

امنیت اطلاعات

پیاده سازی سامانه چت امن

زهره رستمی 9912762858 – الهه رضاپناه 9912762789

مینی پروژه

پروژه "Secure Chat" به منظور ایجاد یک سیستم چت امن طراحی شده است که کاربران بتوانند به صورت خصوصی و گروهی با یکدیگر ارتباط برقرار کنند. این سیستم از رمزنگاری و امضای دیجیتال برای تأمین امنیت پیامها استفاده می کند تا اطلاعات کاربران در طول ارسال و دریافت به صورت محرمانه باقی بماند.

در این سامانه کاربران با استفاده از socket ها به سرور و همدیگر وصل شدند و دیتاهایی که باید ذخیره سازی شوند در فایل های json ذخیره و هندل می شوند.

بخش های مختلف سامانه:

1- ثبت نام

کاربران جدید می توانند با ارائه اطلاعات ایمیل، نام کاربری و رمز عبور خود در سیستم ثبت نام کنند. هنگام ثبت نام، سیستم:

- بررسی می کند که ایمیل وارد شده تکراری نباشد.
- رمز عبور کاربر را به وسیله PBKDF2 با استفاده از salt رمزنگاری می کند.
- یک جفت کلید RSA برای هر کاربر ایجاد می شود که شامل کلید خصوصی و عمومی است.
- اطلاعات کاربر شامل نام کاربری، ایمیل، رمز عبور رمزنگاری شده، salt، کلید خصوصی و کلید عمومی در فایل JSON ذخیره می شود.

2- ورود

کاربران ثبت نام شده می توانند با استفاده از ایمیل و رمز عبور خود وارد سیستم شوند. هنگام ورود، سیستم:

- اطلاعات ایمیل و رمز عبور وارد شده را با اطلاعات موجود در فایل JSON مقایسه می کند.
- رمز عبور وارد شده را با استفاده از salt مربوط به کاربر و PBKDF2 رمزنگاری کرده و با رمز عبور ذخیره شده مقایسه می کند.
- در صورت تطابق، دسترسی به سیستم برای کاربر فراهم می شود.

3- چت خصوصی

کاربران می توانند به صورت امن با دیگر کاربران پیام خصوصی ارسال کنند. هنگام ارسال پیام خصوصی، سیستم:

- پیام را با استفاده از کلید عمومی گیرنده رمزنگاری می کند.
- پیام رمزنگاری شده را با استفاده از کلید خصوصی فرستنده امضا می کند.
- پیام رمزنگاری شده و امضا شده در فایل JSON مربوط به پیامها ذخیره می شود.

4- چت گروهی

کاربران می‌توانند گروه‌های چت ایجاد کرده و به اعضای گروه پیام ارسال کنند.

- ایجاد گروه: کاربر می‌تواند با ارائه یک شناسه گروه، یک گروه جدید ایجاد کند. شناسه گروه و اعضای گروه در فایل JSON ذخیره می‌شود.
- اضافه کردن عضو به گروه: فقط سازنده گروه می‌تواند اعضای جدید را به گروه اضافه کند.
- حذف عضو از گروه: فقط سازنده گروه می‌تواند اعضا را از گروه حذف کند.
- ارسال پیام گروهی: پیام برای هر عضو گروه به صورت جداگانه با کلید عمومی آنها رمزنگاری و امضا می‌شود و سپس در فایل JSON مربوط به پیام‌ها ذخیره می‌شود.

