writeup

原创

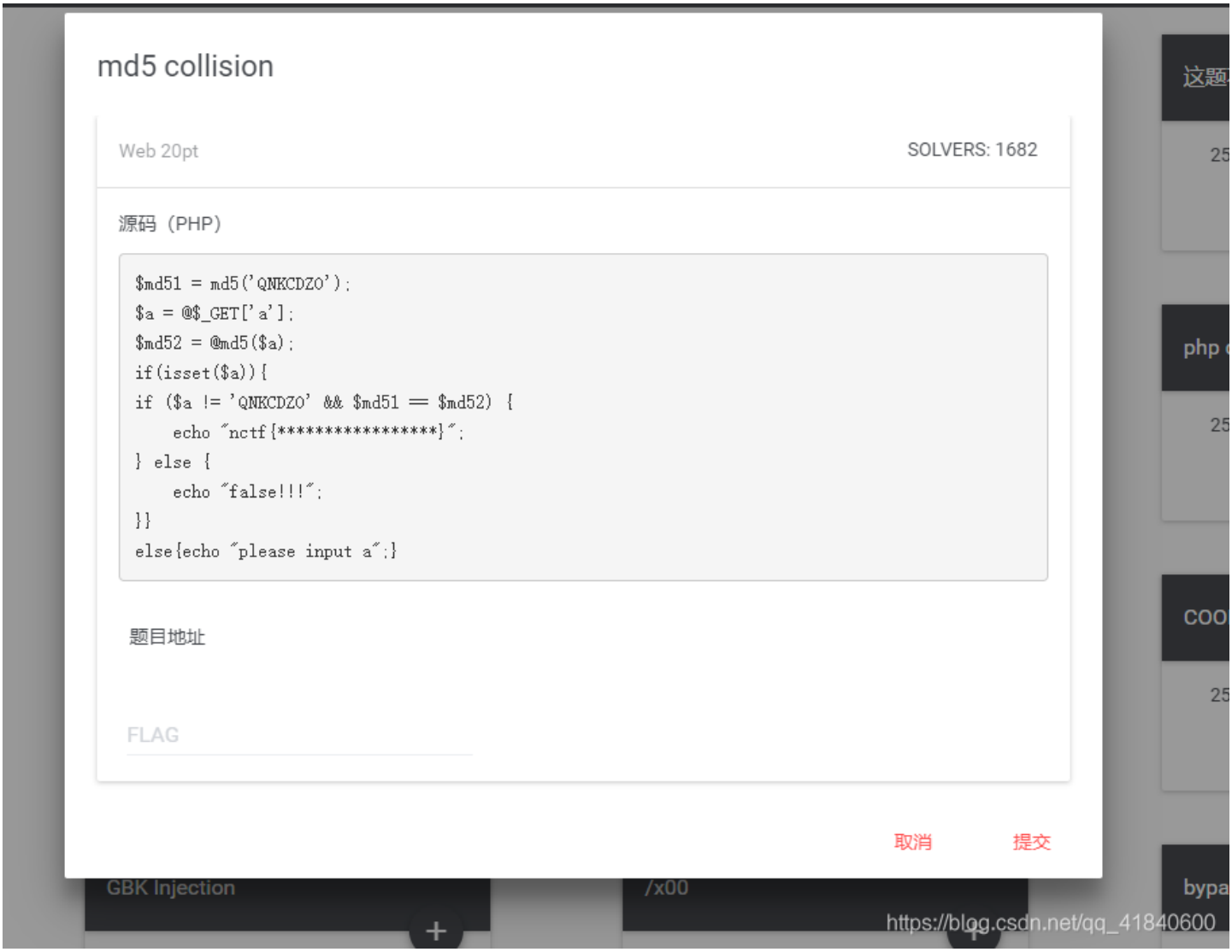
写不出代码的码农 于 2019-02-28 21:52:39 发布 300 收藏

