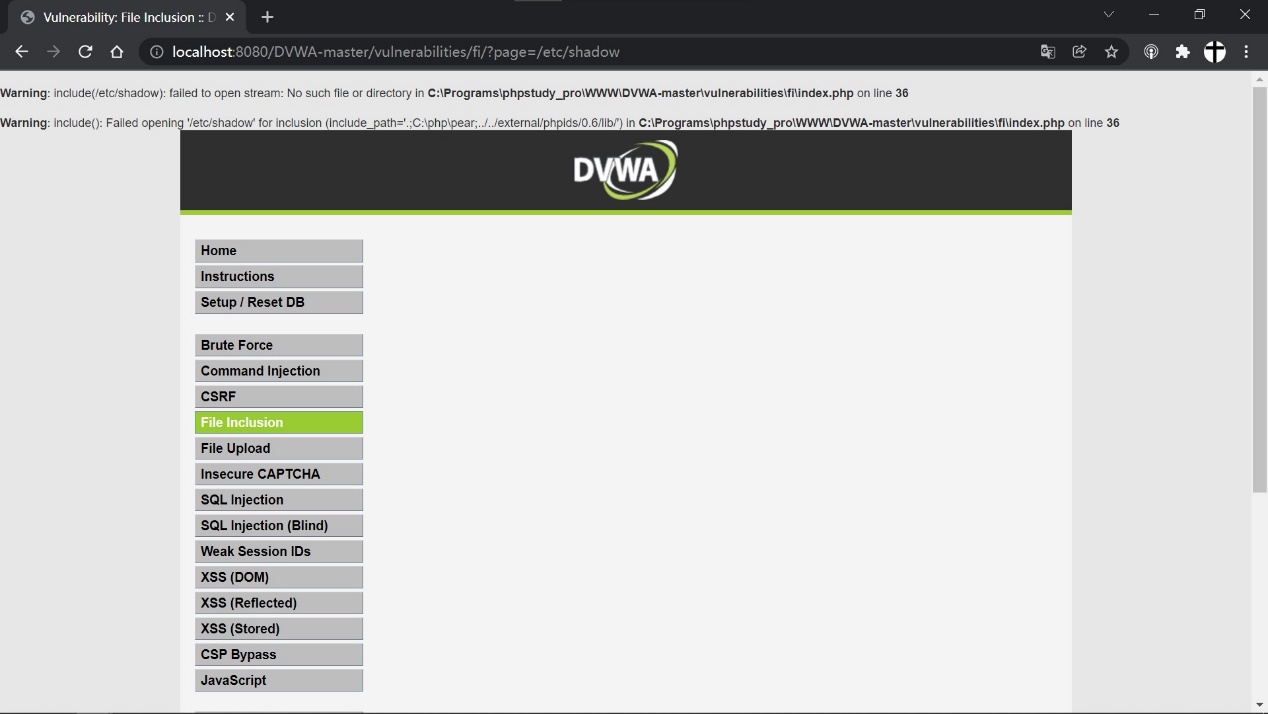
## 一 文件包含

在DVWA的file include界面进行攻击；在php\_study内置的php配置文件中修改allow\_url\_include项使服务器能够对本地和其他服务器上的文件进行检索和使用；使用linux下目录进行测试，返回值不存在该文件，故确定靶机为Windows系统。



