**人员入侵监测系统**

**设计报告**

|  |  |
| --- | --- |
| 项目名称： | **人员入侵监测系统** |
| 小组成员： | **周芷平，付柏逢、张钰杰、王地、王俊铭、张业瑞** |
| 负责人 ： | **周芷平** |

目录

[1. 简介 2](#_Toc108453876)

[1.1 编写目的 2](#_Toc108453877)

[1.3 定义 3](#_Toc108453878)

[1.4 参考资料 4](#_Toc108453879)

[2.需求概述 4](#_Toc108453880)

[2.1 需求概述 4](#_Toc108453881)

[2.2 软件结构 7](#_Toc108453882)

[3.设计描述 8](#_Toc108453883)

[3.1 结构描述 8](#_Toc108453884)

[3.2子模块描述 8](#_Toc108453885)

[3.4前端界面描述 11](#_Toc108453886)

[**4.数据库设计** 19](#_Toc108453887)

[**4.1物理模型** 19](#_Toc108453888)

[**4.2 非关系型数据库** 19](#_Toc108453889)

# 简介

## 1.1 编写目的

本设计报告，说明了人员入侵监测系统的功能结构，详细功能介绍、数据字典和性能、接口需求等。系统包含用户注册，登录，实时监控，入侵回放，入侵记录，入侵统计，用户管理、信息管理和人脸注册等功能。

该系统设计报告是关于人员入侵监测系统的功能需求和性能需求的描述，该设计报告的预期读者为： 用户； 项目管理人员； 测试人员； 设计人员； 开发人员。

明确所要开发的软件应具有的功能、性能与界面，使系统分析人员及软件开发人员能清楚地了解用户的需求。

**1.2 项目背景**

软件名称：人员入侵监测系统

项目开发者：周芷平，付柏逢，张钰杰，王地，王俊铭，张业瑞

目标用户：对人员入侵监测有需求的用户

本项目使用了数据库来记录使用本系统的用户，使用基于springboot、openCV和vue等的技术框架，实现了线上实时视频监控功能和警报记录功能。

## 1.3 定义

1）过程：“一组将输入转化为输出的相互关联或相互作用的活动”。

2）产品：“一组将输入转化为输出的相互关联或相互作用的活动的结果”。

3）质量管理：指导和控制某组织与质量有关的彼此协调的活动。

4）UML：统一建模语言、是一套用来设计软件蓝图的标准建模语言，是一种从软件分析、设计到编写程序规范的标准化建模语言。

5）用例图（User Case）：是被称为参与者的外部用户所能观察到的系统功能的模型图，呈现了一些参与者和一些用例，以及它们之间的关系，主要用于对系统、子系统或类的功能行为进行建模。

6）数据字典：是一种用户可以访问的记录数据库和应用程序源数据的目录。

7）事务流：数据进入模块后可能有多种路径进行处理**。**

## 1.4 参考资料

有关的参考文件：实训教学ppt。

本文件中各处引用的文件、资料，包括所要用到的软件开发标准：

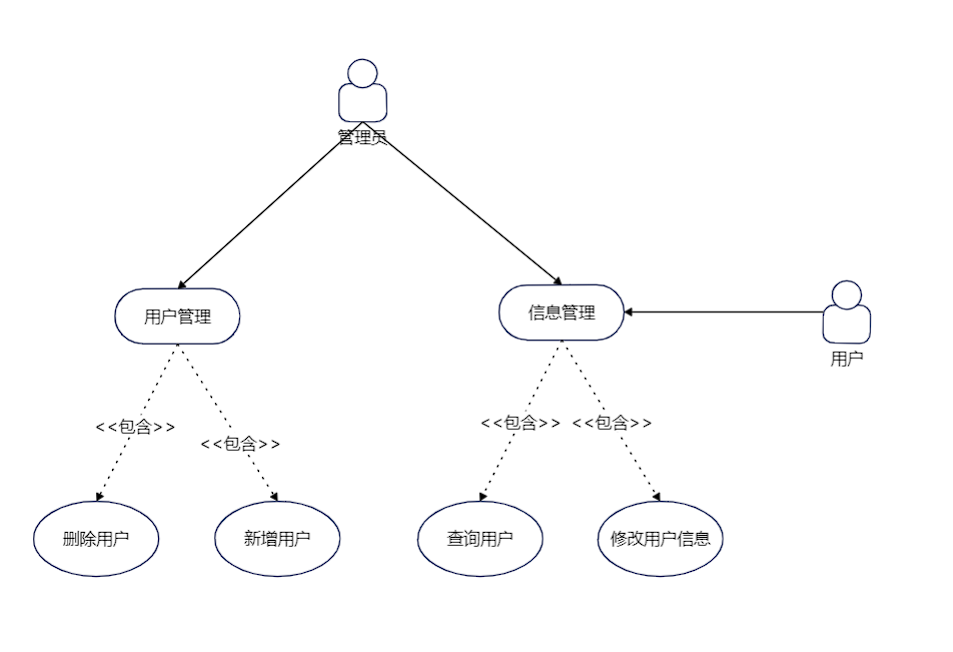
实训教学PPT及相关人员入侵监测系统项目需求分析文档。

## 2.需求概述

## 2.1 需求概述

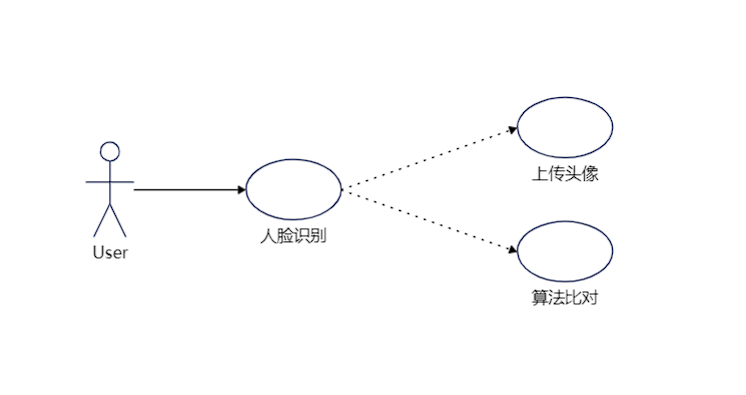
本项目主要针对非对外场所（即内部场所）的监控和警报，对于任何出现在监控范围内的陌生人员进行提醒和跟踪，且对使用者进行邮箱、页面等多重通知警报。

**2.1.1 用户管理需求**



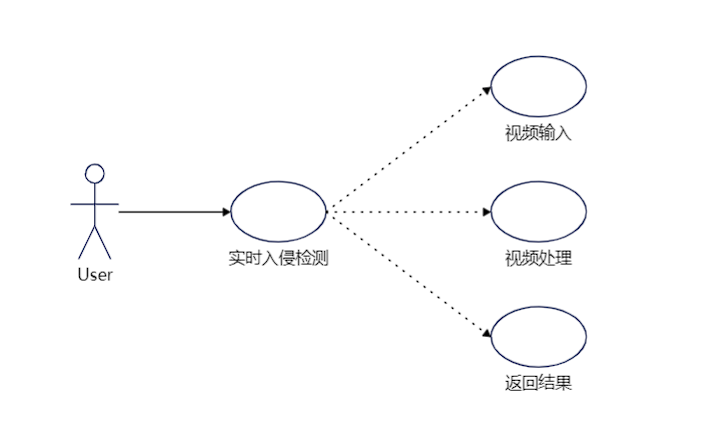
管理员拥有用户管理和信息管理模块的权限，可以对用户信息进行查询修改、新增用户、删除用户，用户本身只具有信息管理权限，只能修改用户自己的信息或是查询其他用户的公开信息但不能修改。