分类专栏： 菜鸡啄米

本文链接：https://blog.csdn.net/qq_41840600/article/details/88045933

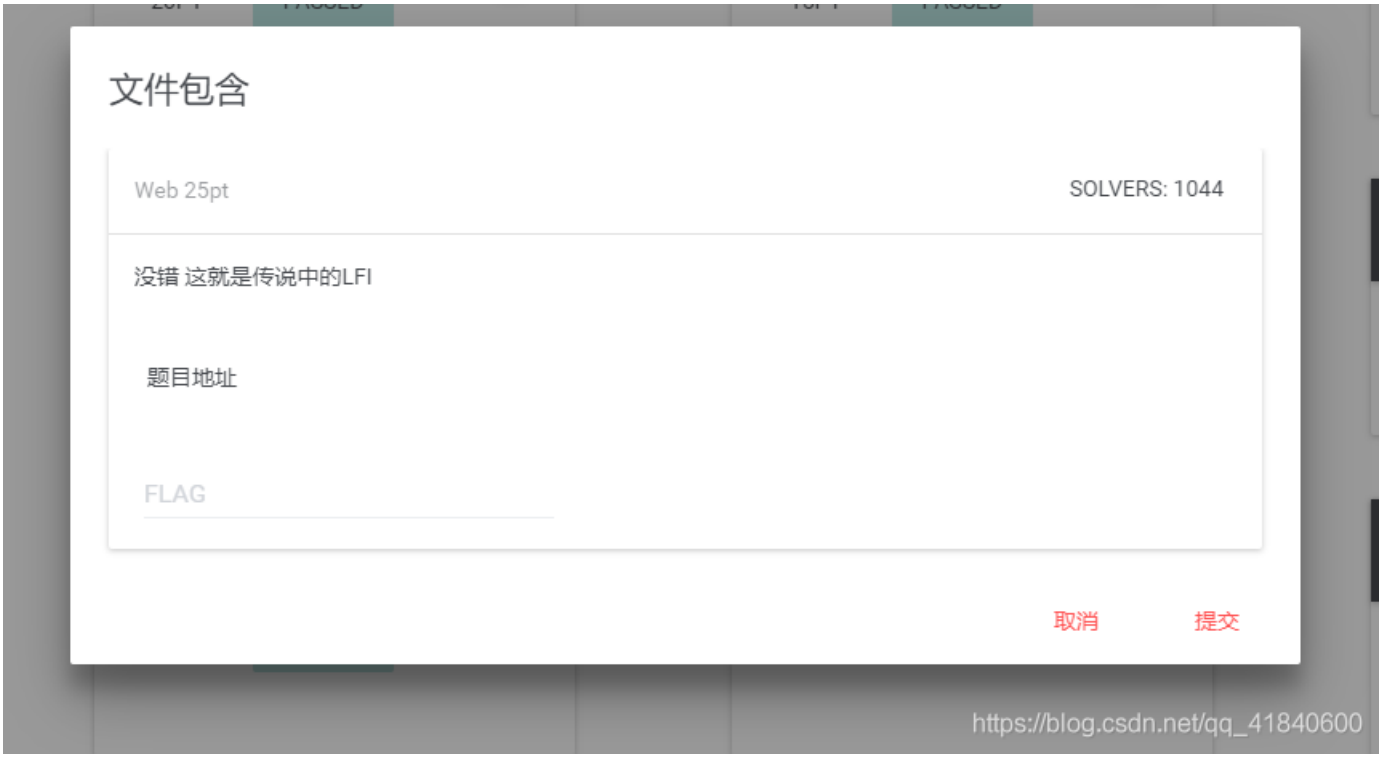
硬盘炸了，临时凭记忆写了一点。。。

1、md5碰撞