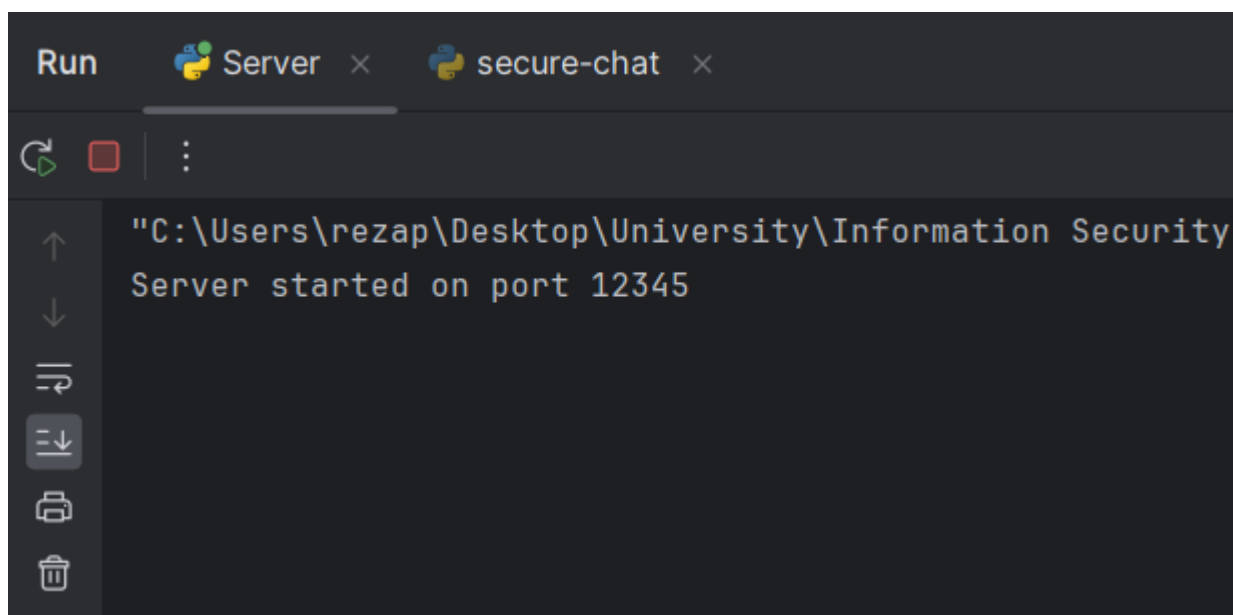
5- مدیریت کاربران

سیستم اطلاعات کاربران را در فایل JSON مدیریت می‌کند که شامل ایمیل، نام کاربری، رمز عبور رمزنگاری شده، salt، کلید خصوصی و کلید عمومی است.

- اطلاعات کاربران به صورت رمزنگاری شده و امن ذخیره می‌شود.
- هنگام ورود و ثبت نام، صحت اطلاعات کاربران بررسی می‌شود.

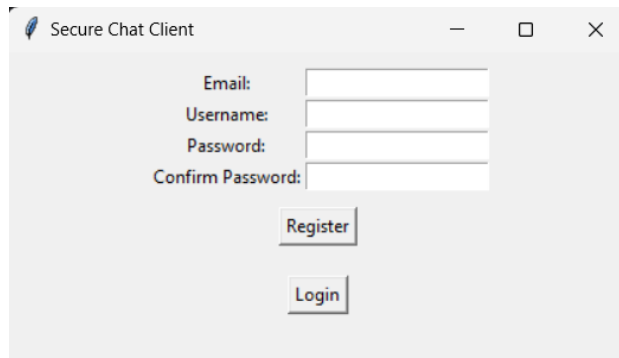
خروجی‌های نهایی:

شروع کار سرور)



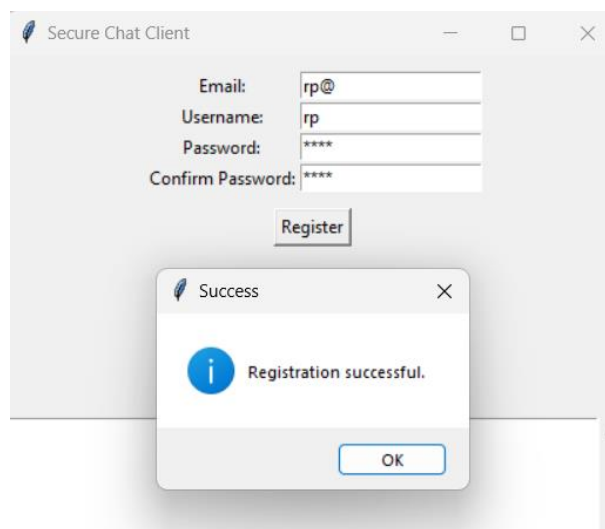
```
Run  Server  secure-chat
C:\Users\rezap\Desktop\University\Information Security
Server started on port 12345
```

صفحه ثبت نام و ورود)



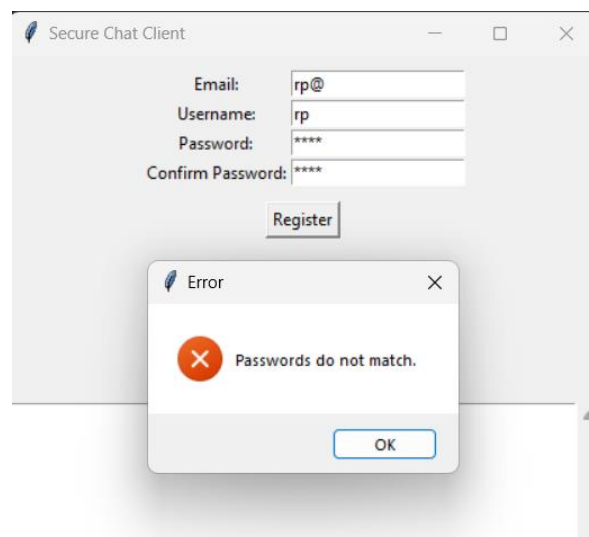
The image shows a window titled "Secure Chat Client" with a registration form. The form contains four input fields: "Email:", "Username:", "Password:", and "Confirm Password:". Below the fields are two buttons: "Register" and "Login".

