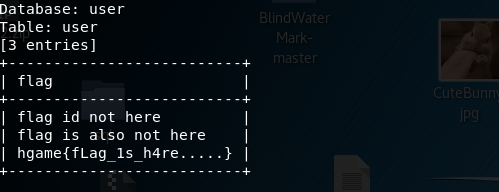
**Web**

**正常的SQL**

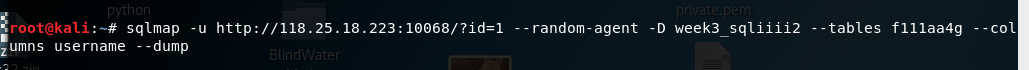
这道题我首先看请求头，发现有一个base64编码的然后解码之后发现刚刚好是hello之后的东西，而且是在cookie中，上网查了一下sql注入居然还有cookie注入这种操作，然后就是sqlmap一番神操作就有了-，-时间盲注真的花了一下午的时间，我觉得主要是要用上插件那个base64encode.py的插件，然后一步步下去就可以了

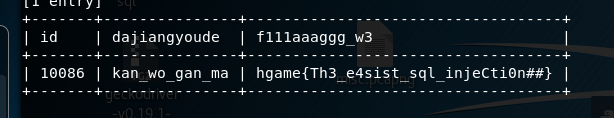


安全到手

**送分的SQL**

打开sqlmap神器发现可以用4种注入方式然后一步一步跑下来就可以了，拿到flag





**Ngc’s blog**

这道题其实很简单我的payload是

</h1> {{ ”.\_\_class\_\_.\_\_mro\_\_[2].\_\_subclasses\_\_()[40](‘./flag’).read() }},

然鹅我一直做不出的原因看来是我没有读过这篇文章

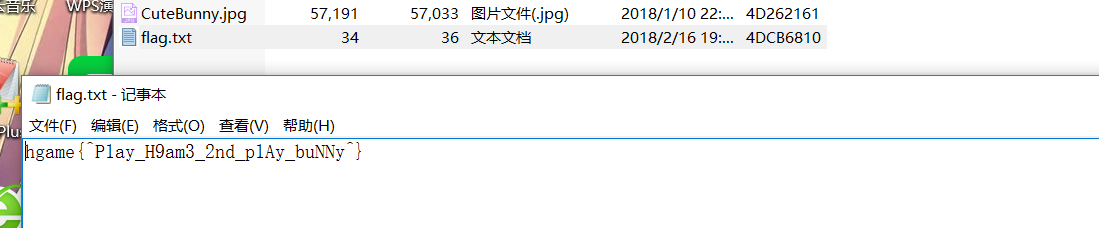
http://www.ckj123.xin/2018/02/24/%E6%8E%A2%E7%B4%A2flask-jinja2%E4%B8%AD%E7%9A%84%E6%9C%8D%E5%8A%A1%E7%AB%AF%E6%A8%A1%E7%89%88%E6%B3%A8%E5%85%A5/

**MISC**

**Bunny treasure**

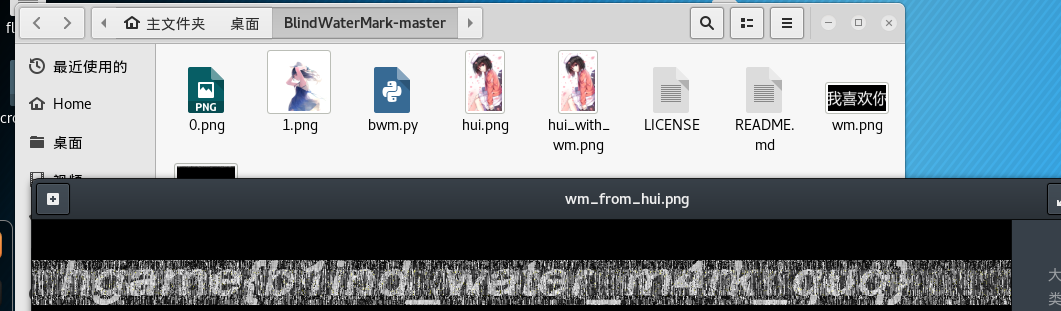
流量包分析题，这道题打开wireshark，然后用http过滤，发现只有两个get请求，将两个get请求中的网址打开就可以把图片和压缩包下载下来，已经有压缩包的一张图片了，使用明文攻击就可以解开这个压缩包（一开始还以为叫CRC32碰撞=。=）

