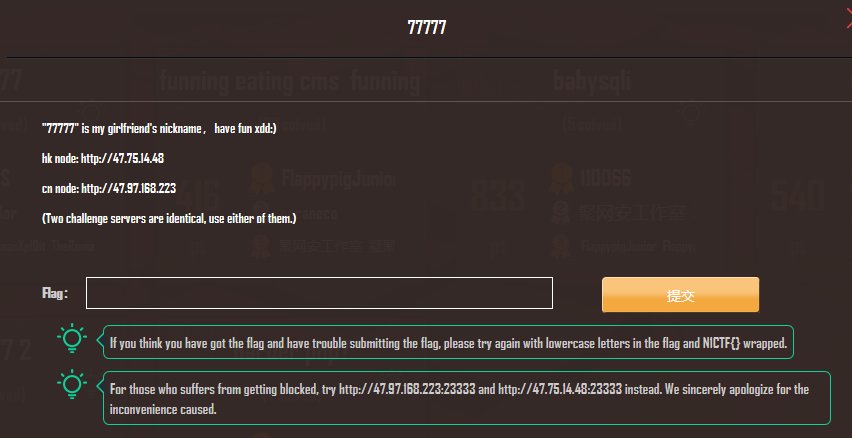
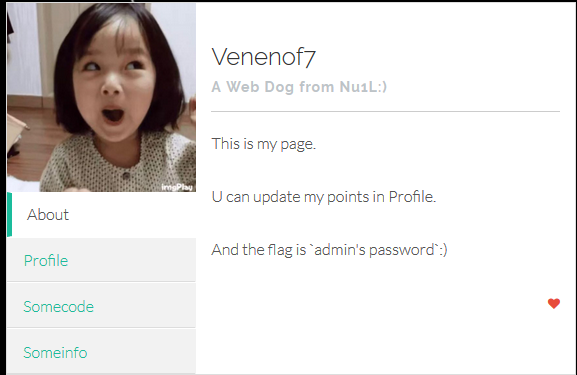
**xctf的一道题目（77777）**



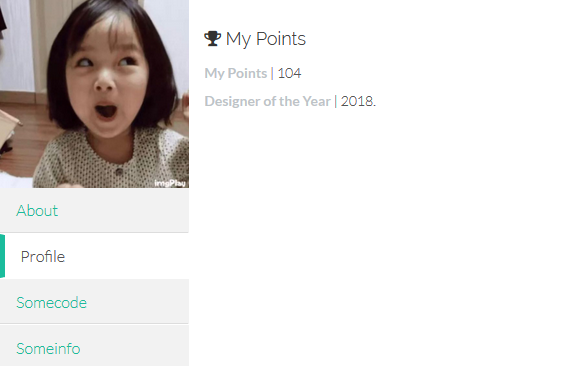
这次比赛我没有参加，这是结束之后才做的题目



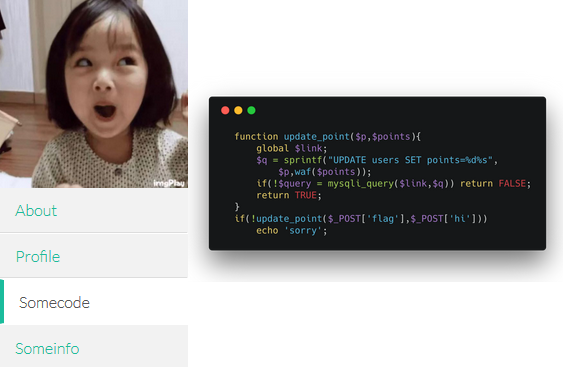
题目链接http://47.97.168.223:23333



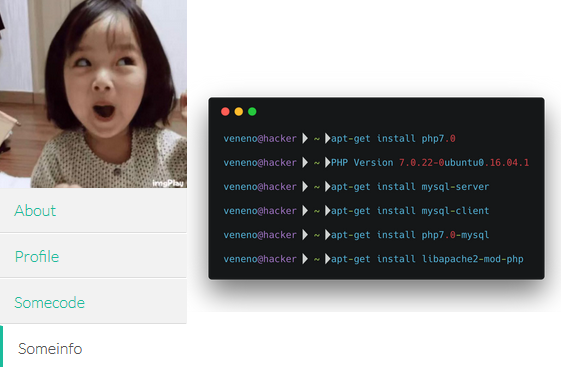
根据题目信息，我们要update那个points值，那就是有很大可能这道题目是一个sql注入的题目，首先要找到那个points值，随意点一下其他几项