در این بخش کاربر با وارد کردن ایمیل، نام کاربری و رمز بسته به نیاز ثبت نام یا ورود به اکانتش میکند.



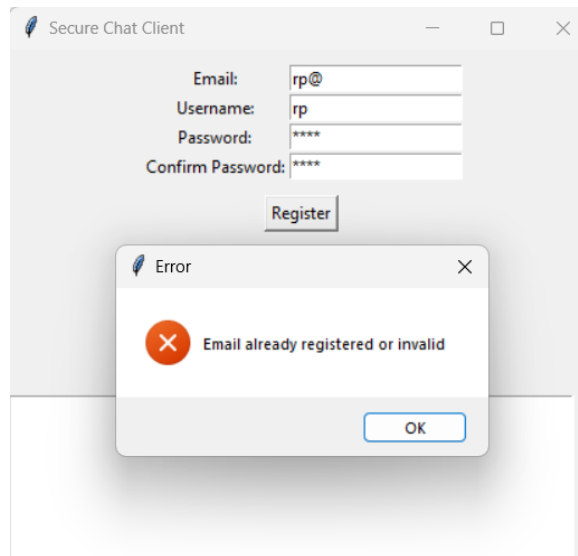
The image shows the "Secure Chat Client" window with the registration form filled out. The "Email" field contains "rp@", "Username" contains "rp", "Password" contains "****", and "Confirm Password" contains "****". The "Register" button is highlighted. A small dialog box titled "Success" is open in the foreground, displaying a blue information icon and the text "Registration successful." with an "OK" button.

در صورتی که تایید پسورد متفاوت باشد ارور خواهیم داشت:

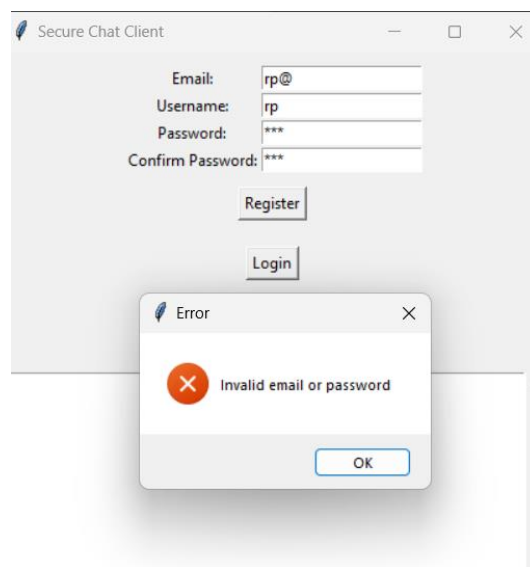


The image shows the "Secure Chat Client" window with the registration form filled out. The "Email" field contains "rp@", "Username" contains "rp", "Password" contains "****", and "Confirm Password" contains "****". The "Register" button is highlighted. A small dialog box titled "Error" is open in the foreground, displaying a red error icon and the text "Passwords do not match." with an "OK" button.

در صورتی که ایمیل ثبت نام شده باشد، ارور خواهیم داشت که این کاربر قبلا ثبت نام شده



و در صورت اشتباه وارد کردن هر یک از اطلاعات و مغایرت با اطلاعات ذخیره شده هم ارور دریافت میشود.



کاربر پس از ثبت نام میتواند وارد صفحه اکانت خود شود.