**2.1.2 人脸识别需求**



系统将所有出现在场景内的人员与白名单人员头像比对若视频中的人员不在库中，则返回结果通知系统

**2.1.3 实时入侵检测需求**



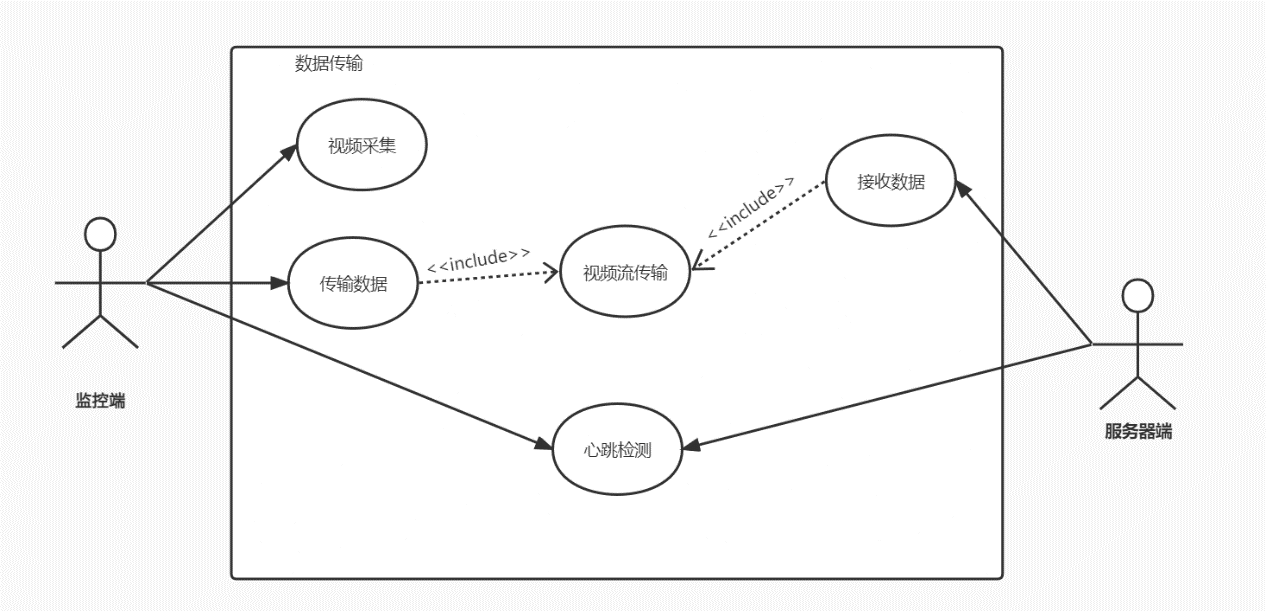
接受视频端的输入（即视频）

执行人脸识别（

若存在违规人员则执行警报处理并将违规人员在视频中标注

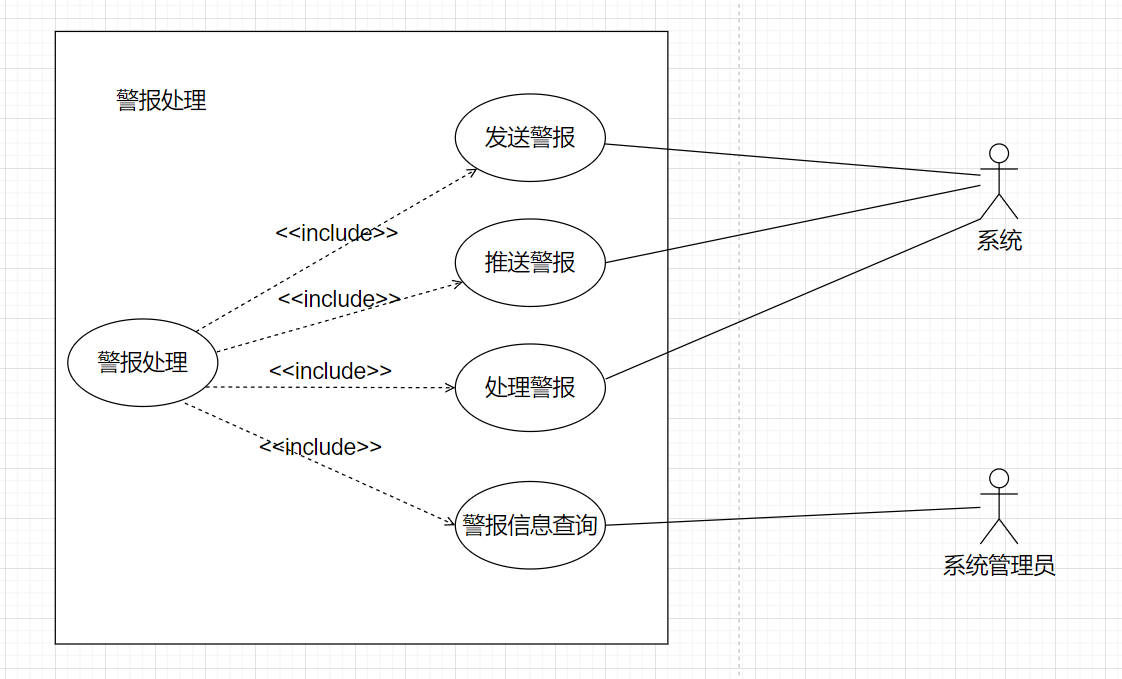
将处理后的视频数据返回给视频端

**2.1.4 数据传输需求**



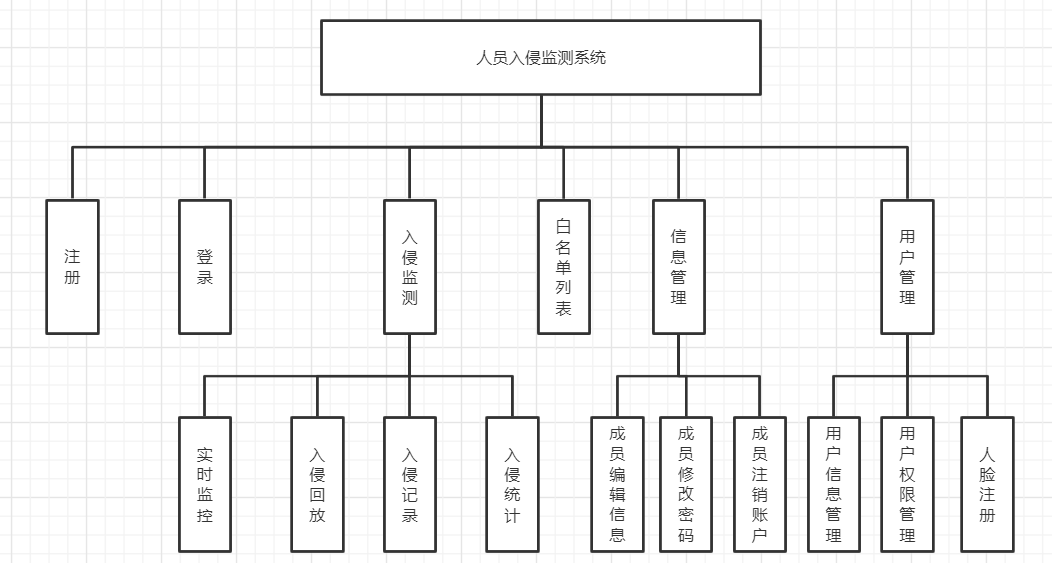
监控端启动之后开始采集视频数据，服务器启动并与监控建立连接之后，监控段开始通过视频流向服务器段传输数据，并由服务器端发起心跳协议进行心跳检测。

**2.1.5 警报处理需求**



当有入侵发生，系统完成警报发送、警报推送、警报处理的功能，同时管理员可以对警报信息进行查询。

## 2.2 软件结构



# 3.设计描述

## 3.1 结构描述

系统使用的开发模式：springboot+OpenCV+vue，它与三层架构的结合中， Vue充当表示层，springboot与OpenCV即模型(包含业务逻辑，数据访问和业务模型类等)充当业务逻辑层和数据访问层。

## 3.2子模块描述

##### 3.2.1 注册

**1**、功能设计描述在注册页面填写注册信息，要求填写用户名（必填，4~20个汉字、字母、数字或下划线组成的字符串，且不能有重名注册），密码（必填，8~12个字符），确认密码（和密码保持一致），进行注册。

提交注册信息时，有必填项未填写或格式不正确时，提示用户正确填写相应项，当注册失败时在注册页面显示“注册失败！”。当所有信息填写正确，提交表单，注册成功跳转到登录页面，如果程序出现异常则跳转到异常页面。

##### 3.2.2 登录/登出

**1**、功能设计描述在登录页面填写用户名、密码，点击“登录”按钮进行登录。要求用户名和密码不能为空，为空则在登录页面给出错误提示。登录失败时在登录页面提示 “用户名或密码错误！”；系统异常，跳转到异常页面；登录成功跳转到新用户页面，并显示当前登录用户名。

已登录的用户，点击新用户页面的“注销登录”链接，清除用户的登录状态。返回到登

录页面。

##### 3.2.3 入侵检测

**1**、简介

已注册成员登录后，可以查看实时监控、入侵回放、入侵记录、入侵统计

**2**、功能列表

|  |  |
| --- | --- |
| 功能名称 | 功能描述 |
| 实时监控 | 查看摄像头的实时监控 |
| 入侵回放 | 查看哪个日期有入侵情况，有入侵的日期可以查看回放。 |
| 入侵记录 | 查看到具体时间段的入侵记录，并且可以查看截图。。 |
| 入侵统计 | 查看过往入侵记录的统计信息。 |