Points值在这里



这里有部分代码

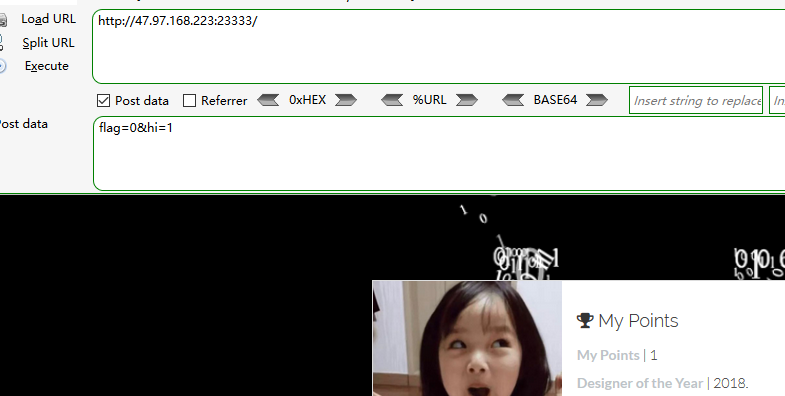


这个不知道是什么

发现了代码，那就是要先看一下代码

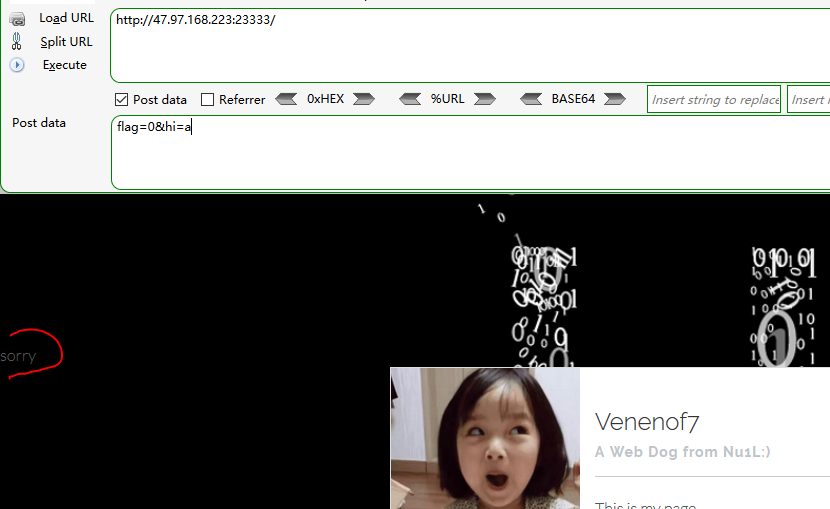
可以看到这里传进来了两个参数，一个是flag，一个是hi，然后两个值用spintf格式化传进sql语句，有要求，flag只能传进数字，hi没有规定，但是有waf，也就是说我们的注意点就存在hi值这里，也就是题目说的update points值

观察代码，发现如果出现执行不了就输出sorry，也就是说如果顺利执行的话，就没有什么提示



输入flag=0&hi=1，发现points值为1，那就是代码所说的

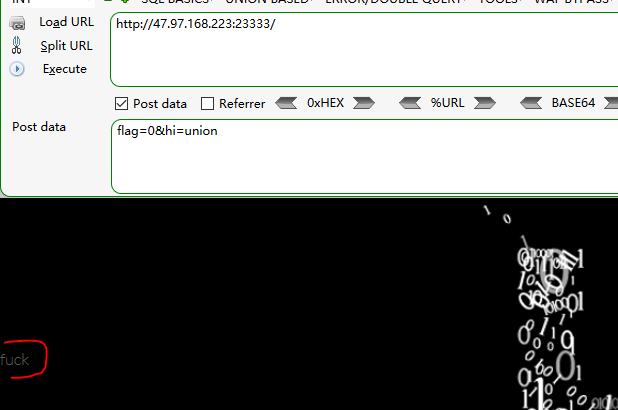
那就尝试让他出现sorry



输入flag=0&hi=a

出现了sorry，这里一定要注意看，因为这个颜色和背景颜色太贴近了

接下来就看看过滤了什么



输入hi=union

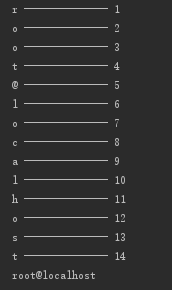
出现了fuck，那就是被过滤了

测试了一下常用的函数

被过滤函数 union in sleep limit =

看到被过滤的函数，然后就想到查不了表了，那就是说，只能靠猜了

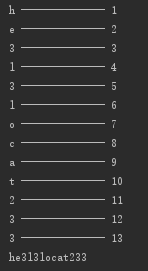
先把user跑出来



知道了user是root

（在查不了表的情况下，问了一下朋友，朋友说，权限是root，查不了表，结合题目说的是admin’s password，想到了是root这个用户的password）

然后就是查那个root的密码，用不了limit，那就用条件，where user like ‘root’



密码就是这个了，看了朋友的wp，证明这个是正确的