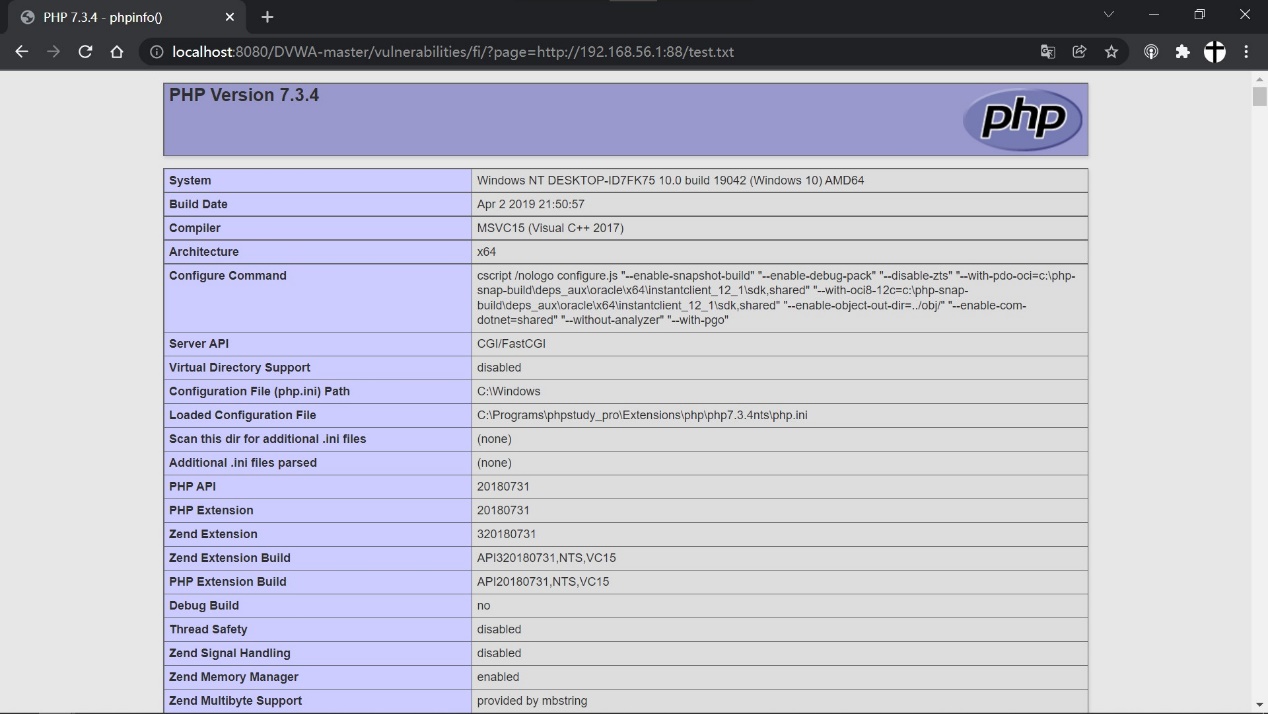
### 本地文件包含

上传恶意php文件后，利用上述漏洞进行访问执行。



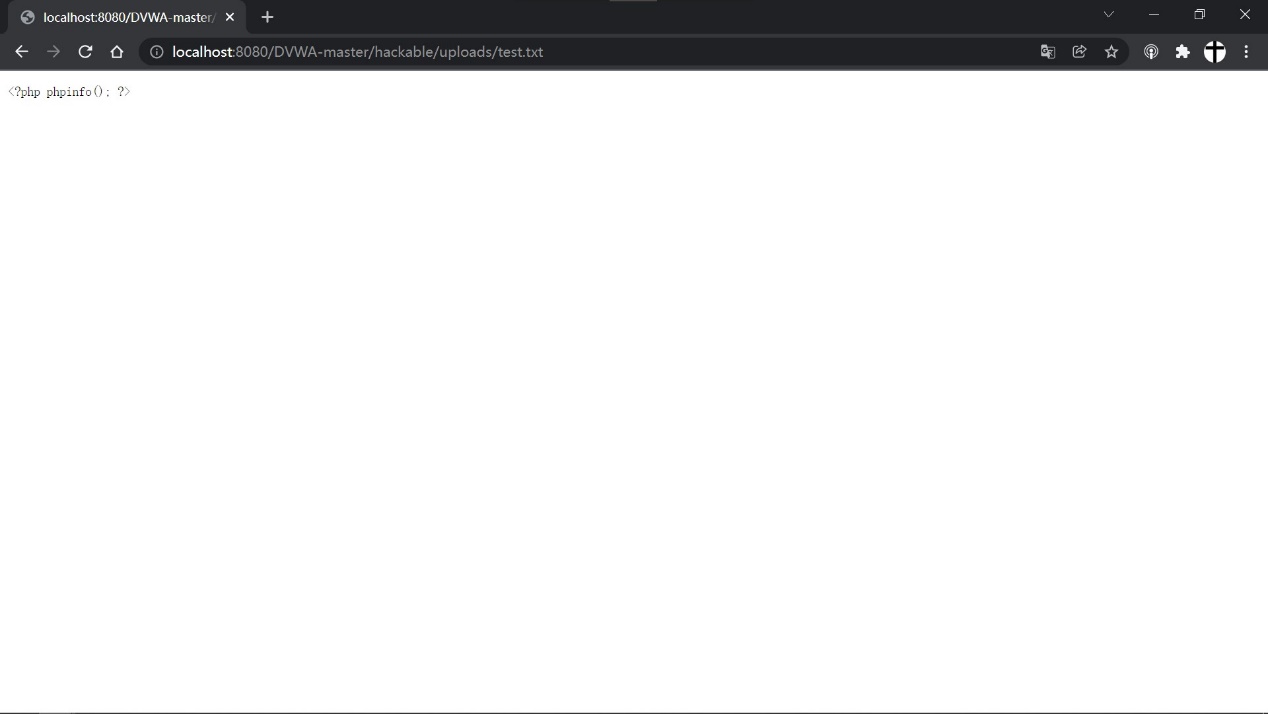
