**1.设计思路**

hash算法与RSA非对称加密算法认证

假设对一件商品进行认证，根据该商品的信息进行一次hash，生成哈希值，作为第一层防伪；并且同时生成一对密钥，私钥由商品所有人进行保存，公钥由认证机构进行保存。

第一层hash验证通过时候再使用第二层密钥进行验证，加快服务端的处理效率。

**2.程序架构**

前端使用Boostrap+jquery，发送ajax请求到后端

后端使用Python Flask框架

**3.程序使用流程**

用户先添加一件商品，商品添加成功后下载该商品的私钥，其他用户购得该商品可通过验证去判断商品的真伪性

1.HASH算法，根据商品的名字以及所对应的描述，进行hash比较，若于添加的商品一致，则进行第二轮验证

2.第二轮上传该商品的私钥，程序会根据自动帮用户进行一次签名，用系统存放的公钥进行比对，验证通过则商品正确

**4.优势**

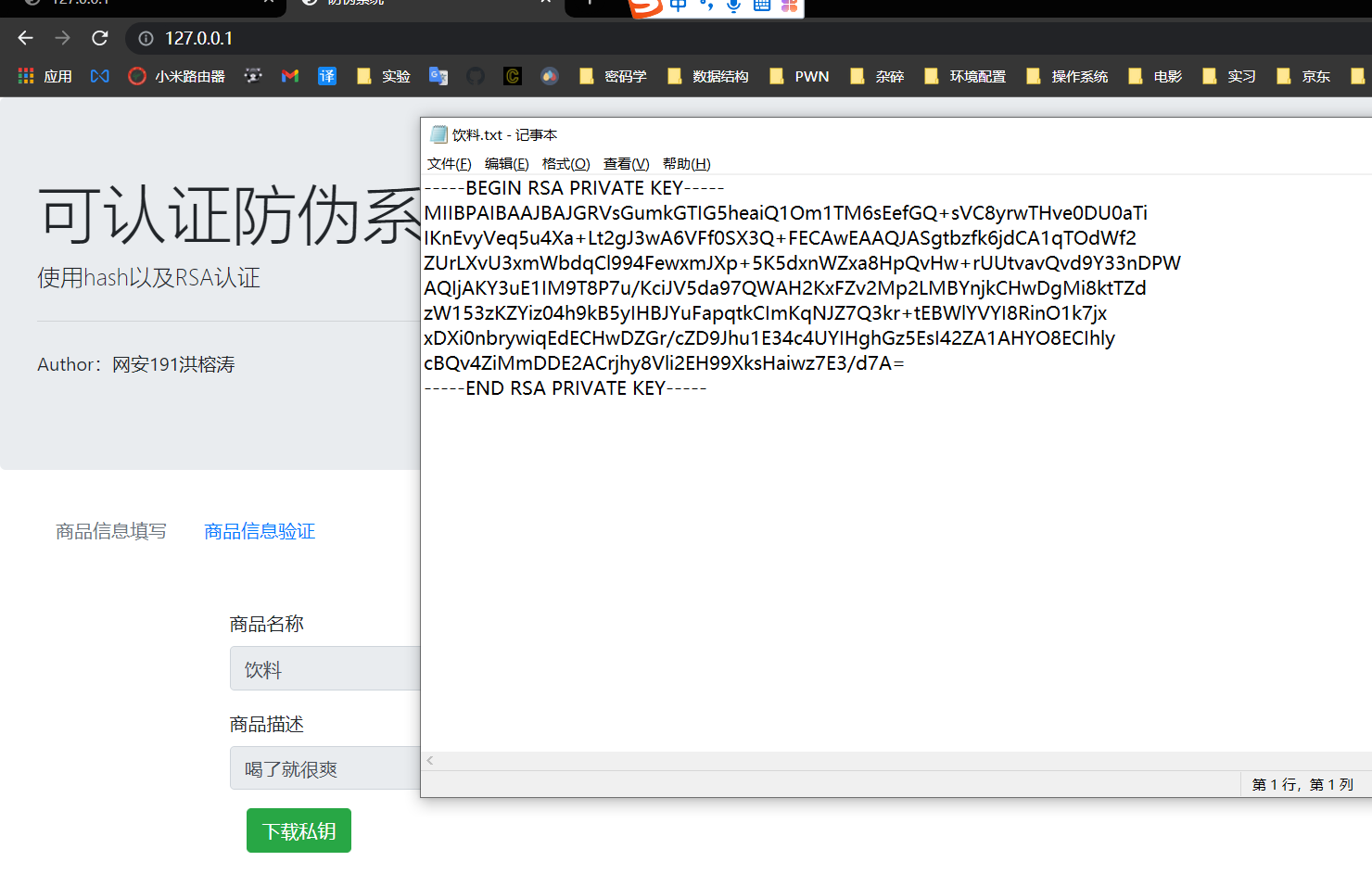
分成两次验证有利于防止暴力破解，并且程序只存放公钥，只有拥有商品的用户才能私钥进行验证，非对称签名相比于对称加密更能防止程序信息的泄露造成商品的伪造。