##### 3.2.4 白名单列表

**1**、简介

系统管理员可以编辑白名单内人员，在白名单内的成员进入系统监测范围内不会报警。

##### 3.2.5用户个人信息管理

**1**、简介

已注册普通成员登录系统后，可以编辑自己的基础信息、修改自己的密码，也可以注销自己的账户。

**2**、功能列表

|  |  |
| --- | --- |
| 功能名称 | 功能描述 |
| 编辑信息 | 用户可以编辑自己的基本信息 |
| 修改密码 | 用户可以修改自己的密码 |
| 注销账户 | 用户可以注销自己的账户 |

##### 3.2.6 用户管理

**1**、简介

系统管理员登录系统后，可以对普通成员的基础信息与权限进行编辑。

**2**、功能列表

|  |  |
| --- | --- |
| 功能名称 | 功能描述 |
| 用户管理 | 对普通成员的基础信息进行编辑。 |
| 权限管理 | 对普通成员的权限等级进行编辑 |
| 人脸注册 | 帮助上传成员的人脸信息进行注册。 |

##### 3.3 接口设计

**3.3.1 注册**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名称 | 注册 | | | |
| 接口说明 | 连接用户注册界面 | | | |
| 请求方法 | get | | | |
| 请求地址 | /Register | | | |
| 请求参数 | 参数名 | 说明 | 类型 | 备注 |
| userName | 用户名 | String | 用户名不可重复 |
| password | 密码 | String | 用户密码 |
| emai | 邮箱 | String | 用户邮箱 |
| code | 验证码 | String | 用户需通过邮箱获得验证码进行注册 |
| account | 用户账号 | Int | 用户账号 |
| repassword | 重复密码 | String | 重复密码必须与密码相同才可注册成功 |

**3.3.2 登录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名称 | 登录 | | | |
| 接口说明 | 用户登录入侵监测系统 | | | |
| 请求方法 | get | | | |
| 请求地址 | /Login | | | |
| 请求参数 | 参数名 | 说明 | 类型 | 备注 |
| userName | 用户名 | String | 用户名不可重复 |
| password | 密码 | String | 用户密码 |

**3.3.3 用户删除**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名称 | 用户删除 | | | |
| 接口说明 | 用户权限及信息管理界面的用户删除功能 | | | |
| 请求方法 | get | | | |
| 请求地址 | /user\_info\_jurisdiction | | | |
| 请求参数 | 参数名 | 说明 | 类型 | 备注 |
| userid | 用户id | String | 用户id |

删除用户后，数据库与页面都会将这条记录删除

**3.3.4 用户权限编辑**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名称 | 用户权限编辑 | | | |
| 接口说明 | 用户权限及信息界面的用户权限编辑功能 | | | |
| 请求方法 | get | | | |
| 请求地址 | /user\_info\_jurisdiction | | | |
| 请求参数 | 参数名 | 说明 | 类型 | 备注 |
| username | 用户名 | String | 用户名称 |
| rights | 权限等级 | Int | 可以编辑权限等级 |
| userid | 用户id | String | 用户id |

管理员可以修改普通成员的权限等级，数据库与页面会同步更新

**3.3.5 用户人脸注册**

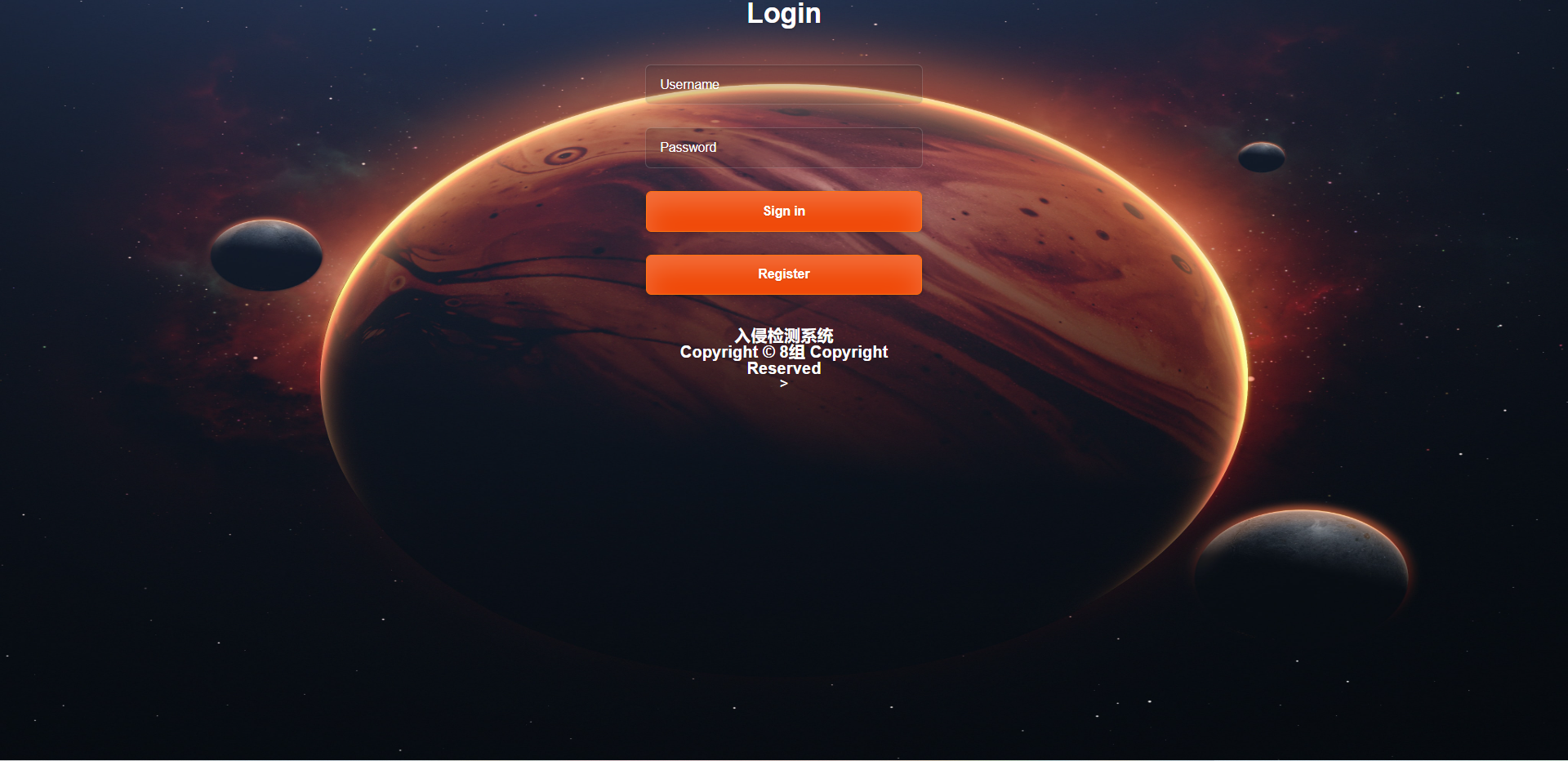
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名称 | 用户人脸注册 | | | |
| 接口说明 | 用户上传人脸进行白名单注册功能 | | | |
| 请求方法 | get | | | |
| 请求地址 | /face | | | |
| 请求参数 | 参数名 | 说明 | 类型 | 备注 |
| username | 用户名称 | String | 用户名称 |
| userid | 用户id | String | 用户id |

**3.3.6 入侵记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名称 | 入侵记录 | | | |
| 接口说明 | 系统监测到入侵时将对监控进行截图，截图记录在入侵记录里可以查看 | | | |
| 请求方法 | get | | | |
| 请求地址 | /record\_admin、/record\_mem | | | |
| 请求参数 | 参数名 | 说明 | 类型 | 备注 |
| fileid | 截图文件id | String | 截图文件的id |
| filename | 截图文件名称 | String | 截图文件的名称 |
| filedate | 入侵截图的日期 | Date | 入侵截图的日期 |
| userid | 用户id | String | 用户id |