### 远程文件包含

利用php的url\_include函数功能，使靶机远程调用服务器上的文件。

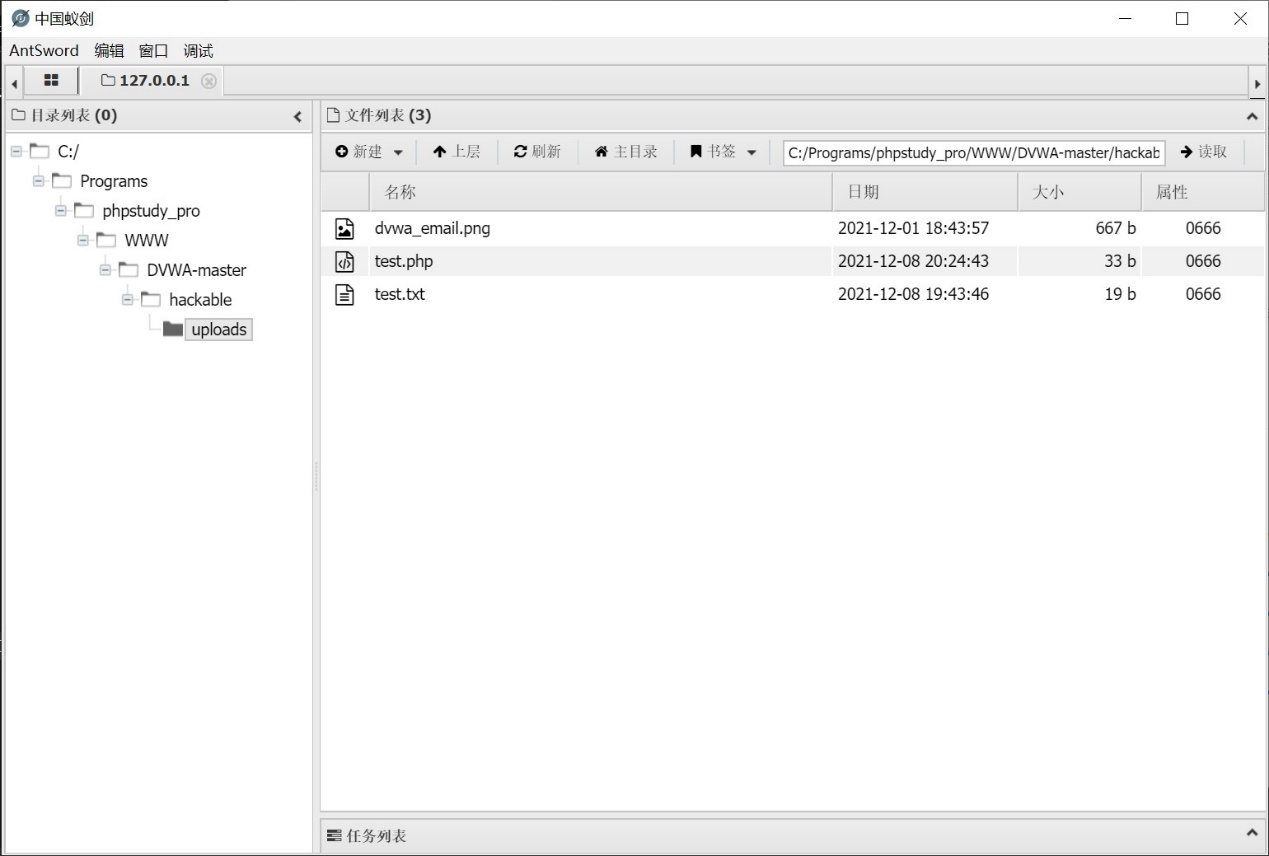