Secure Chat Client

Fetch Messages

Receiver:

Message:

Send

Group ID:

Create Group

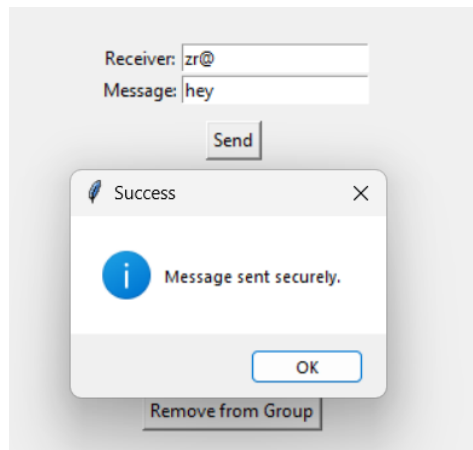
Add to Group

Remove from Group

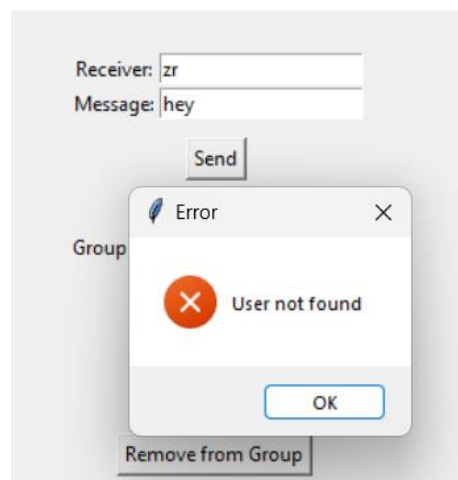
Send Group Message

صفحه چت خصوصی)

هر کاربر در صفحه اکانت خود با وارد کردن ایمیل گیرنده و نوشتن پیامش در اینپوت مشخص شده میتواند به هر کاربری که در سیستم ثبت نام شده پیام خصوصی ارسال کند.



در صورت نبودن اون کاربر در سیستم خطا دریافت میشود.

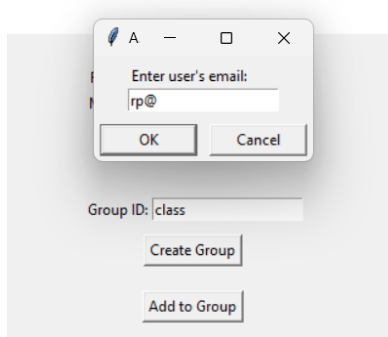
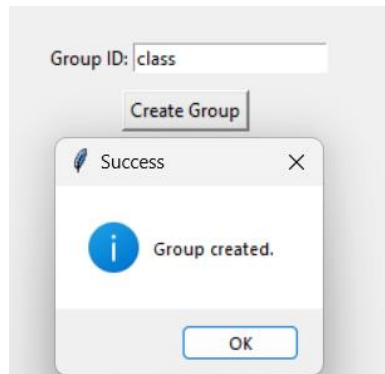


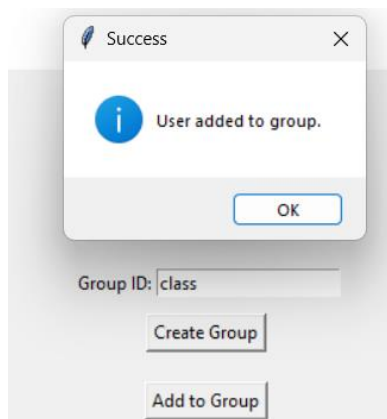
هر کاربر در صفحه اکانت خود با زدن fetch messages می توانند پیام های دریافتی خود را مشاهده کند.



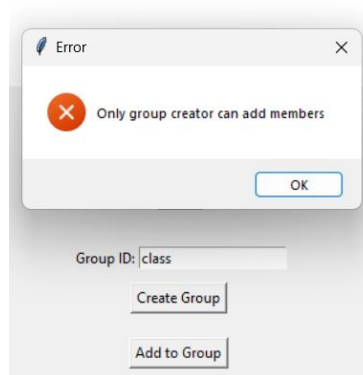
صفحه چت گروهی)

هر شخص در سیستم قادر است با مشخص کردن یک ID گروهی بسازد و اعضای مورد نظرش رو در اون گروه اضافه کند.