明文攻击用



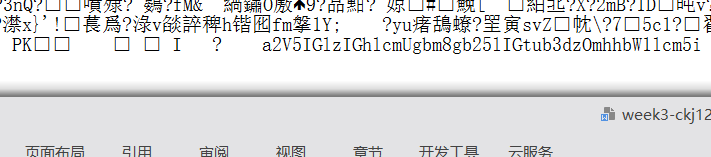
**画风不一样的她**

这道题有两张图，我先使用神器stegsolve.jar打开一张图片之后在使用Image Combiner，好像有一次看图片隐写的时候双兔都是这么做的，我就这样了，然后看到有些蓝色细条在图片中，又想起看过的一道题目，就是如果不是单个的细条如果很多的话，就是盲水印隐写，Google了脚本直接跑出来了

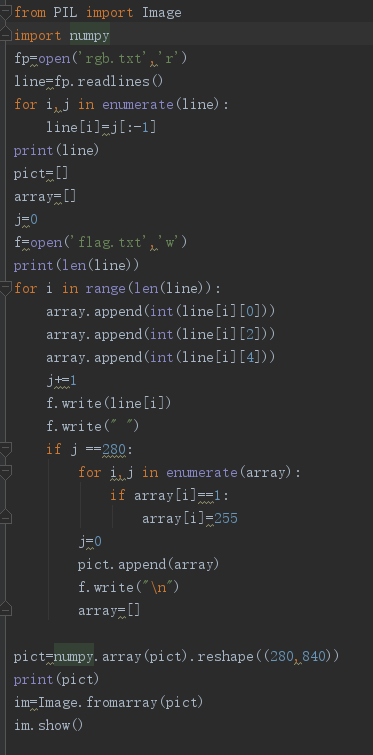


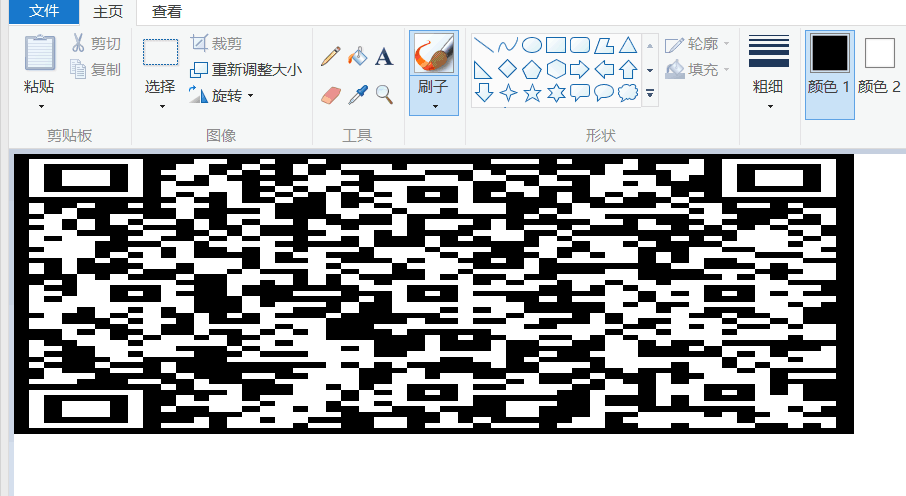
**这是啥**

**这道题真的很复杂。。先下载下来然后用txt打开**



这一段用base64解码得到hammernb就是压缩包密码。就打开里面的rgb.txt，看着名字我就觉得应该是张图片，三原色，而且里面只有01，那我估计就是一个二值化的图片，然后在电脑里面写了个脚本

跑出来了二维码有点斜用了画图的工具转转正



扫码出来是个文件=。=真的麻烦我要打人，然后文件名是md5加密，解出来是hammer666，hammer好厉害，文件内容看一下就是base64加密，解出来就是16进制的内容！！！我在这卡了好久！！！我一直使用的是notepad，后来一不小心试了试winhex，然后就压缩了，是个zip文件因为16进制中有504b 是zip中很有特点的，我一直以为密码是hammer666！！！！，后来实在不行跑字典了，密码是hgame，我列个去，然后拿到flag联系出题人。。。