- 任务详情
- 上周任务完成情况
- 上周任务详情
    - 1. 重新调试通过上学期的系统
    - 2. 哈希口令并加盐
    - 3.使用国密证书
- 上周撰写的文档
- 下周计划
    - 详细计划路径

任务详情

- 上周任务完成情况（代码链接，所写文档等）
- 本周计划

上周任务完成情况

1. 将上学期电子公文传输系统重新调试通过
2. 哈希存储用户口令并且加盐，能够切换哈希算法
3. 使用国密证书

任务	完成情况
启动系统	成功
哈希口令并加盐	成功
使用国密证书	失败

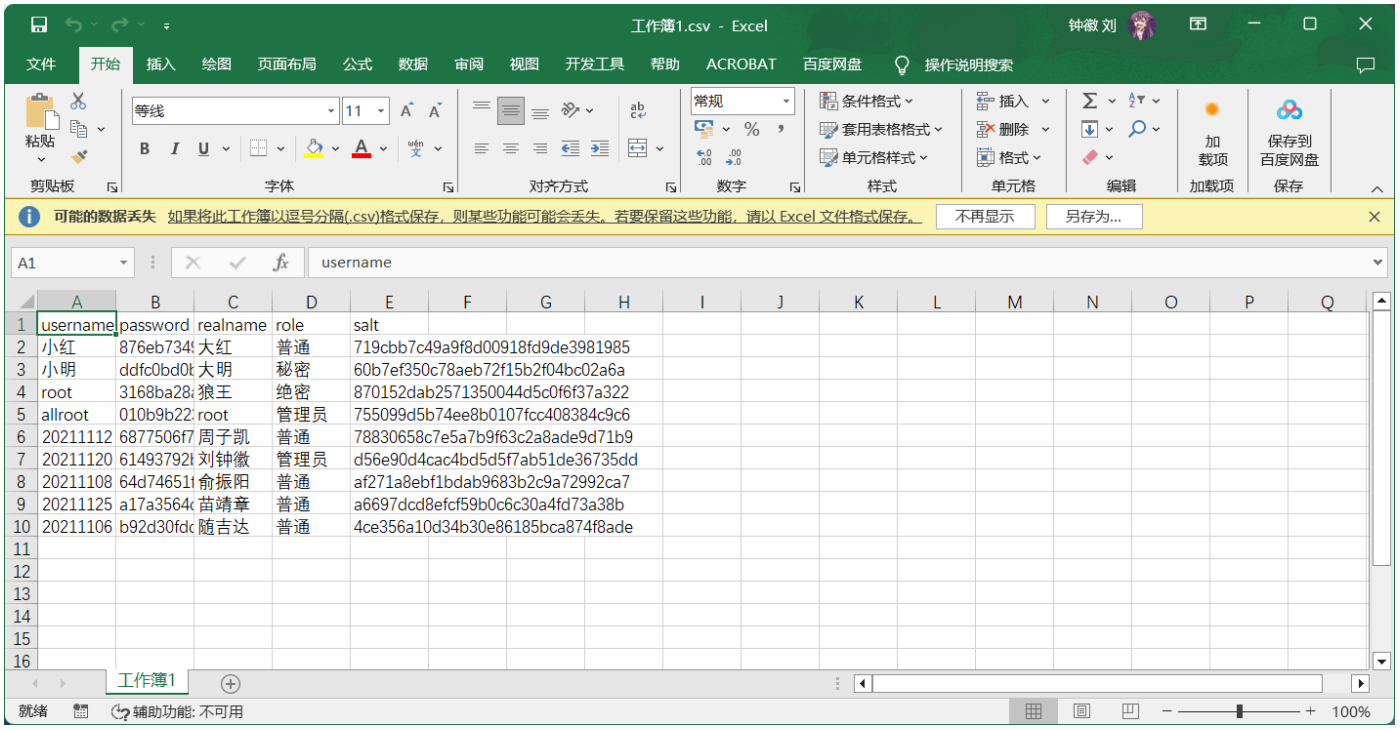
上周任务详情

1. 重新调试通过上学期的系统

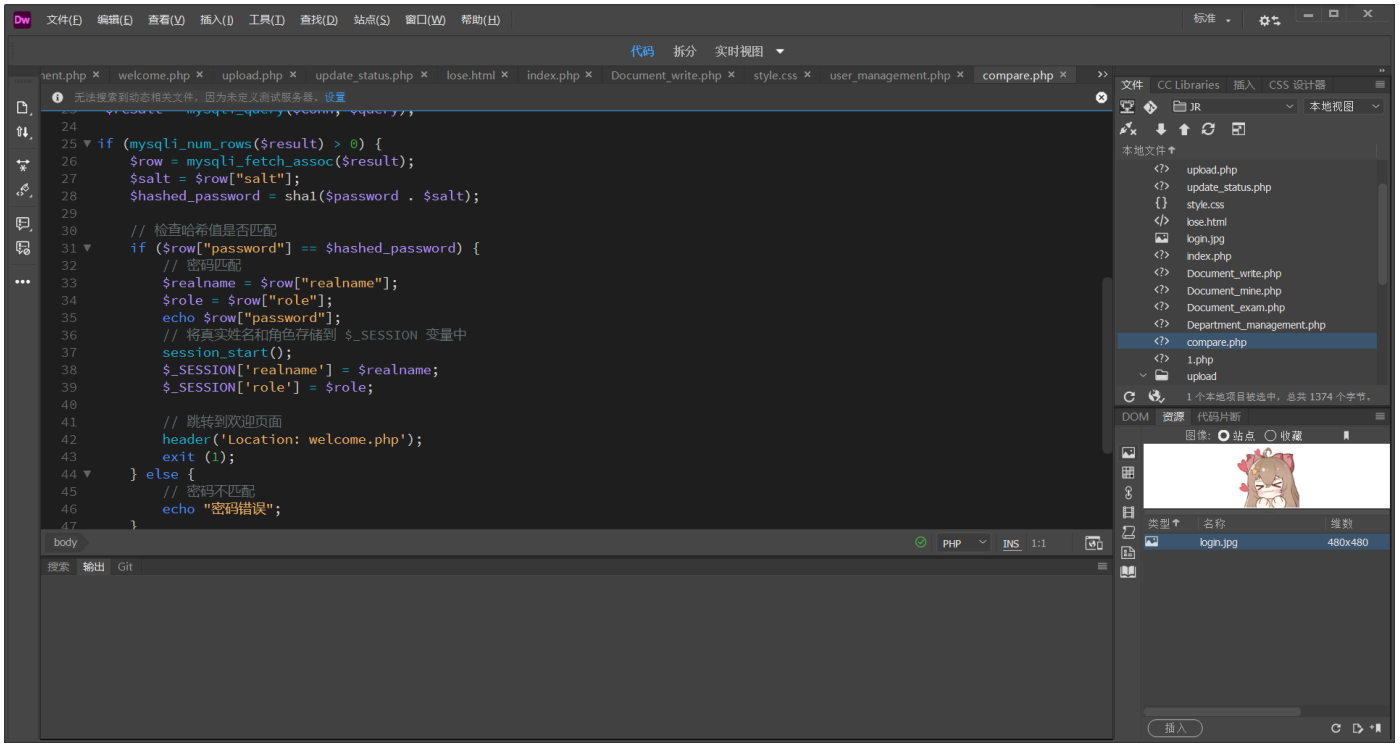
上学期做的系统主要采用的方法是html形式的，无法很好满足这学期的任务需求。于是重新将原来的html形式的改为python形式。

2. 哈希口令并加盐

已经有哈希和盐了，可以把哈希算法换为sha256或者SM2



加盐后数据库示意图（无明文密码） 完成登录加盐



相关代码截图

```
$hashed_password = sha1($password . $salt);

    // 检查哈希值是否匹配
    if ($row["password"] == $hashed_password) {
        // 密码匹配
        $realname = $row["realname"];
        $role = $row["role"];
```

```
            echo $row["password"];
        // 将真实姓名和角色存储到 $_SESSION 变量中
        session_start();
        $_SESSION['realname'] = $realname;
        $_SESSION['role'] = $role;
```

代码详情

3.使用国密证书