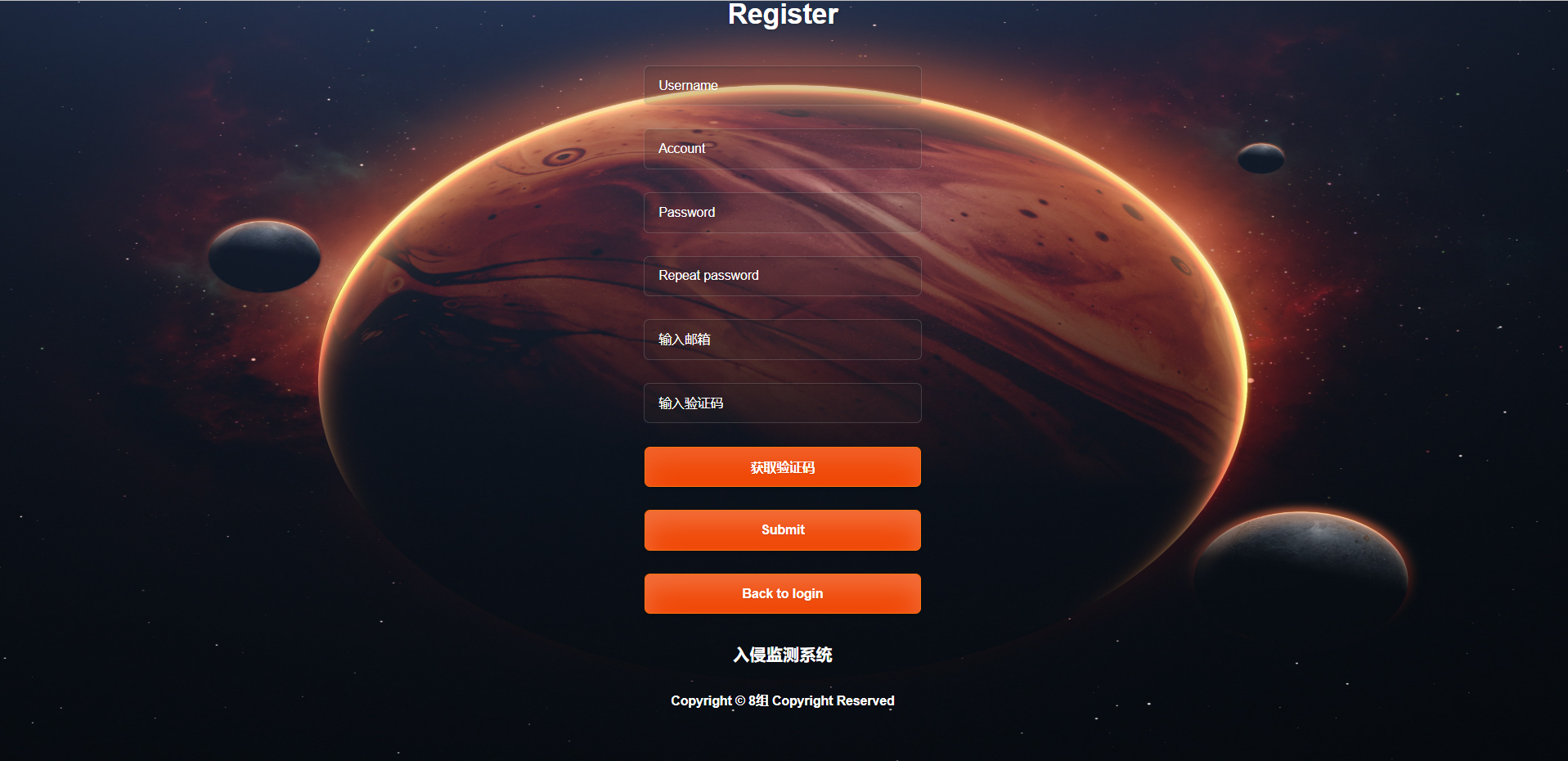
## 3.4前端界面描述

**3.4.1 登录界面**



输入账号密码即可登录，如果没有账号则可以注册

**3.4.2 注册用户**



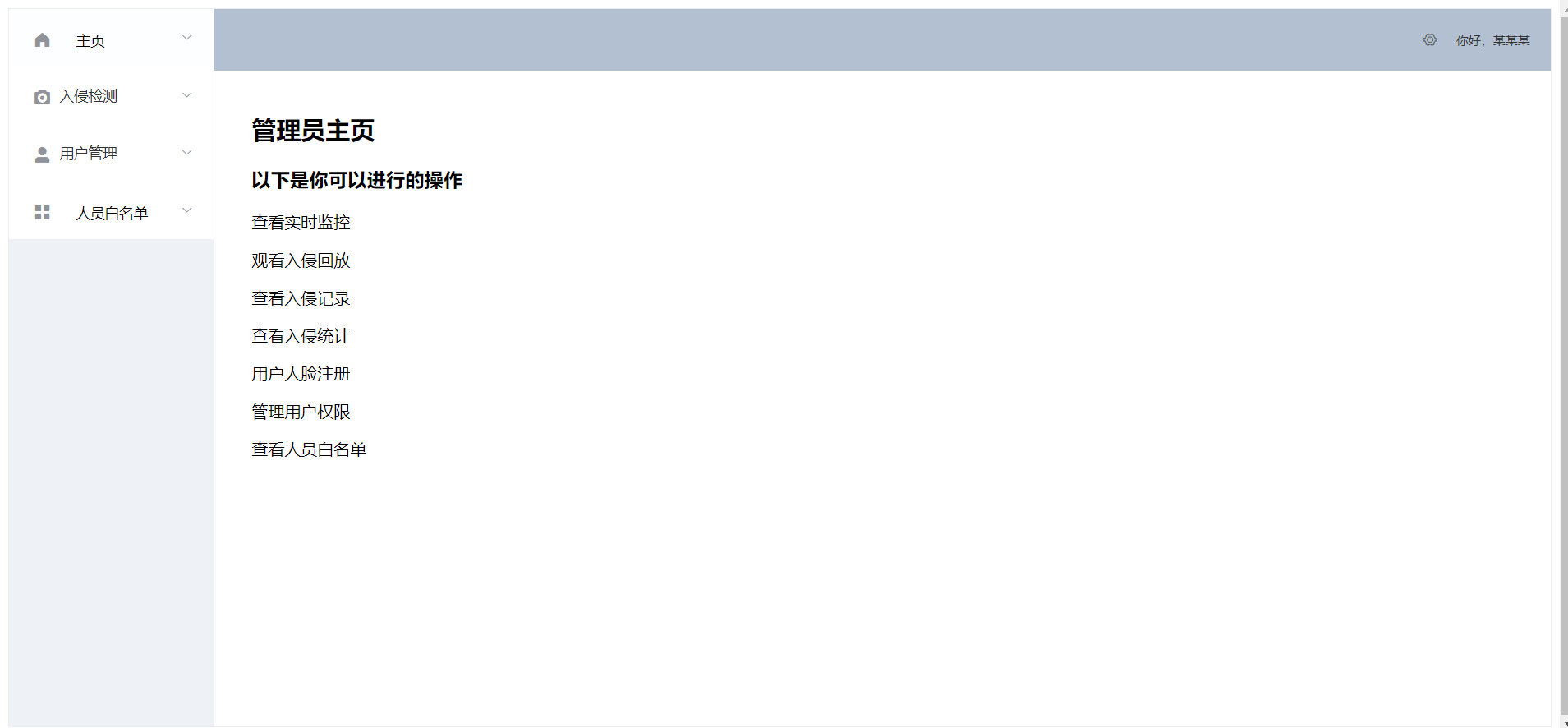
输入自己的名称、账号、密码、邮箱，通过邮箱获取验证码完成注册

**3.4.3 主页**

**3.4.3.1 普通用户主页**



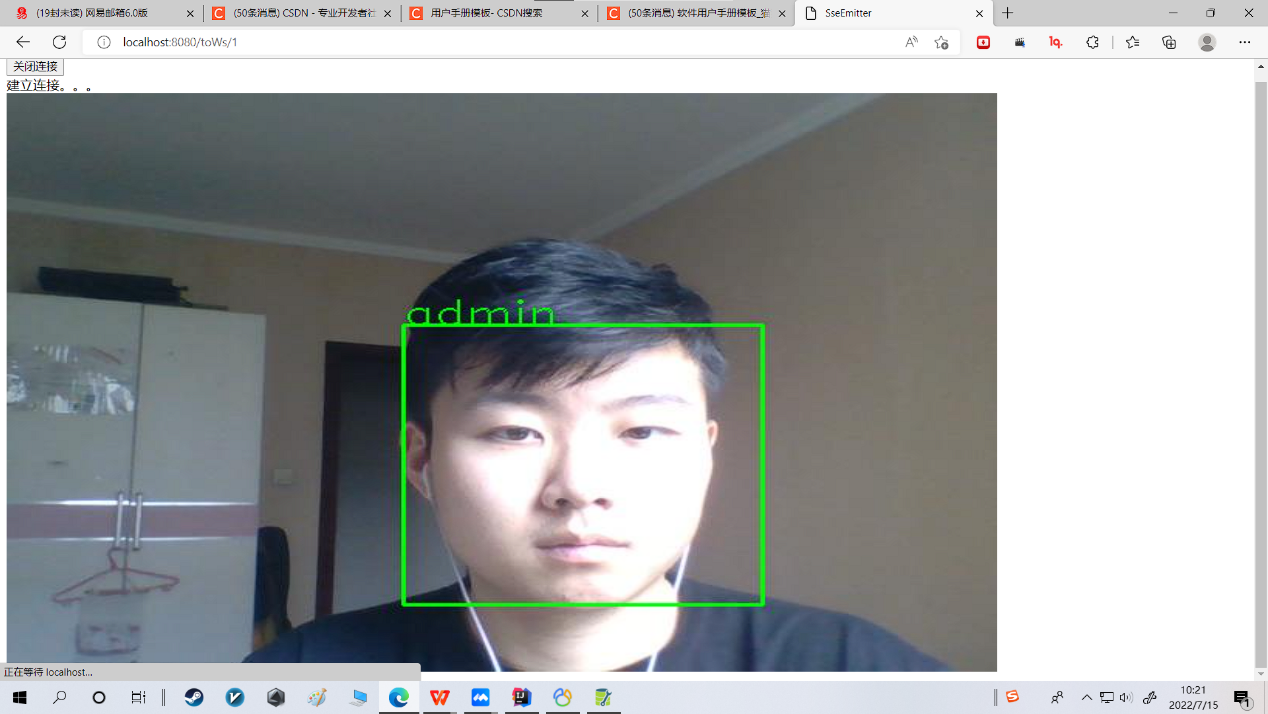