随后我百度md5值，巴拉巴拉一大长串，大概得出MD5值为弱口令，存在md5碰撞的方法，可以做到使头部相等得到*对应的flag

2、文件包含



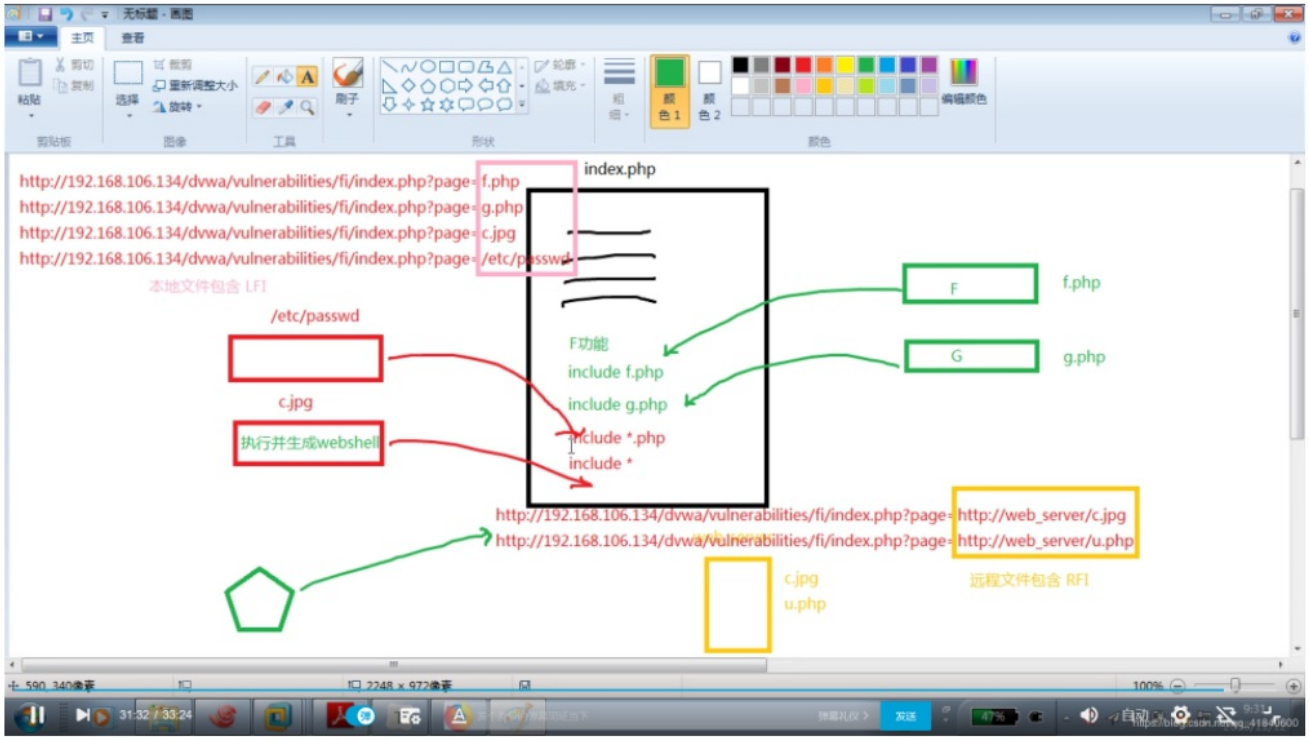
文件包含类似于c中的include作用，开发人员在写代码时要调用多个函数库就可以使用文件包含，文件包含又分为本地文件包含和远程文件包含。