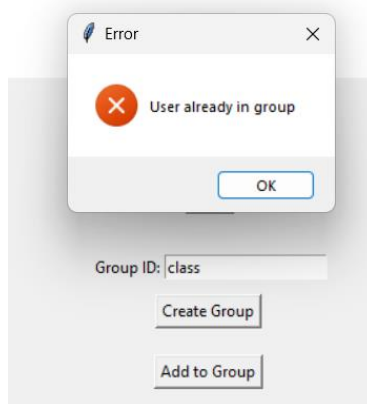




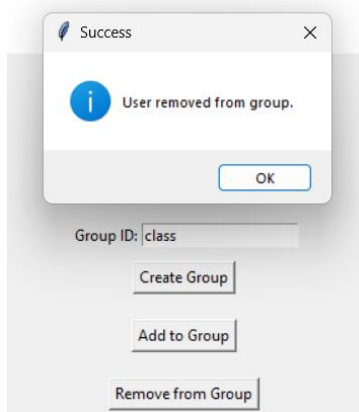
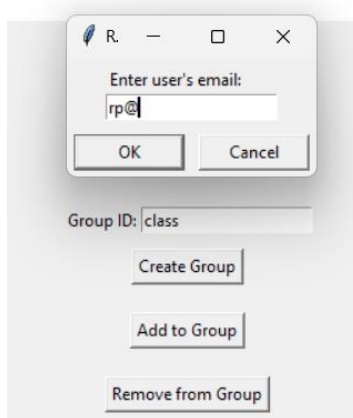
قابلیت های حذف و اضافه کردن اعضا به گروه هم صرفا توسط سازنده گروه قابل انجام است.



و در صورت تلاش برای اد کردن کاربری در گروه که قبلا اد شده هم ارور دریافت میشود.



و فرآیند حذف عضو از گروه هم به همین ترتیب فقط توسط سازنده گروه قابل انجام هست.



برای ارسال پیام در گروه با وارد کردن ID گروه و نوشتن پیام و انتخاب گزینه ارسال پیام گروهی توسط اعضای آن گروه پیام برای همه ی اعضای آن گروه با ذکر شدن نام گروه در صفحه پیام های دریافتی آنها نمایش داده می شود.

Success

Group message sent securely.

OK

Receiver:

Message:

Im tired _-

Send

Group ID:

class

Create Group

Add to Group

Remove from Group

Send Group Message

From: zr@

Group: class

Message: Im tired _-

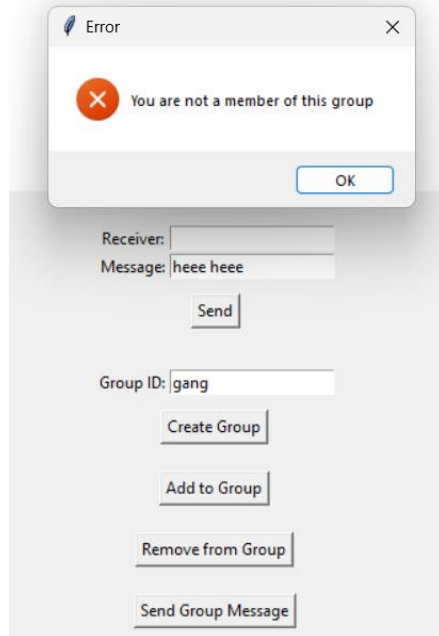
Receiver:

Message:

Send

Group ID:

و در صورتی که کسی که در گروهی حضور ندارد اقدام به ارسال پیام در آن گروه کند با خطا مواجه میشود.



دیتا ها)

تمامی دیتاهایی که باید ذخیره شوند در فایل های json قرار گرفته و در سیستم هندل میشوند.

اطلاعات کاربران: (user-data.json)

```
{
  "rp@": {
    "username": "rp",
    "password": "jFtLn85wQqx4VfL2pgJipHvXP5hy6dvKlf3pL0ruKA=",
    "salt": "ctYSqBep8zZM3bbnhS80wg=",
    "private_key": "-----BEGIN RSA PRIVATE KEY-----\nMIIeowIBAAKCAQEAnxFT/Kw0vPAYN45+2B2urUEBoSJKVPixbFHQ/vKTHnJVF1RT\nny7D4Ns",
    "public_key": "-----BEGIN PUBLIC KEY-----\nMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnxFT/Kw0vPAYN45+2B2u\nnrUEBoSJKVPix",
  },
  "zr@": {
    "username": "zr",
    "password": "U7iZb6u6HvvHifhz1uW20WoL5IRJcLmKhWqAhzBmWW4=",
    "salt": "1tQcdGAJ148uFv0JkdjVaQ=",
    "private_key": "-----BEGIN RSA PRIVATE KEY-----\nMIIeogIBAAKCAQEAqn/HMBLI6bCp/YnFjW0rSZU0HjNjX88zrU1liwPBqUEA6piy\nnPwtVrF",
    "public_key": "-----BEGIN PUBLIC KEY-----\nMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqn/HMBLI6bCp/YnFjW0r\nnSZU0HjNjX88z",
  },
  "jk@": {
    "username": "jk",
    "password": "qNLCjmiKtiawMVnSSlnJX0MgVEWjc05Qf1VTPlpf0x4=",
    "salt": "3mnP0sMFHnUt0D63aJH7WQ=",
    "private_key": "-----BEGIN RSA PRIVATE KEY-----\nMIIeowIBAAKCAQEA5ZMD8mRckDasZ9RzLfgacMsjX2R903IL88X21C40zsmD9Fd\nnLKbsar",
    "public_key": "-----BEGIN PUBLIC KEY-----\nMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5ZMD8mRckDasZ9RzLfga\nncMsjX2R903IL",
  }
}
```