**3.4.3.2 管理员主页**



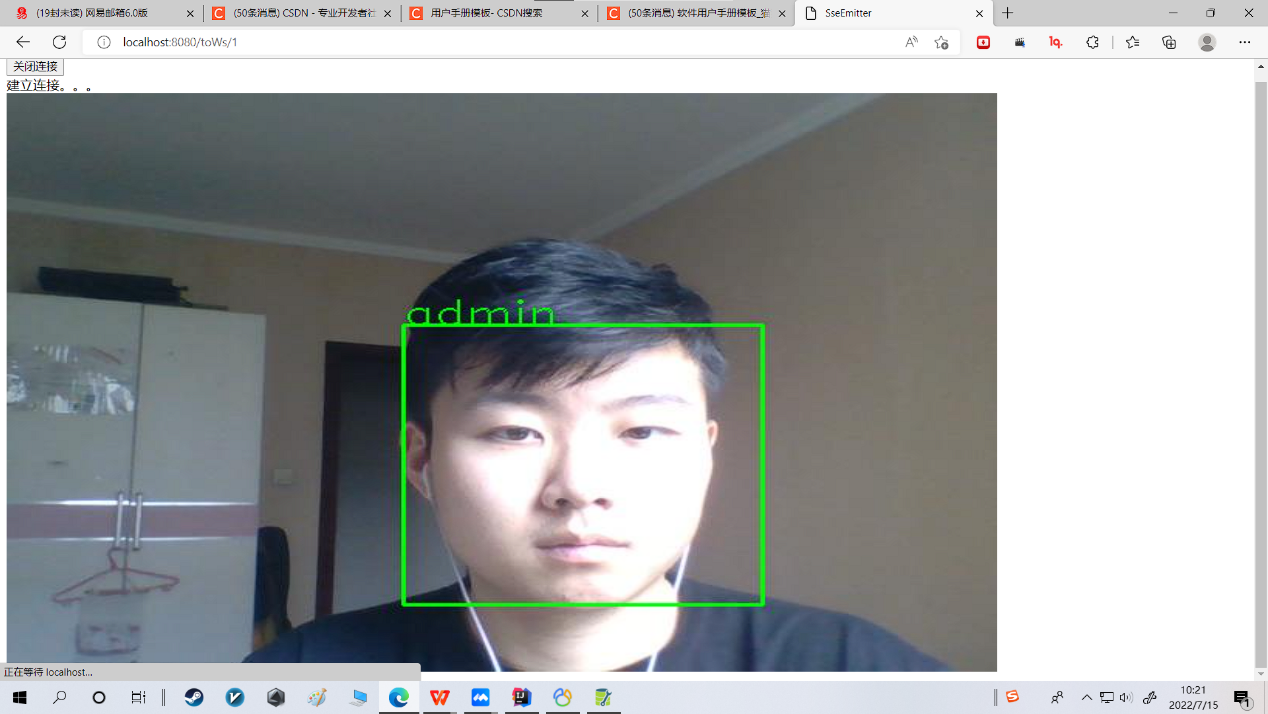
在主页可以查看自己可以进行的操作

**3.4.4 实时监控页面**

**3.4.4.1 管理员监控画面**



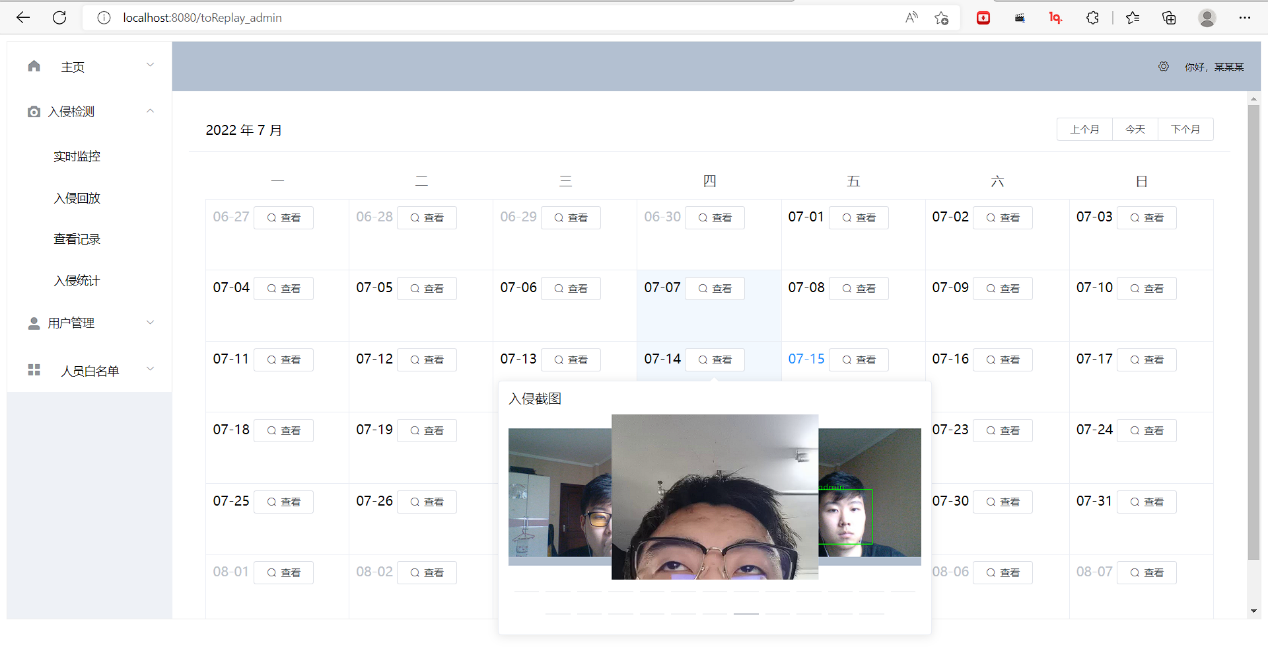
**3.4.4.2 普通成员监控画面**



普通成员与管理员都可以查看实时监控信息

**3.4.5 入侵回放**

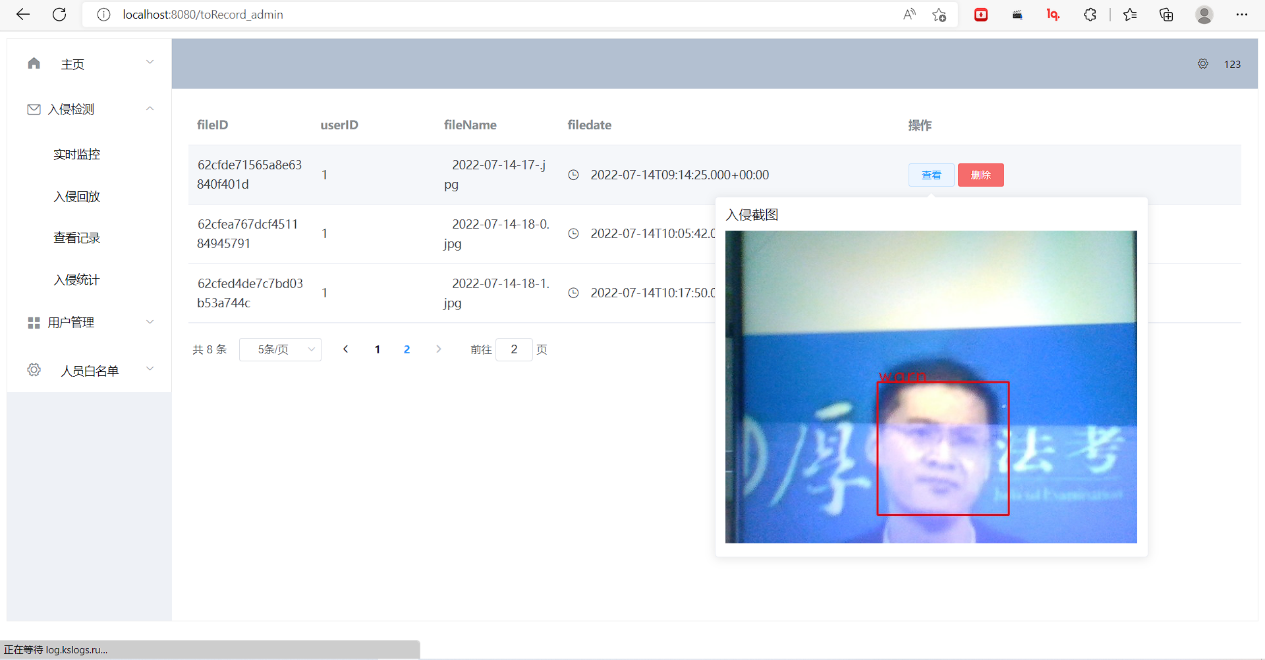
由于管理员与普通成员关于入侵回放的界面只有导航栏不同，所以下面只展示管理员的界面。