## 二 文件上传

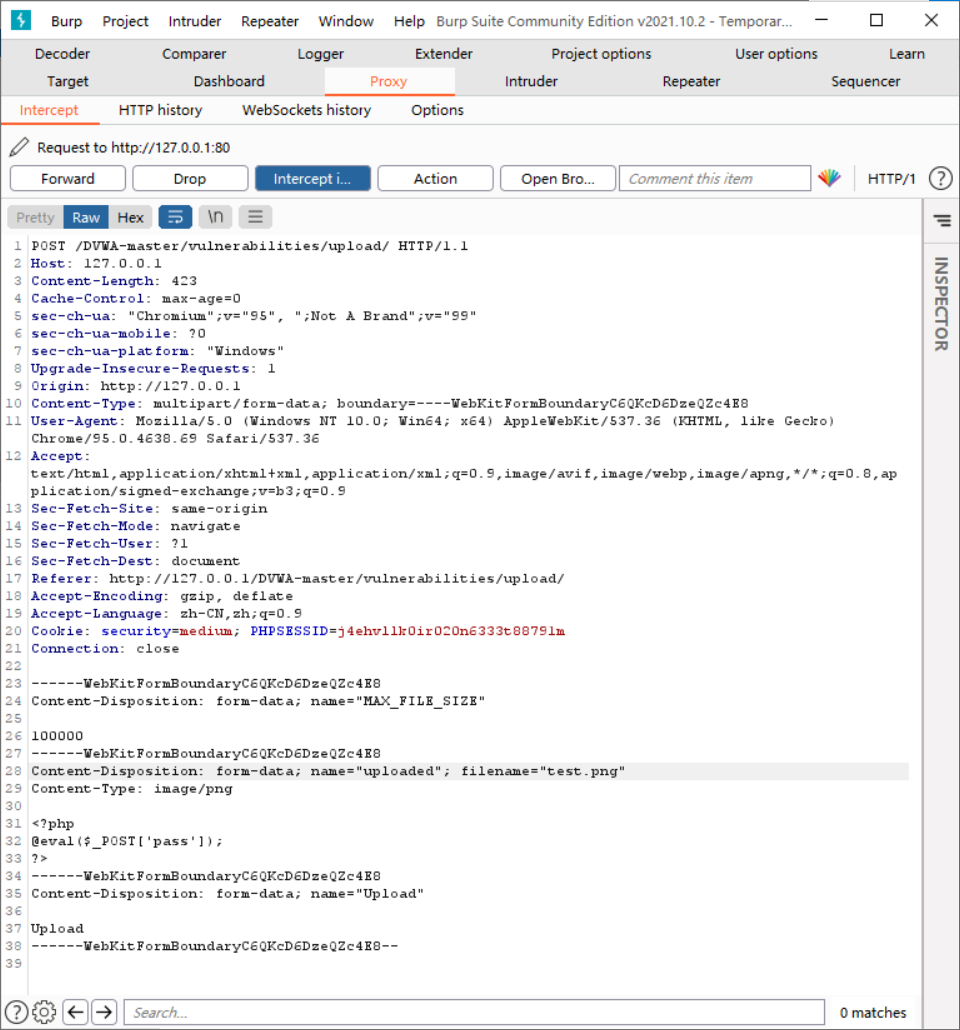
随意上传一个文件后，页面直接返回了上传后文件在靶机上的相对路径，故构造上传test.php文件，使用文件包含漏洞进行执行。