اطلاعات گروه ها: (group_data.json)

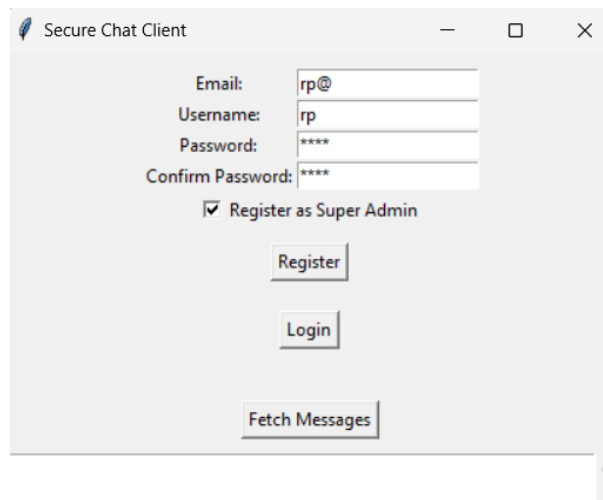
```
{
  "class": {
    "creator": "zr@",
    "members": [
      "zr@",
      "rp@",
      "jk@"
    ]
  },
  "gang": {
    "creator": "rp@",
    "members": [
      "rp@",
      "jk@"
    ]
  }
}
```

اطلاعات پیام ها: (messages_data.json)

```
{
  "zr@": [
    {
      "sender": "rp@",
      "encrypted_message": "d5Veedum5m0bkTzQEEx2cznPbgzKEz94DnCNhi03MvBQ0Q+QN7Nm",
      "signature": "Cjv9kJs4MXn9tBhb9hgwLXmjwQjZ3ghWqnLM773+IFF3mQ02xHEGT7Ij3zS1"
    }
  ],
  "rp@": [
    {
      "sender": "zr@",
      "encrypted_message": "gnZpg2wkbs8kH4mW3WRgYxSi29C0WpoKTjQE0B3oAgkFFBYfFBxJ",
      "signature": "FK1rmv17WDXyiWENVouRGytrewUrCKxEVpJPK+WFCdnVQjKLeJX/fs9Bhsf"
    }
  ]
}
```

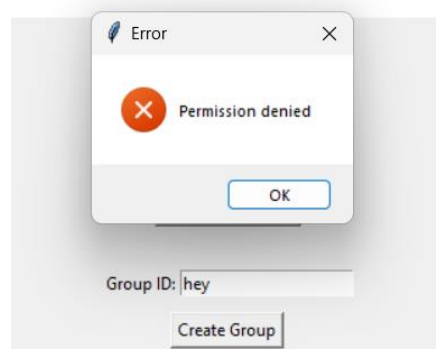
مدیریت کاربران

در هنگام ثبت نام گزینه ای به عنوان ثبت نام در نقش super admin وجود دارد که اگر زده بشه اون شخص سوپر ادمین میشود و در صورت نزدن اون گزینه user به عنوان نقش در نظر گرفته می شود.