在出现入侵的日期可以点击“查看”按钮进行入侵截图的查看，这里利用一个轮播图进行当天入侵截图的展示。

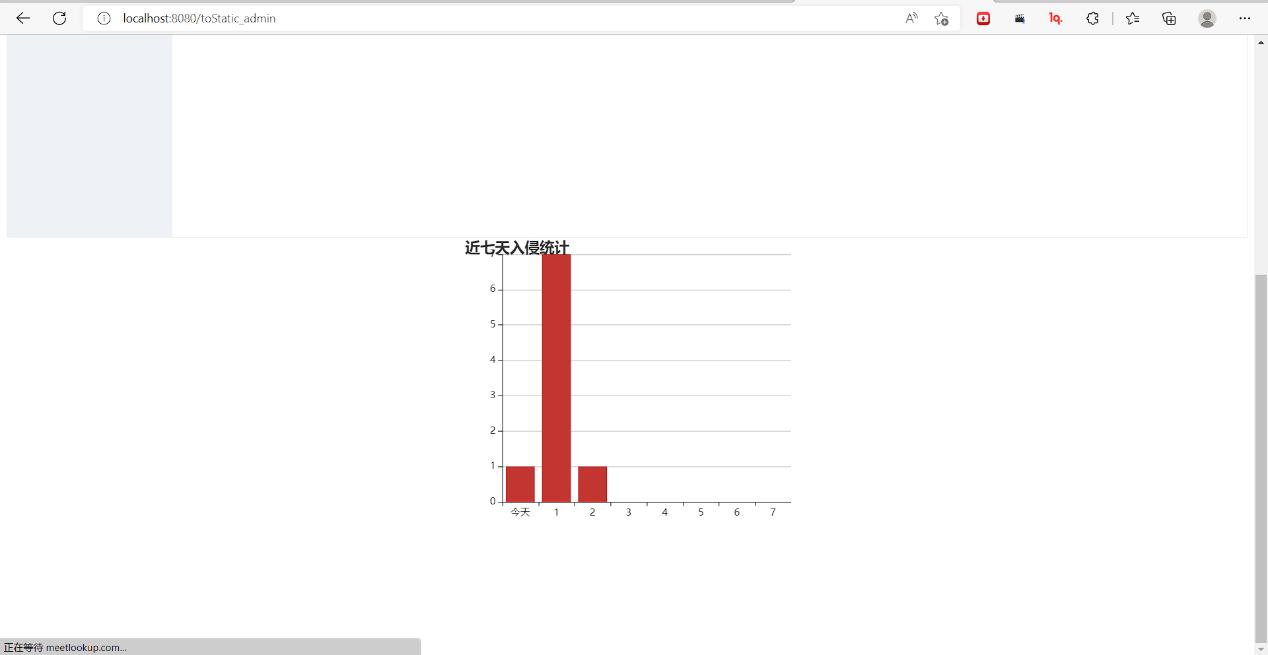
**3.4.6入侵记录**

**3.4.6.1 管理员界面的入侵记录**



管理员除了可以查看入侵截图，还可以删除入侵记录。而普通成员只能查看入侵记录

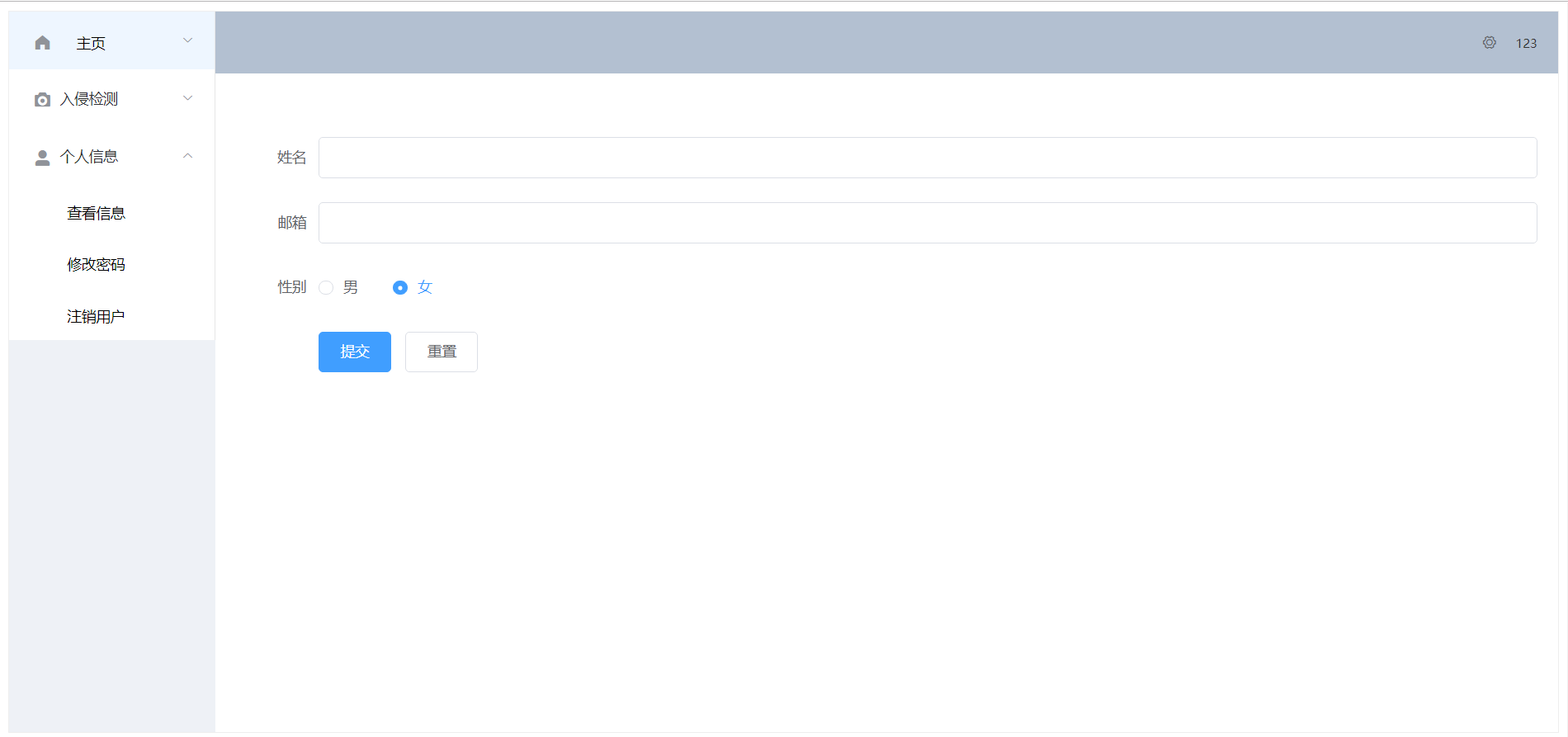
**3.4.7 入侵统计**



基于过去7天的入侵数据进行统计，以直方图形式显示统计结果。

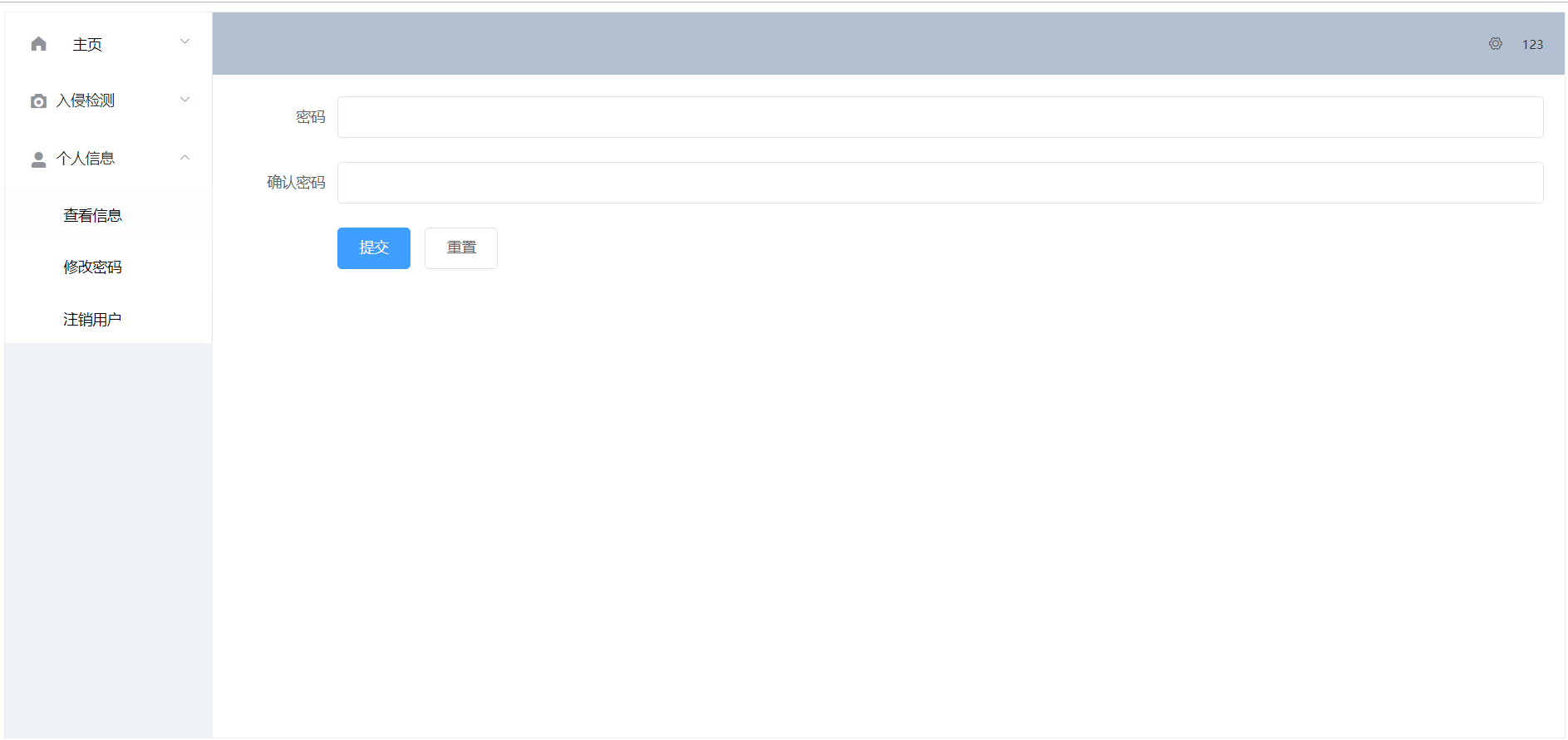
**3.4.8 普通成员个人信息**

**3.4.8.1编辑个人信息**



普通用户可以编辑自己的信息