经过具体的尝试，但是失败了 过程和原因归纳如下： 国密证书需要符合国密标准的服务器，但是服务器基于centos 7 ， 需要配置一台新的主机（或者云服务器or虚拟机），工程量太大，并且需要根据其设备要求进行完整的配置，短期难以实现。

上周撰写的文档

1. Core.Software.Security.Security.at.the.Source.CN.软件安全.从源头开始》&《The.Security.Development.Lifecycle.CN.软件安全开发生命周期》读书报告*5（一人一份）；
2. 《加固计划书》一份；
3. 系统安全性设计报告一份。

下周计划

根据发布的任务要求，提出下周的修改计划

- 实验三
  - 基本要求
    - 符合GM/T0054，GB39786要求
    - 密码算法要合规/正确/高效实用
      - 只能使用商用密码算法
      - 正确使用对称和非对称算法以及HASH算法
      - 对称算法模式要正确，密钥长度要足够
      - 非对称算法加密解密/签名验签要正确使用，密钥长度要足够
      - 通信加密/存储加密
    - 要正确管理密钥
      - 秘密信息不能明存
      - 有密钥生命周期相关内容
    - 系统要符合“黄金”法则，具有认证/访问控制/审计功能
      - 认证至少有用户名+PIN，PIN不能明存，要通过“HASH+盐”方式防止彩虹表攻击
      - 至少具有基于角色的访问控制
      - 审计至少支持日志（谁什么时候做了什么）
  - 加分项目
    - 融入龙脉智能钥匙
    - 能进行商用密码应用安全性评估量化评估
    - 融入更多商用密码标准
    - 其他功能

1. 使用商用密码算法
2. 完善通讯加密/存储加密

详细计划路径

现在有一部分算法使用的还不是商用密码算法，如哈希存储口令还有sha256算法，与服务器认证过程中有RSA算法。下周计划使用数字信封形式，替代掉认证过程中的非商用

密码算法。同时完善通信加密/存储加密。

---

written by 20211108俞振阳