商品信息填写：





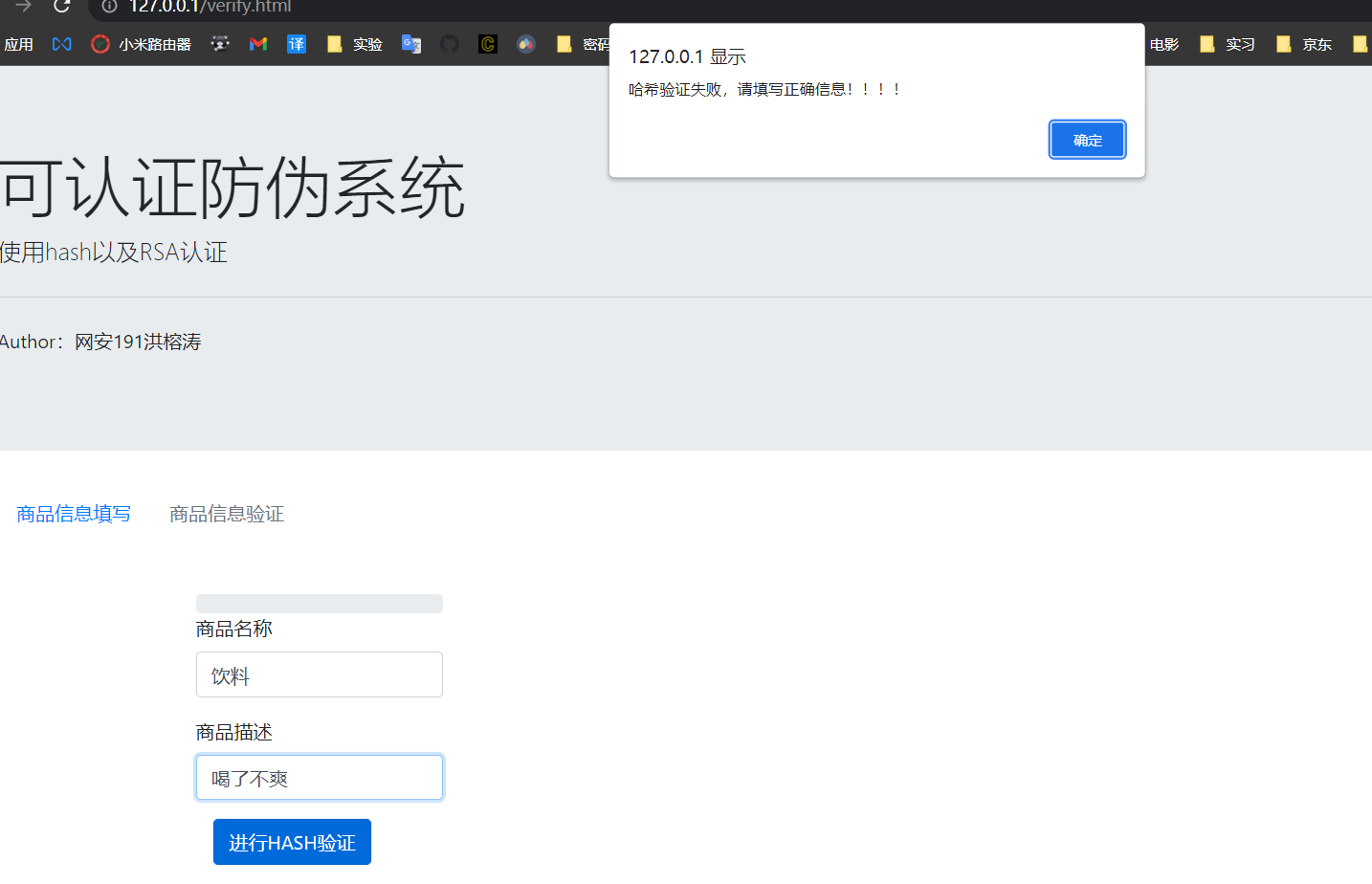
该商品对应私钥



信息验证：



验证不通过：



HASH验证通过：



RSA非对称验证通过