**3.4.8.2 修改密码**



普通用户可以修改自己的密码

**3.4.8.3 注销账户**



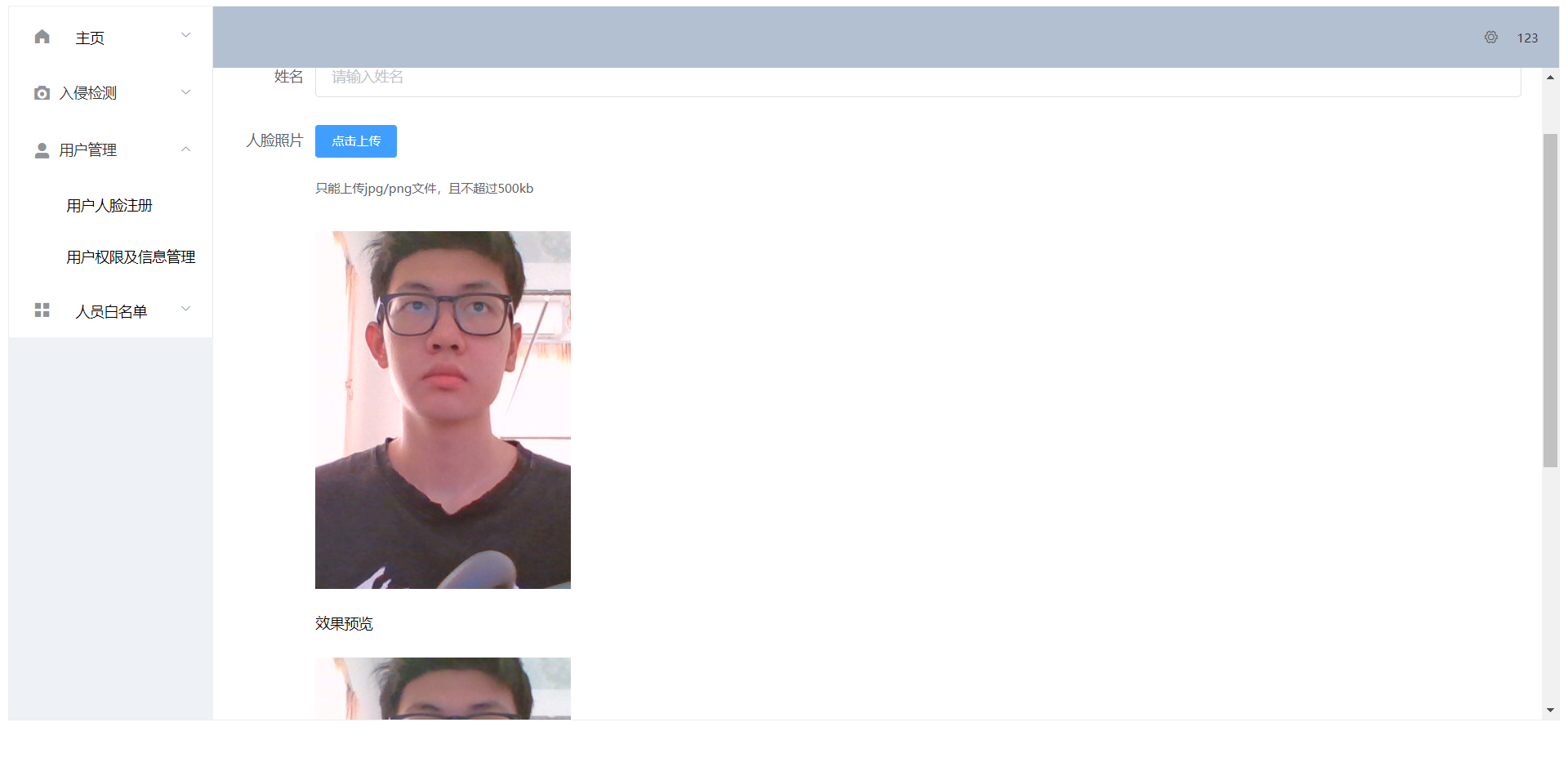
普通用户可以注销自己的账户

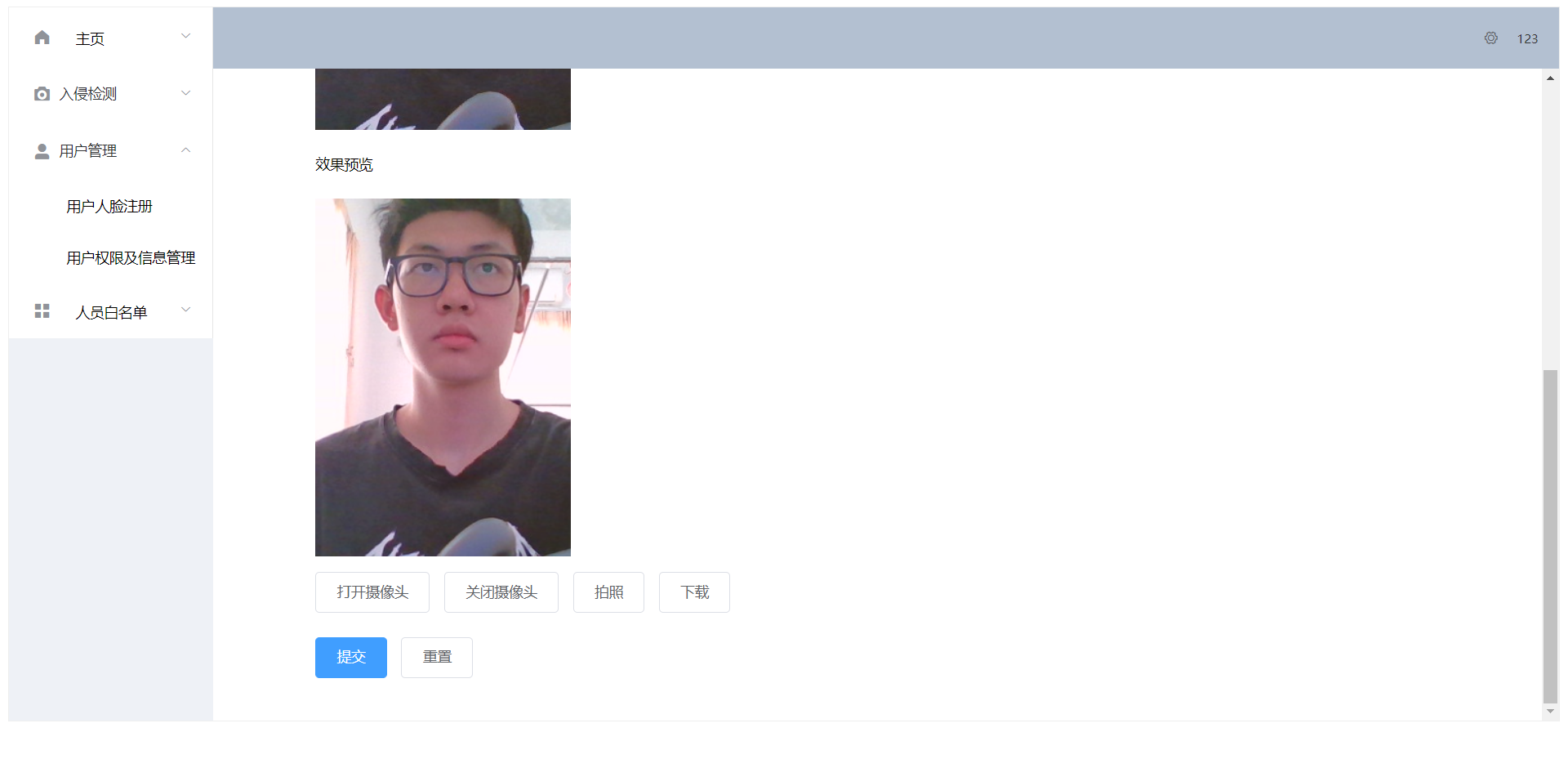
**3.4.9 用户管理**

**3.4.9.1 用户人脸注册**



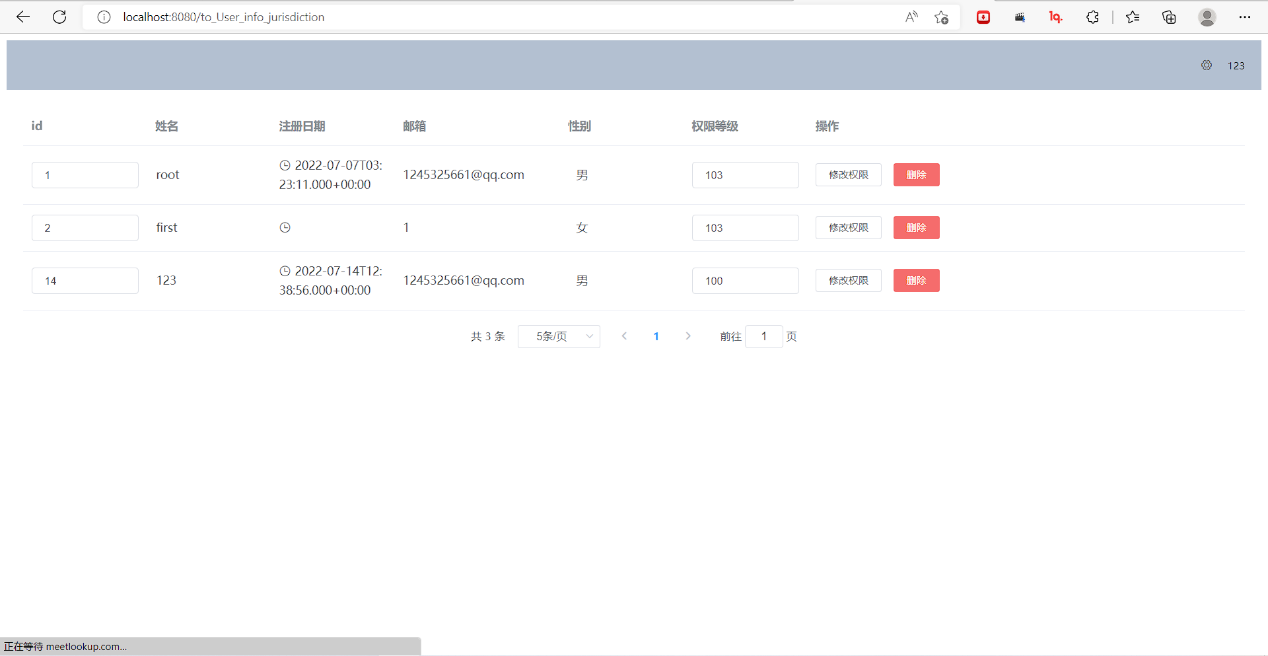
管理员可以上传人脸照片进行注册





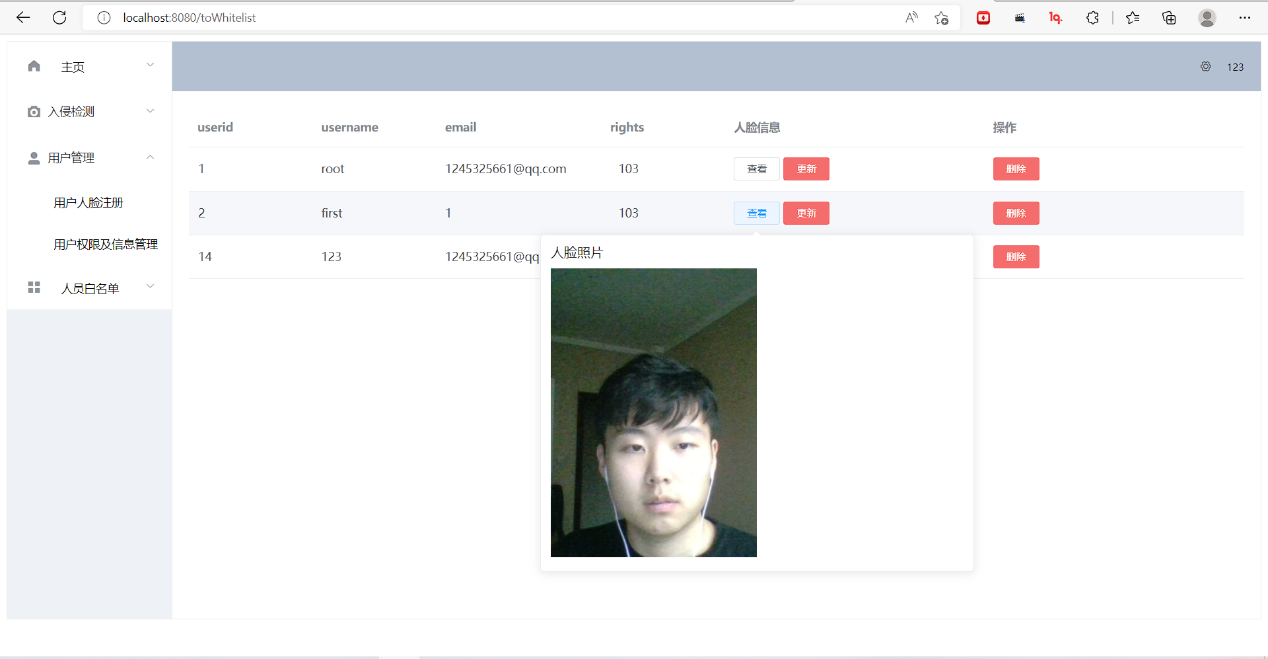
也可以现场拍照上传

**3.4.9.2 用户权限及信息管理**



管理员可以修改对应用户的权限等级

**3.4.10 白名单列表**

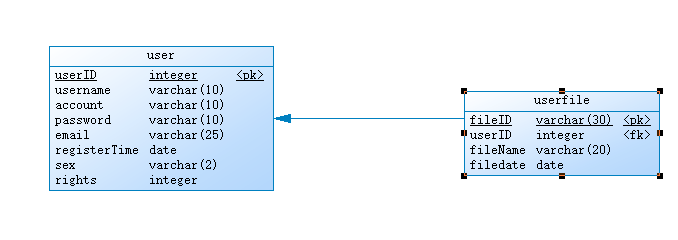


在白名单里的人员进入视频监测区域不会报警，管理员可以查看更新白名单人员里的人脸信息，也可以删除白名单里的人员。

**4.数据库设计**

**4.1物理模型**

以下是基于MySQL的物理模型。



其中user表是用户信息表，userfile表示存在mongodb数据库里文件的信息，可以通过该信息在mongodb进行查询。

**4.2 非关系型数据库**

当有入侵发生，系统完成警报发送、警报推送、警报处理的功能，同时管理员可以对警报信息进行查询。