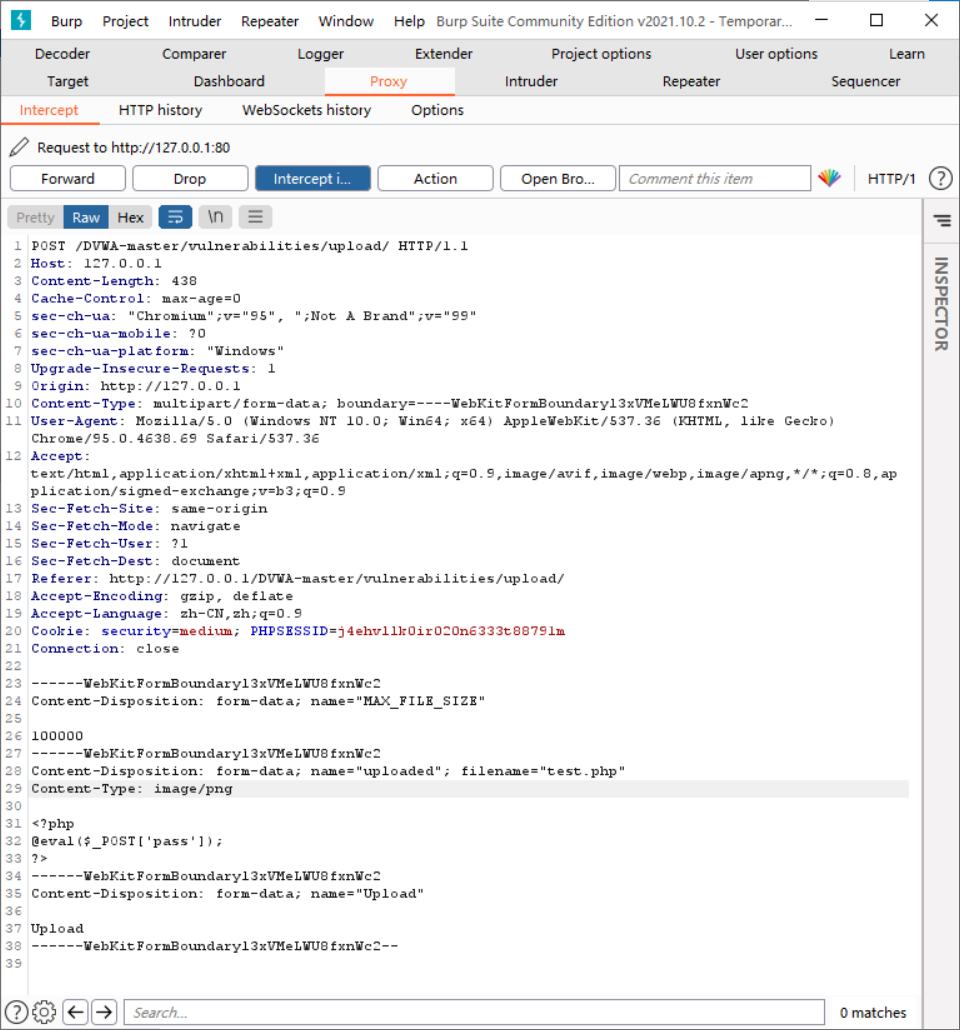


使用中国蚁剑进行文件上传漏洞的利用。



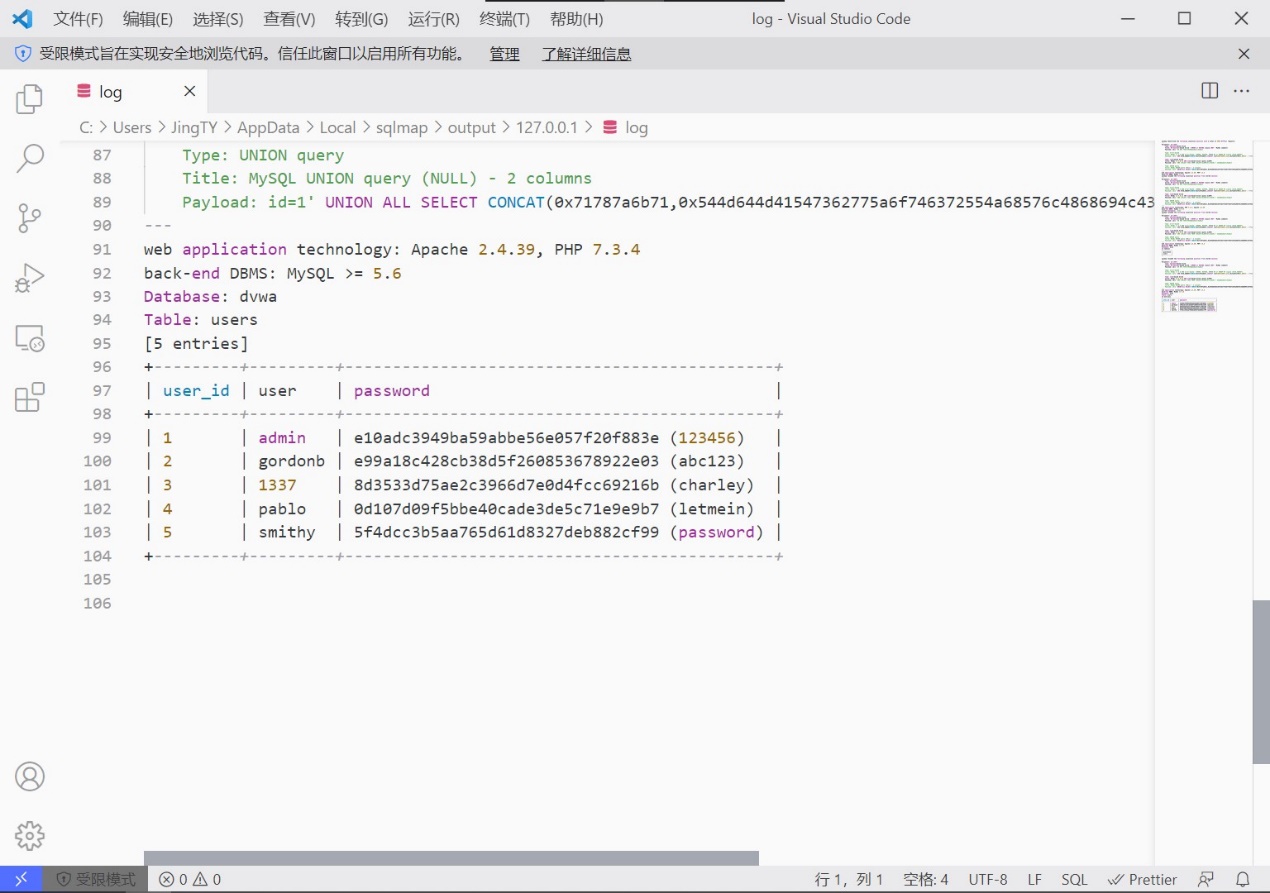
