**一、安全性与稳定性**

1. **非法操作**的处理

*路由导航守卫*：①用户未登录（sessionStorage中token不存在）状态下→如果用户企图在网址栏输入内部网页链接（如”http://localhost:8080/#/search”等），拦截该请求并强制跳转至登录页面；②已登录状态下，在网址栏输入非法网址尝试跳转（如登录”[http://localhost:8080/#/login](http://localhost:8080/" \l "/login)”或注册、忘记密码等页面），请求不被执行；③在sessionStorage中存在token且与后端值相等时，判断浏览器Cookies中的role值是否与后端相等，条件成立时才可以继续执行。

***动态路由***：在登录的时候，根据后端返回的role值动态添加路由。如”role = volunteer”，则添加**属于该角色的志愿者动态组件**，在该状态下能且只能访问志愿者的组件（①无法访问其他角色的动态组件；②在每次到达新的网页前，上传该用户下的token和role值至后端服务器，判断数据是否一致，防止缓存数据被恶意篡改），效果图如下：



图1-1，账号的角色为志愿者

图1-2，动态添加属于该角色的组件



图1-3，无法访问属于其他角色的组件

*请求拦截器*：略。

1. 当输入不匹配的url时，跳转至**404页面**。

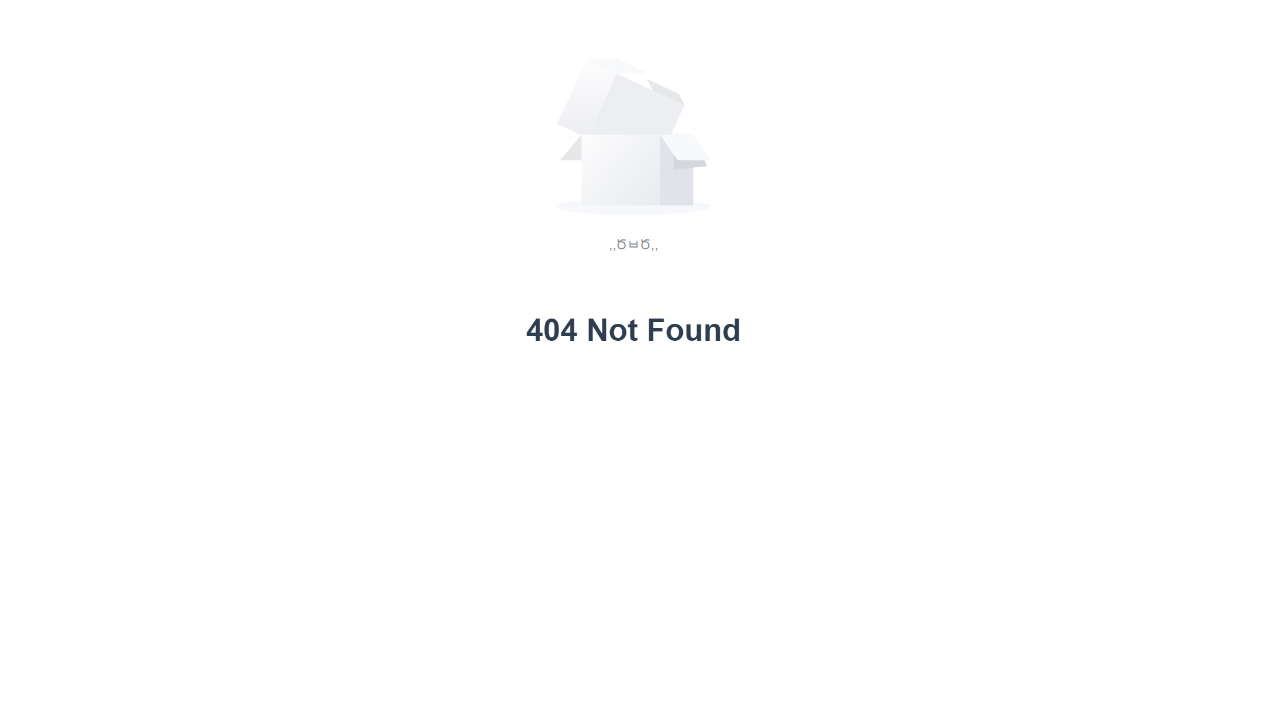


图1-4，404页面

1. **数据接口**（测试）
2. 登录页面：

用户点击“登录”，<url:’/login’,method:’POST>’，表单提交用户信息数据结构：

{

username(id): '\*', // 用户名（身份证号）

password: '\*', // 密码

}

如果账号或密码错误，后端返回{data: ‘user\_error’}；否则返回

data:{

username(id): '\*', // 用户名（身份证号）

//avatar: '\*.jpg', // 头像

token: '\*', // 密钥，后端的token初始值为空会有安全风险

role: '\*', // 用户角色，\*={村居:villager, 志愿者:volunteer, 村支部:villageBranch, 乡镇党委:townCommittee, 县委:countyCommittee}

