

گزارش مینی پروژه

هما بدیعی 9912762278

عسل خوش قامت آزاد 9922762231

گزینه های برنامه:

برای اجرای پروژه باید به ترتیب کلاس های CA, Server, SystemHandler اجرا شوند و کلاس SystemHandler باید به تعداد یوزر هایی که می خواهیم در سیستم داشته باشیم، اجرا شود.






با اجرای برنامه منوی زیر نمایش داده می شود:



```
1. Register
2. Login
3. Exit
Enter your choice:
```

که با توجه به اینکه قبلا اکانت ساخته شده یا می خواهیم اکانت بسازیم، login یا register را انتخاب می کنیم.

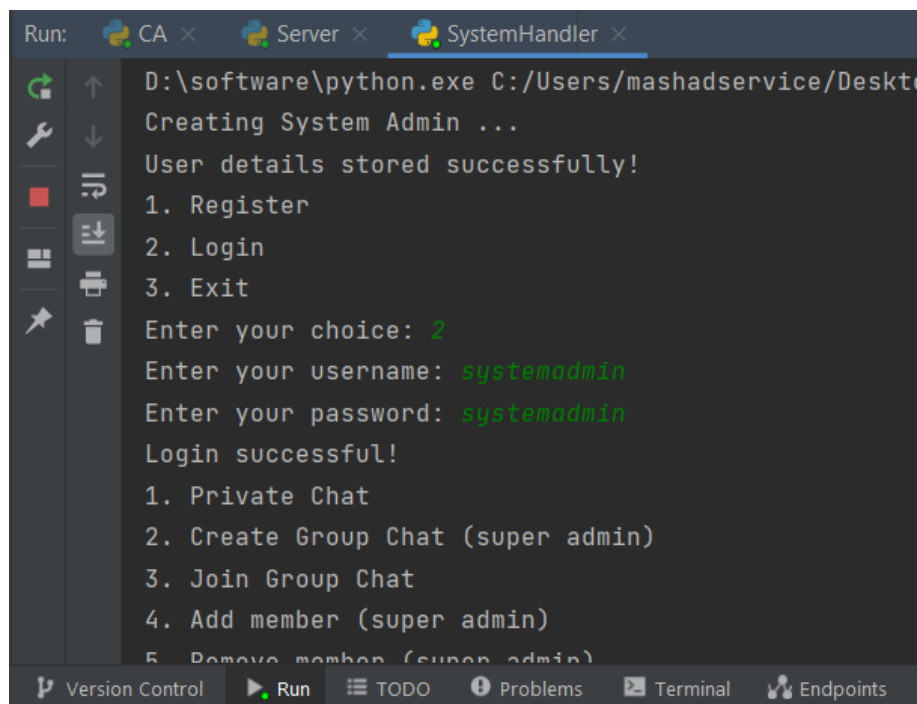
• در صورتیکه انتخاب ما Register باشد:

```
CA x Server x SystemHandler x
D:\software\python.exe C:/Users/mashadservice/Des
1. Register
2. Login
3. Exit
Enter your choice: 1
Enter your email: a@email.com
Enter your username: a
Enter your password: a
Confirm your password: a
User details stored successfully!
1. Register
2. Login
3. Exit
Enter your choice: |
```

> project > SecretFiles				
Name	Date modified	Type	Size	
 a.crt	7/7/2024 1:02 PM	Security Certificate	1 KB	
 CA.crt	7/7/2024 7:19 PM	Security Certificate	1 KB	
 database.txt	7/7/2024 1:06 PM	Text Document	1 KB	
 group_id.txt	7/7/2024 5:47 PM	Text Document	1 KB	
 private_key.pem.encrypted	7/7/2024 7:19 PM	ENCRYPTED File	3 KB	

> project > a				
Name	Date modified	Type	Size	
 a.pem	7/5/2024 12:24 AM	PEM File	2 KB	
 private_key.pem	7/5/2024 12:24 AM	PEM File	2 KB	

- در ابتدای برنامه کاربر systemadmin با دسترسی superadmin ایجاد می شود.