这道题还有PHP的filter协议

https://blog.csdn.net/qq_38183886/article/details/79374951

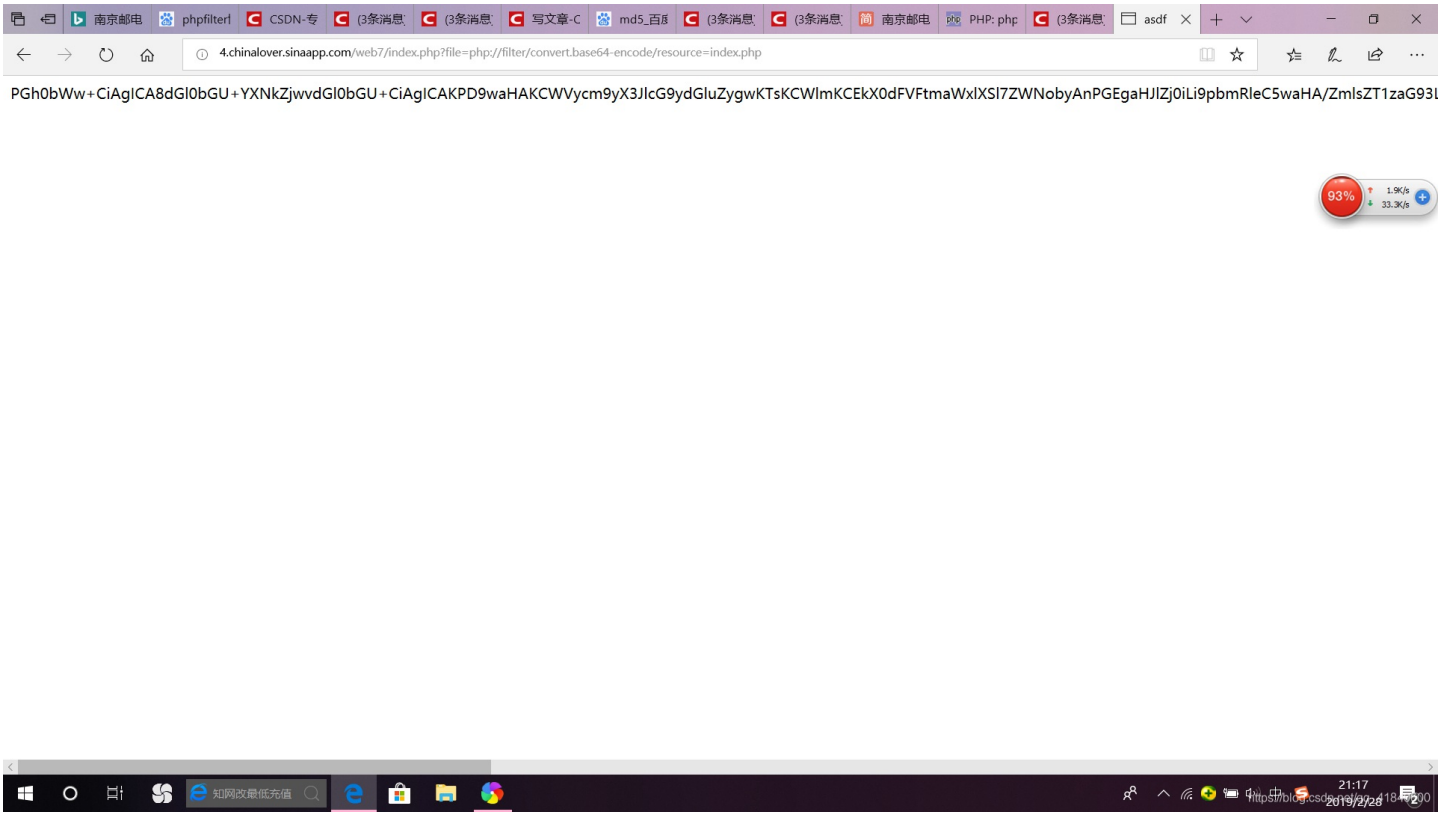
文件包含漏洞