}。

1. 注册页面：
   1. 用户点击“发送验证码”，[url: ’/verifyCode’, method: ’POST](url:’/verifyCode’,%20method:’POST)’，表单提交的数据结构：

{

tel: \*, // 手机号码

}

如果手机号已被注册，返回{code: -1}；否则，返回{code: ‘sent’}。

* 1. 用户点击“注册”，[url: ’/signUp](url:’/signUp)’, method: ‘POST’(GET方式有安全风险)，表单提交：

{

id: \*, // 身份证号(primary key)

username: \*, // 用户名

tel: \*, // 手机号码

password: \*, // 密码

role: \*, // 用户角色

verifyCode: \*, // 验证码

}

发送验证码之后，手机号不允许被修改，如果需要修改手机号，需要重新填写。**后端再次判断手机号是否被修改？**

后端判断身份证号是否已被注册，如果已被注册，返回{'identity\_status': -1}；否则，返回{'identity\_status': 1}。

后端判断验证码是否一致，如果不一致，返回{'code\_status': -1}；否则，返回{'code\_status': 1}。

1. 路由导航守卫（页面验证）：

用户每到达一个新的页面之前，都会将sessionStorage中的token、username和Cookies中的role发送至后端，url: '/certification', method: 'POST'，提交的数据结构为：

{

'token': \*,

'role': \*,

'id': \* // id === username === 身份证号，primary key，用来匹配信息

}

后端验证数据有效性，返回布尔值。

1. 报表查询：

url: '/getTable', method: 'GET'

后端返回数据

tableData = [

{

type: "到户联系",

volunteer: "\*",

villager: "\*",

district: '保靖县/\*乡/A村',

detail: '\*'

},

{

type: "民情走访",

volunteer: "\*",

villager: "\*",

district: '保靖县/\*乡/A村',

detail: '\*'

},

……

]