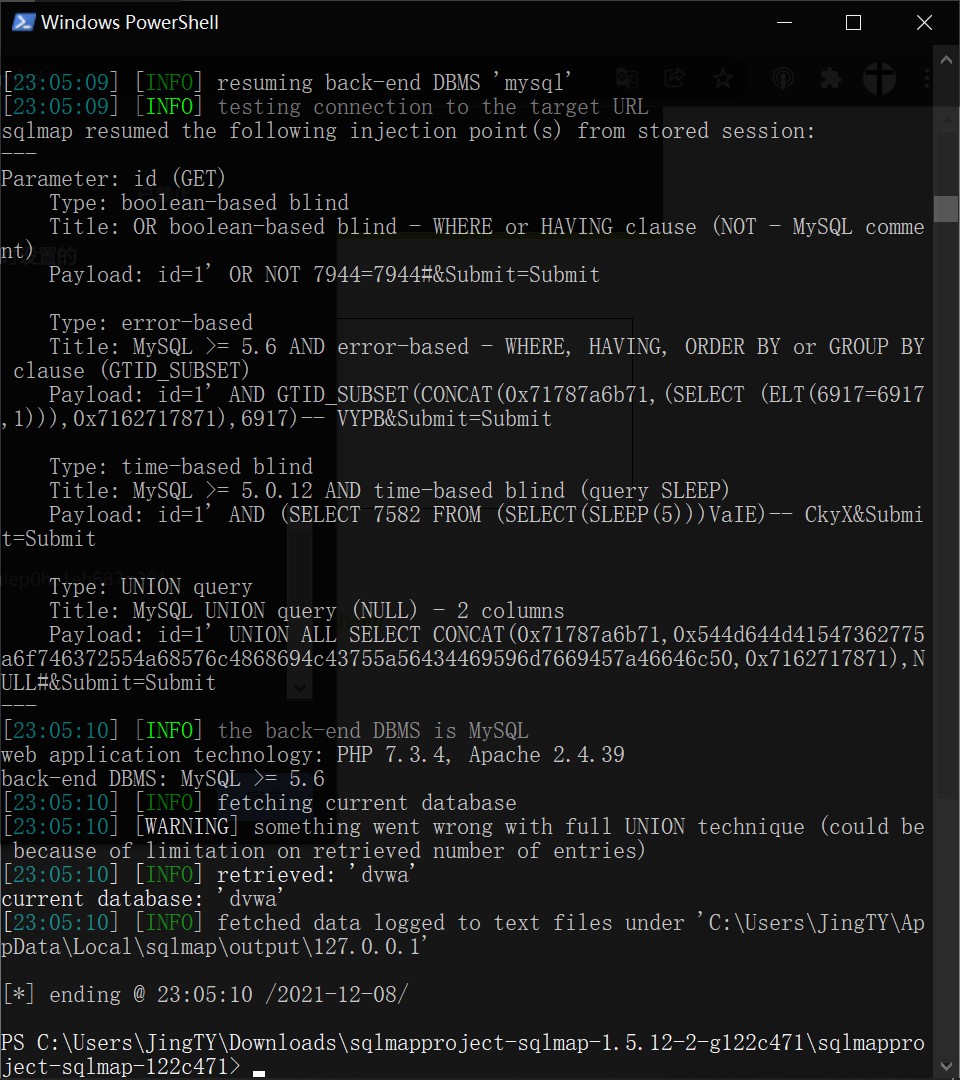
Medium难度下，前端发送http请求时会堆文件类型进行检测，故使用burpsuite抓包，修改请求。分为修改请求中的文件名后缀和修改文件类型两种方法。