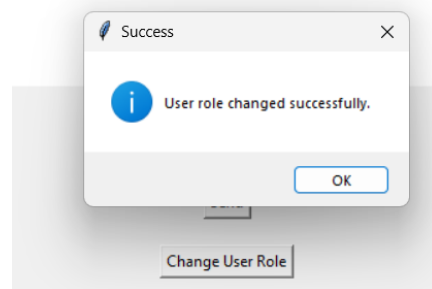
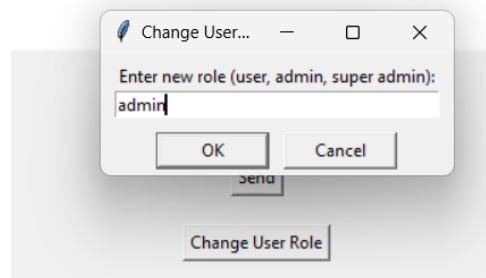
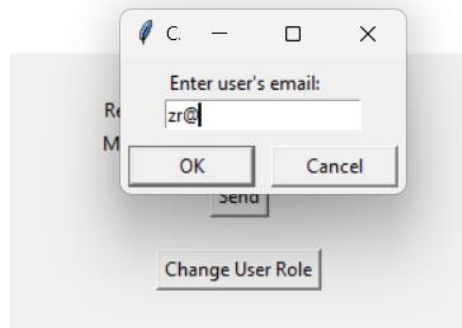
The image shows a 'Secure Chat Client' window with a registration form. The form includes fields for 'Email' (containing 'rp@'), 'Username' (containing 'rp'), 'Password' (containing '****'), and 'Confirm Password' (containing '****'). There is a checkbox labeled 'Register as Super Admin' which is checked. Below the form are three buttons: 'Register', 'Login', and 'Fetch Messages'.

```
{
  "rp@": {
    "username": "rp",
    "password": "57X2gBuifEZh7ehMaos1jgNW2ZWk8wFHjECUVH32kNY=",
    "salt": "BXb09KNCg-33fy_XaeioLw==",
    "private_key": "-----BEGIN RSA PRIVATE KEY-----\nMIIEogIBAAKCAQEAodx0XJnxbpHLDwF",
    "public_key": "-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC",
    "role": "super admin"
  },
  "zr@": {
    "username": "zr",
    "password": "6BjqSti75y7RA1fhXrzj05Ffq7hq036V8PhYRWxw404=",
    "salt": "I3AKd8CcacZ2iHR3k77VcA==",
    "private_key": "-----BEGIN RSA PRIVATE KEY-----\nMIIEpAIBAAKCAQEA7c0yf+Zk4Kdq0z2",
    "public_key": "-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC",
    "role": "user"
  }
}
```

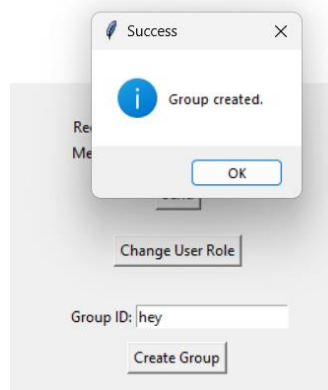


The image shows an 'Error' dialog box with a red 'X' icon and the text 'Permission denied'. Below the dialog box is a text input field labeled 'Group ID:' containing the text 'hey', and a 'Create Group' button.

و همچنین super admin توانایی تعویض نقش کاربران را دارد.



و زمانی که شخص admin میشود توانایی زدن گروه را دیگر دارد.



پروژه پایانی)

دارایی‌ها:

1- سرور و زیرساخت‌های شبکه:

- سرور اصلی
- شبکه و زیرساخت‌های ارتباطی
- پایگاه‌های داده

2- نرم‌افزارها و سرویس‌ها:

- کد سرور (server.py)
- کد کلاینت (secure-chat.py)
- کتابخانه‌های مورد استفاده (مثل cryptography)
- فایل‌های داده (user_data.json, group_data.json, messages_data.json)

3- اطلاعات و داده‌ها:

- اطلاعات کاربران (ایمیل، رمز عبور، کلیدهای رمزنگاری)
- پیام‌های چت خصوصی
- پیام‌های گروهی

4- روابط و ارتباطات:

- ارتباطات کاربران با سرور
- ارتباطات سرور با پایگاه‌های داده
- ارتباطات کاربران با یکدیگر در چت‌های خصوصی و گروهی

ارزش‌گذاری دارایی‌ها:

1- سرور و زیرساخت‌های شبکه:

اهمیت: بسیار بالا

ارزش: سرور اصلی که بستر اجرای سیستم است، در صورت خرابی کل سیستم از کار خواهد افتاد. درواقع امنیت سرور باید تضمین شود تا از نفوذ و حملات جلوگیری شود.

2- نرم‌افزارها و سرویس‌ها:

اهمیت: بالا

ارزش: کد سرور و کلاینت برای اجرای صحیح سیستم حیاتی هستند. هرگونه نقص در این کدها می‌تواند منجر به مشکلات امنیتی و عملکردی شود.

3- اطلاعات و داده‌ها:

اهمیت: بسیار بالا

ارزش: اطلاعات کاربران و پیام‌های چت خصوصی و گروهی از حساس‌ترین دارایی‌ها هستند. در صورت دسترسی غیرمجاز به این اطلاعات، می‌تواند منجر به آسیب‌های جدی به حریم خصوصی کاربران و اعتبار سیستم شود. همچنین در صورت نقض می‌تواند منجر به از دست رفتن اعتماد کاربران و پیامدهای قانونی شود.

4- روابط و ارتباطات:

اهمیت: بالا

ارزش: ارتباطات ایمن بین کاربران و سرور برای عملکرد صحیح سیستم و حفظ امنیت اطلاعات بسیار مهم است.