**三、功能**

1. 登录：

根据role和rightList，动态添加路由规则，分配给不同角色不同的权限，除公共页面之外，可以为每一种角色单独展示只属于该角色的系统页面。

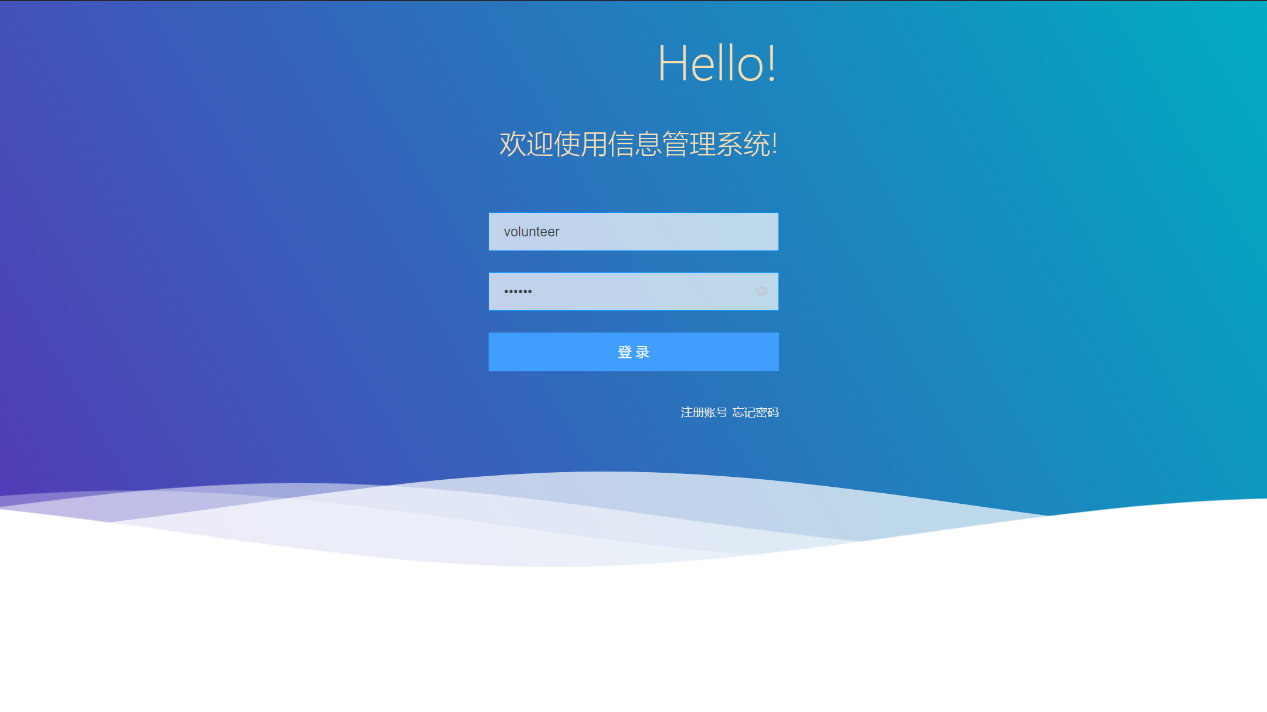


图3-1，登录页面

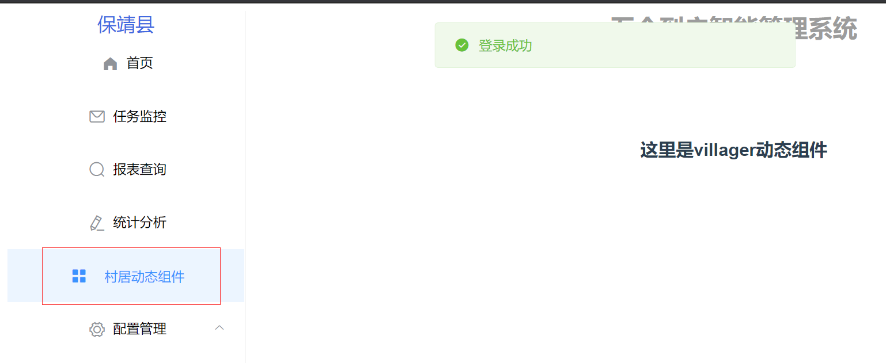


图3-2，“村居”角色的动态组件



图3-3，“村支部”角色的动态组件

1. 注册页面：

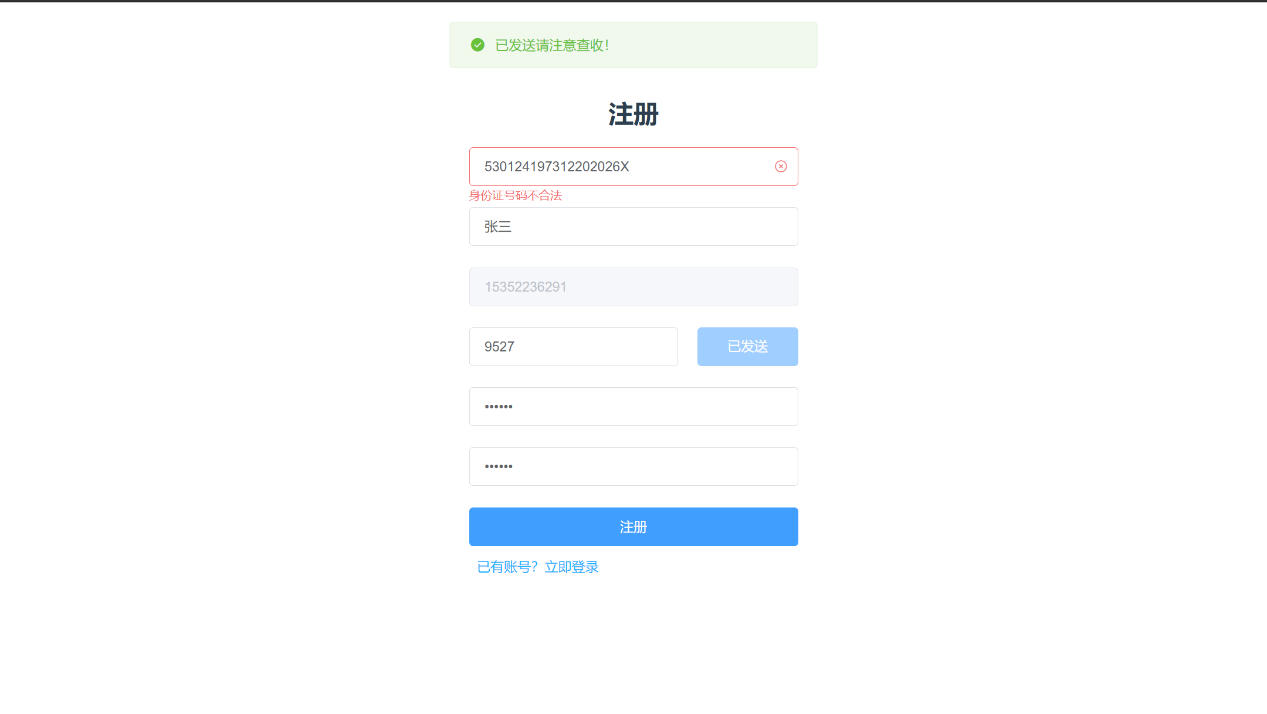