文件包含漏洞又分为**本地文件包含**和**远程文件包含**



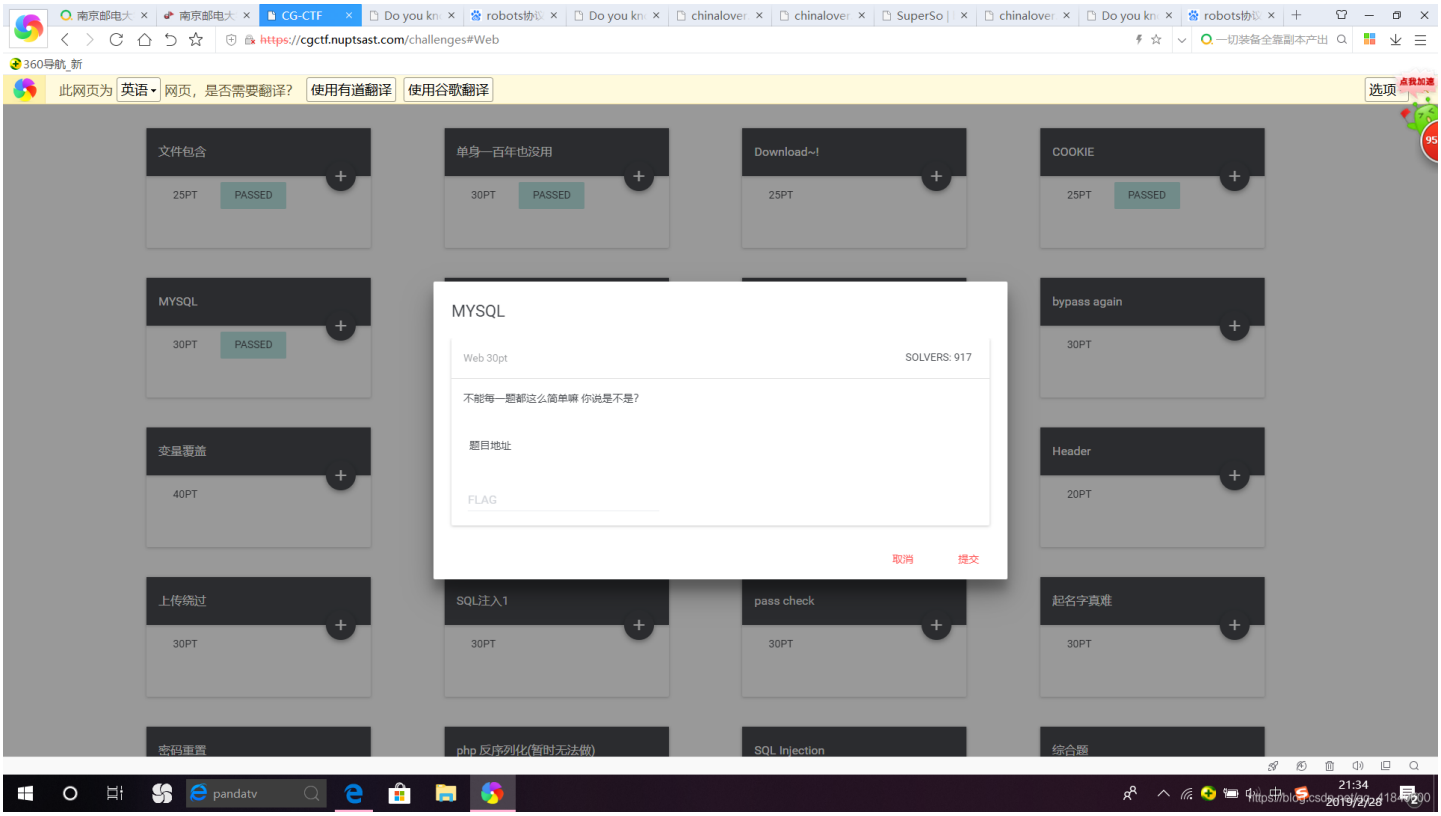
文件包含可类比为c语言中的include ， java中的import语句可以方便开发人员调用函数库