تشخیص آسیب‌پذیری‌ها:

برای تشخیص آسیب‌پذیری‌ها، باید نقاط ضعف و نقص‌های موجود در سیستم که می‌توانند مورد سوءاستفاده قرار گیرند، شناسایی شوند.

1- سرور و زیرساخت‌های شبکه:

- عدم پیکربندی صحیح فایروال و پورت‌ها
- عدم مانیتورینگ و مدیریت لاگ‌ها
- عدم استفاده از SSL/TLS برای ارتباطات شبکه
- دسترسی غیرمجاز به سرور می‌تواند منجر به افشای اطلاعات حساس شود
- حملات مرد میانی (MITM) اگر ارتباط بین کلاینت و سرور امن نباشد، مهاجم می‌تواند پیام‌ها را شنود و تغییر دهد.

2- نرم‌افزارها و سرویس‌ها:

- نقاط ضعف در کدهای سرور و کلاینت
- وابستگی به کتابخانه‌های شخص ثالث با نسخه‌های قدیمی و آسیب‌پذیر

3- اطلاعات و داده‌ها:

- ذخیره رمزهای عبور بدون رمزنگاری مناسب
- مدیریت نادرست کلیدهای رمزنگاری
- ذخیره اطلاعات حساس در فایل‌های JSON بدون رمزنگاری (رمز عبورها و کلیدهای خصوصی باید به صورت امن ذخیره شوند).
- حملات Brute Force: تلاش برای کشف رمز عبور کاربران از طریق حملات فراگیر.

4- روابط و ارتباطات:

- عدم احراز هویت صحیح کاربران
- استفاده از پروتکل‌های ناامن برای ارتباطات
- عدم بررسی صحت پیام‌ها و امضاها
- عدم کنترل دسترسی مناسب: امکان ارسال پیام در گروه‌ها توسط افراد غیرمجاز.

تحلیل آسیب پذیری ها:

1- سرور و زیرساخت های شبکه:

- تأثیر: بالا
- احتمال بهره برداری: متوسط
- اولویت: بالا

2- نرم افزارها و سرویس ها:

- تأثیر: بالا
- احتمال بهره برداری: بالا
- اولویت: بسیار بالا

3- اطلاعات و داده ها:

- تأثیر: بسیار بالا
- احتمال بهره برداری: بالا
- اولویت: بسیار بالا

4- روابط و ارتباطات:

- تأثیر: بالا
- احتمال بهره برداری: متوسط
- اولویت: بالا

5- حملات مرد میانی (MITM):

- تأثیر: بالا
- احتمال بهره برداری: متوسط
- اولویت: بالا

6- حملات Brute Force:

- تأثیر: متوسط
- احتمال بهره برداری: بالا
- اولویت: بالا

7- عدم کنترل دسترسی مناسب:

- تأثیر: بالا
- احتمال بهره برداری: متوسط
- اولویت: بالا

اقدامات لازم برای رفع آسیب پذیری ها:

1- سرور و زیرساخت های شبکه:

- پیاده سازی SSL/TLS برای تمام ارتباطات شبکه
- پیاده سازی فایروال و IDS/IPS
- پیکربندی مناسب فایروال و محدود کردن پورت ها به ضروری ترین ها
- راه اندازی مانیتورینگ و مدیریت لاگ ها
- محدود کردن دسترسی های فیزیکی و منطقی به سرور
- به روز رسانی مرتب سیستم عامل و نرم افزار های سرور

2- نرم افزار ها و سرویس ها:

- بازبینی و رفع نقاط ضعف در کدهای سرور و کلاینت
- به روز رسانی کتابخانه های استفاده شده و بررسی امنیت نسخه های جدید

3- اطلاعات و داده ها:

- رمزنگاری اطلاعات حساس مثل رمزهای عبور و پیام ها
- استفاده از روش های امن برای مدیریت کلیدهای رمزنگاری
- جلوگیری از ذخیره اطلاعات حساس در فایل های متنی بدون رمزنگاری

4- روابط و ارتباطات:

- احراز هویت کاربران با استفاده از روش های امن
- بررسی صحت پیام ها و امضاها
- استفاده از پروتکل های امن برای تمام ارتباطات

5- حملات مرد میانی (MITM) :

- استفاده از TLS/SSL برای ارتباطات بین کلاینت و سرور
- استفاده از گواهی های دیجیتال معتبر

6- حملات Brute Force:

- پیاده سازی مکانیزم قفل کردن حساب کاربری پس از چندین تلاش ناموفق
- استفاده از CAPTCHA برای تشخیص انسان از ماشین