图3-4，注册页面（1）



图3-5，注册页面（2）

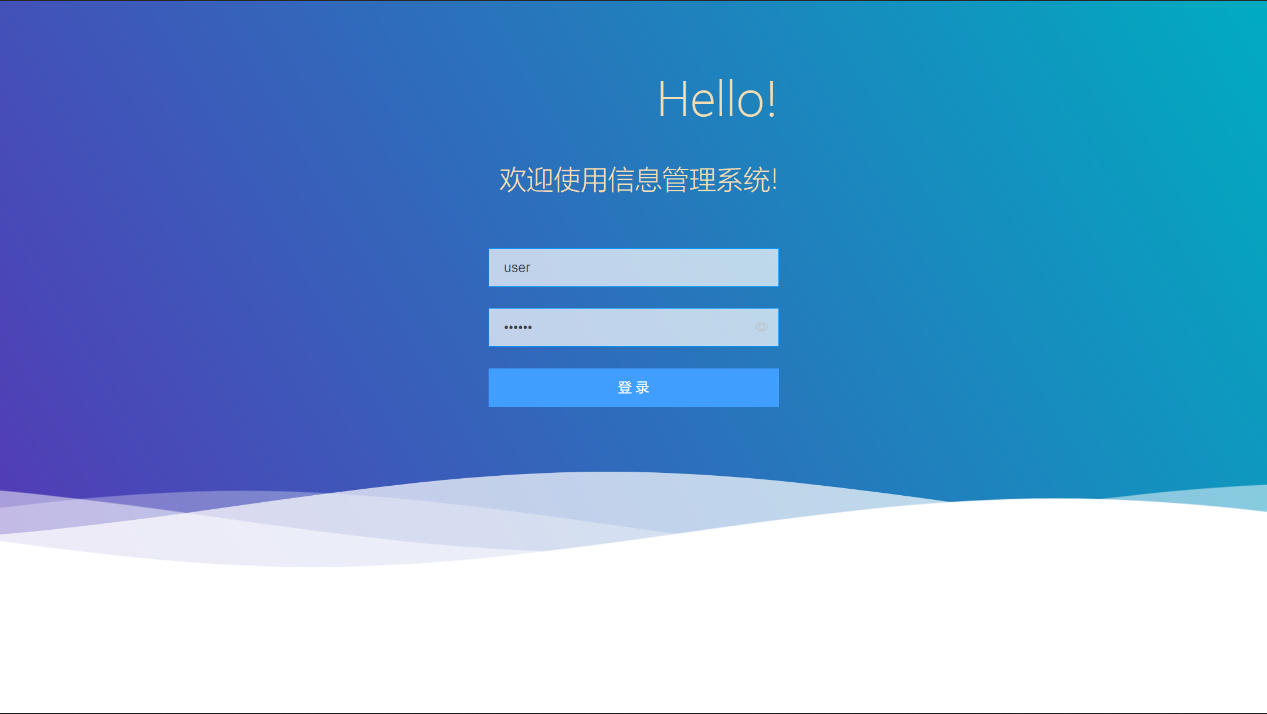
1. 忘记密码：

暂未开发。

**四、可能存在的问题**

|  |  |
| --- | --- |
| 问题描述 | 解决办法 |
| “无痕浏览”模式导致缓存失效 | 关闭“无痕浏览”即可 |
| 前端对用户访问和操作权限控制存在的漏洞不可避免 | 用户对于敏感数据的访问和操作，必须由后端再次确认 |

附，开发图预览：



Pic-登录页面



Pic-主界面