其中本地件包含指的是上传一个含有创建一个php指令的php或txt文件

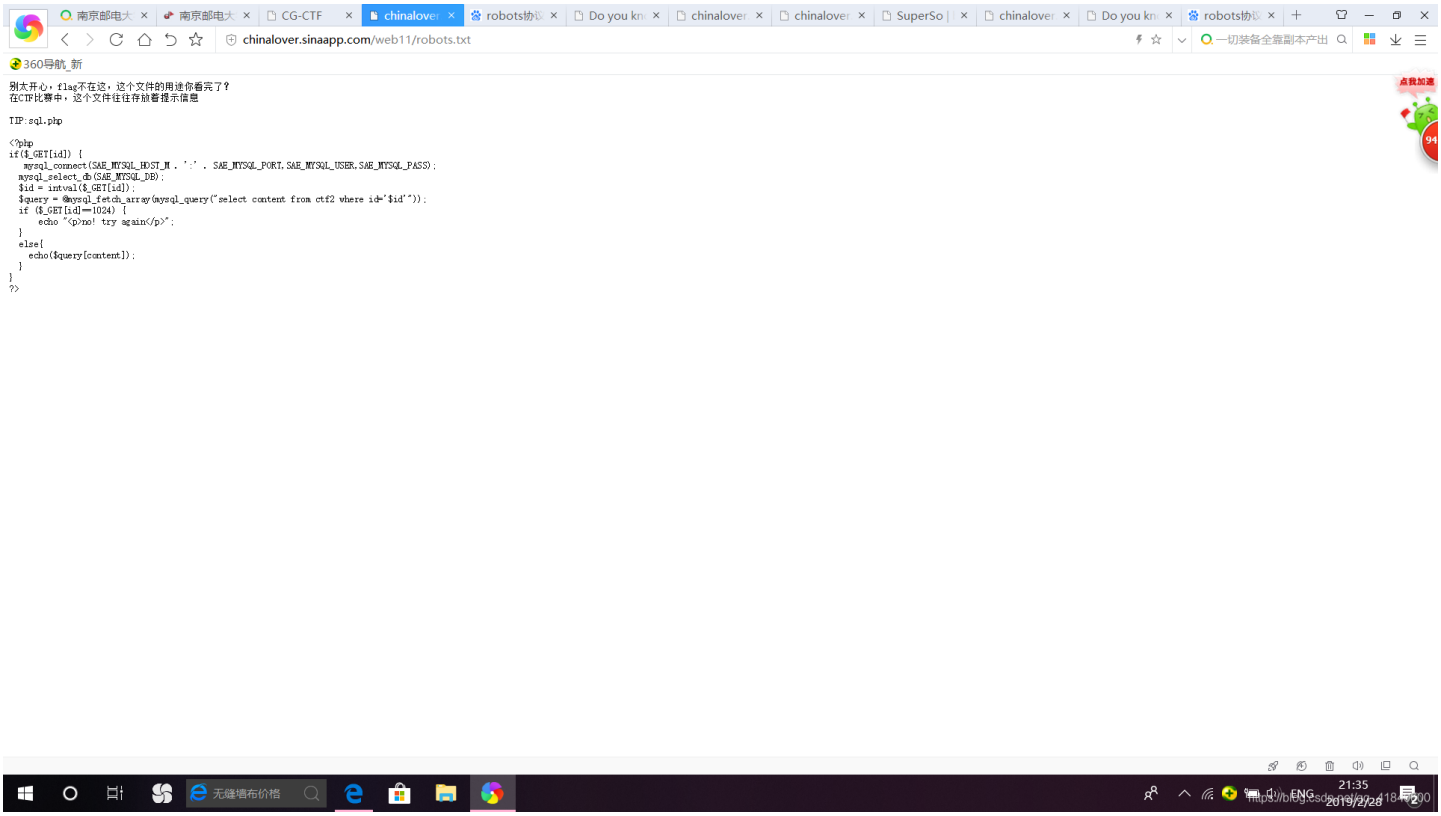


对得到的base64解码得到flag

3、mysql

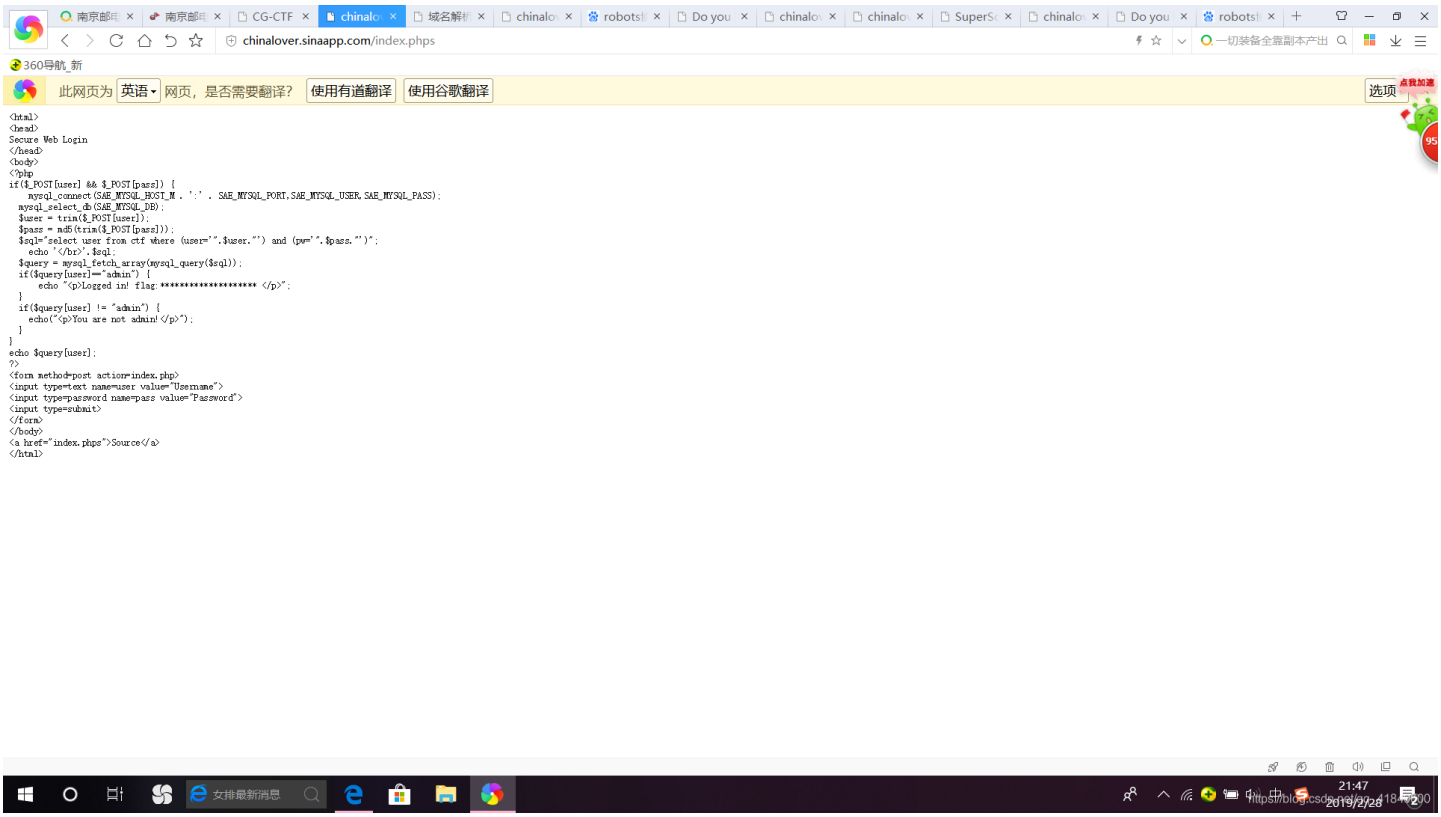


点开后进入一个连接，试一下这个目录发现源码



根据大概意思尝试提交1024，失败，1024.3得出flag。应该是精度问题

4、sql注入



代码的意思就是post user与pass,然后提交post的user必须是admin.但是密码不知道,所以就得在

sql= 这句想办法绕过*and*(*pw*= ” pass.”’) 这段

所以构造的语句就是这样

admin’)#.

得到sql:

“select user from ctf where (user=‘admin’)#.’”) and (pw=’".$pass."’)"前者被注释，得到flag