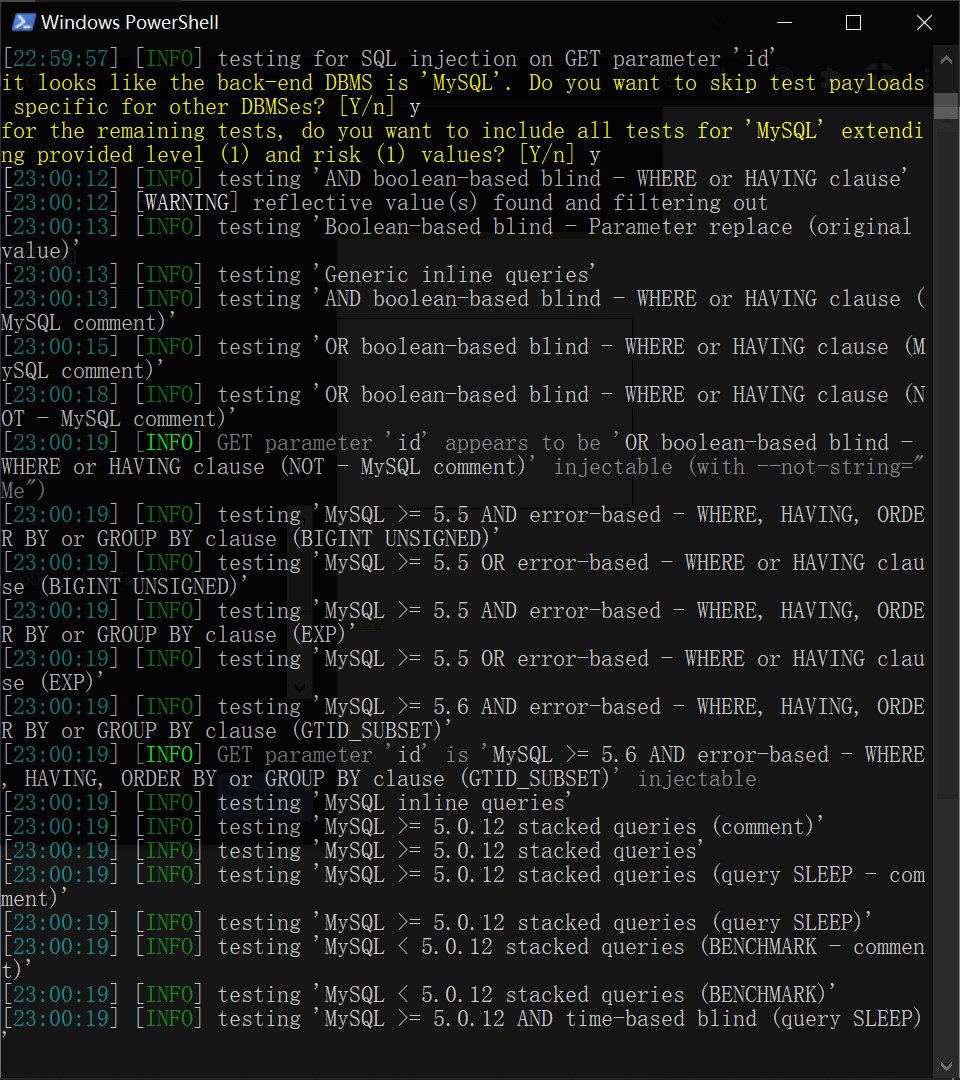
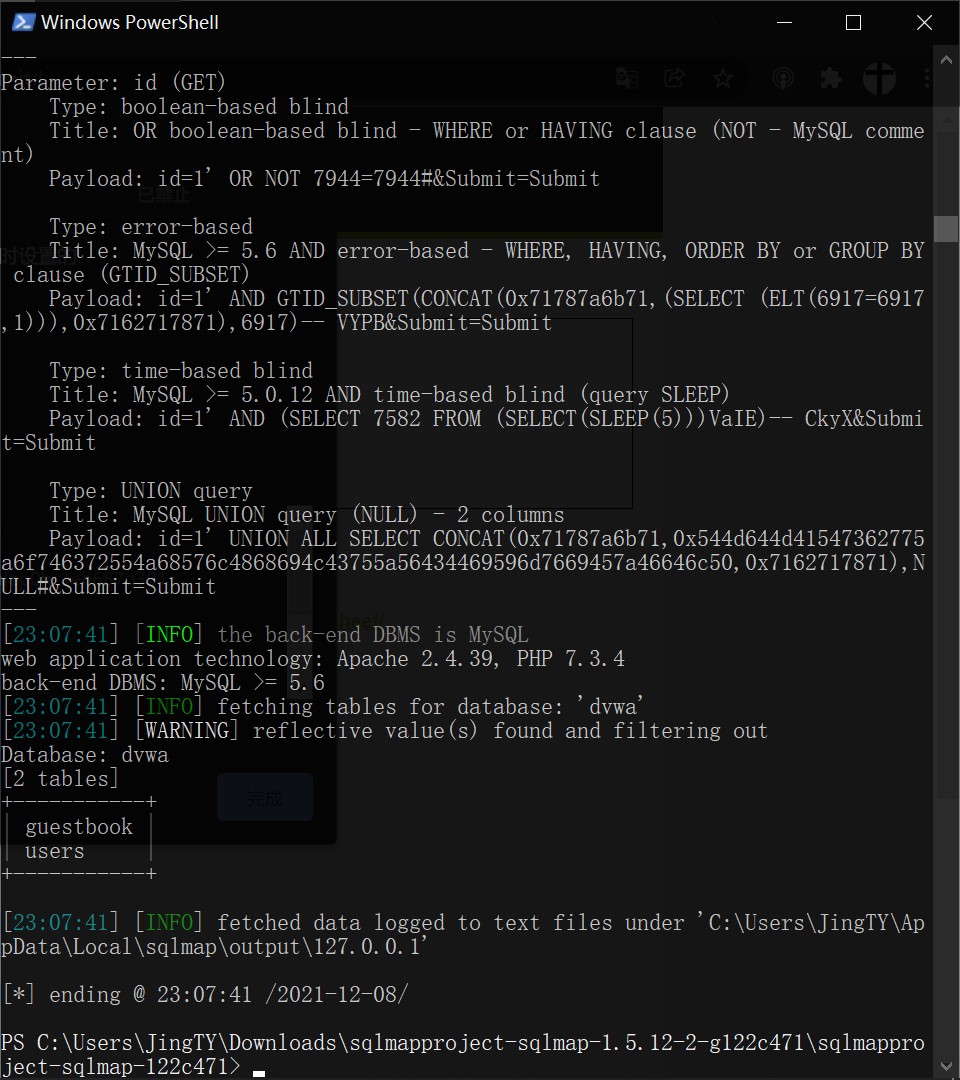


## 三 SQL注入

使用sqlmap进行sql注入。Sqlmap的功能非常强大，可以自动检测版本，自动爆破，自动获取项和表，搜去关键信息等。



获取关键table的值并打印



## 四 小结

本节课主要进行了文件包含，文件上传，sql注入三种漏洞利用的学习，比上节课的实际可行性更高；其中，sqlmap的使用使sql注入的流程有了相当的简化，但想使用好这几种工具需要下不小的功夫。