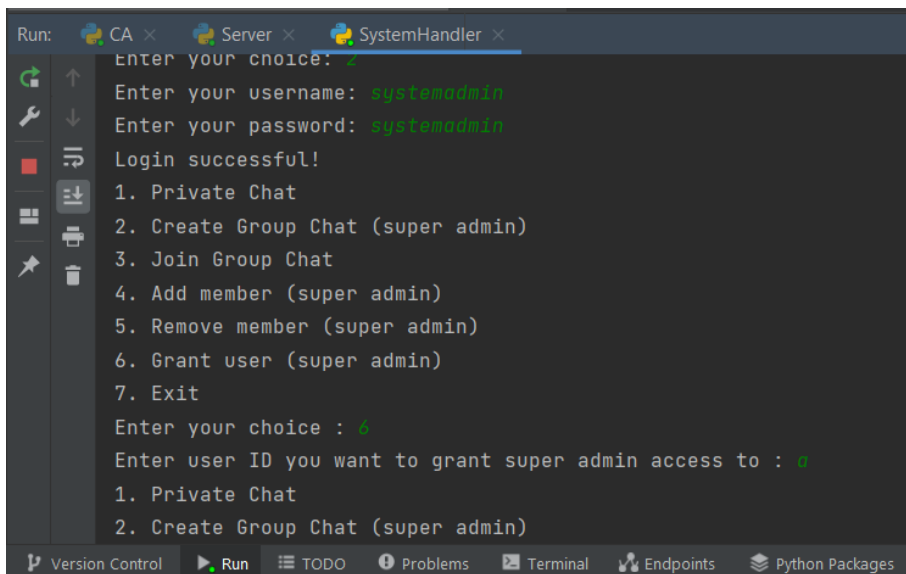


```

Run: CA x Server x SystemHandler x
D:\software\python.exe C:/Users/mashadservice/Desktop/...
Creating System Admin ...
User details stored successfully!
1. Register
2. Login
3. Exit
Enter your choice: 2
Enter your username: systemadmin
Enter your password: systemadmin
Login successful!
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)

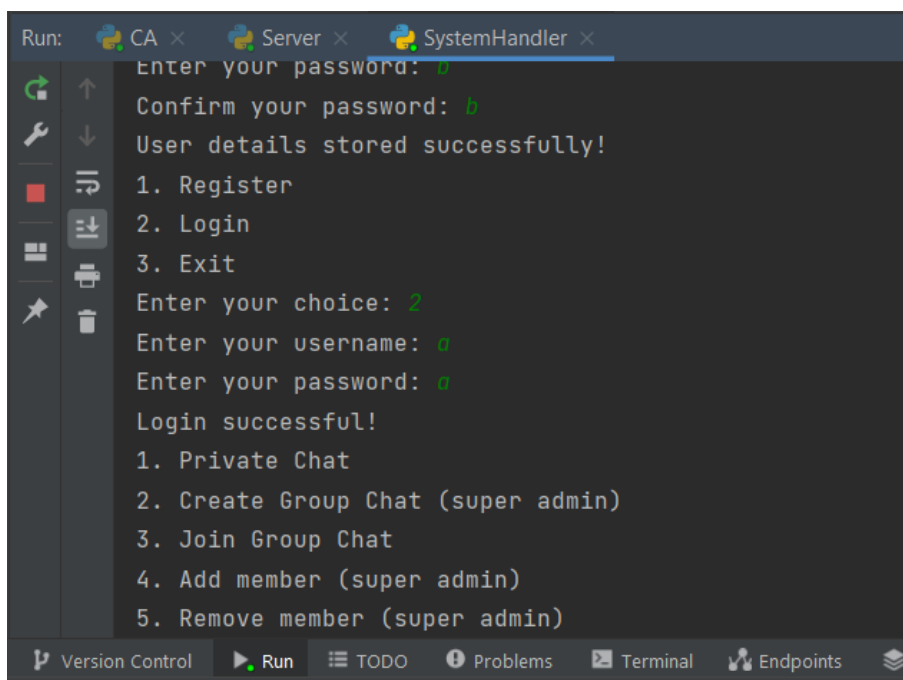
```

با انتخاب گزینه grant user، systemadmin می تواند به یک کاربر عادی سطح دسترسی superadmin اعطا کند تا بتواند گروه ایجاد کند، اعضای را به گروه اضافه کند یا از آن حذف کند.



```
Run: CA x Server x SystemHandler x
Enter your choice: 6
Enter your username: systemadmin
Enter your password: systemadmin
Login successful!
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 6
Enter user ID you want to grant super admin access to : a
1. Private Chat
2. Create Group Chat (super admin)
```

• در صورتیکه انتخاب ما Login باشد:



```
Run: CA x Server x SystemHandler x
Enter your password: a
Confirm your password: b
User details stored successfully!
1. Register
2. Login
3. Exit
Enter your choice: 2
Enter your username: a
Enter your password: a
Login successful!
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
```

بعد از اینکه login با موفقیت انجام شد، منوی انتخاب نوع چت نمایش داده می شود:

1. برای شروع چت فردی بین دو کاربری که login کرده اند.
2. ایجاد یک گروه جدید که فقط توسط superadmin امکان پذیر است.
3. ارسال پیام در گروه به شرط اینکه کاربر عضو گروه باشد و قبلا توسط ادمین به گروه اضافه شده باشد.

4. اضافه کردن کاربر جدید به گروه که فقط توسط superadmin انجام می شود.

5. حذف کاربر از گروه که توسط superadmin انجام می شود.

6. اعطای دسترسی superadmin به اعضای گروه که فقط توسط superadmin انجام می شود.

7. خروج از برنامه.

Options:

(1) Private chat

زمانی که گزینه private chat انتخاب می شود، با توجه به اینکه کاربر می خواهد پیام بفرستد یا پیام دریافت کند، یکی از دو گزینه send message یا receive message را انتخاب می کند:

در حالتی که send message انتخاب شده باشد، نام کاربری شخصی که می خواهد با آن چت کند را وارد می کند.

```
Run: SystemHandler x
Enter your password: 1234
Login successful!
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 1
1. Send Message
2. Receive Message
Enter your choice : 1
Enter the ID you want to chat with : 1
```

```
Run: CA x Server x SystemHandler x
Enter your username: admin
Enter your password: 1234
Login successful!
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 1
1. Send Message
2. Receive Message
Enter your choice : 2
```

یک نمونه چت خصوصی:

```
SystemHandler x
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 1
1. Send Message
2. Receive Message
Enter your choice : 1
Enter the ID you want to chat with : a
hi
b (you) : hi
a : hey
|
```

```
Run: CA x Server x SystemHandler x
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 1
1. Send Message
2. Receive Message
Enter your choice : 2
b : hi
hey
a (you) : hey
|
```

Version Control Run TODO Problems Terminal Endpoints Python

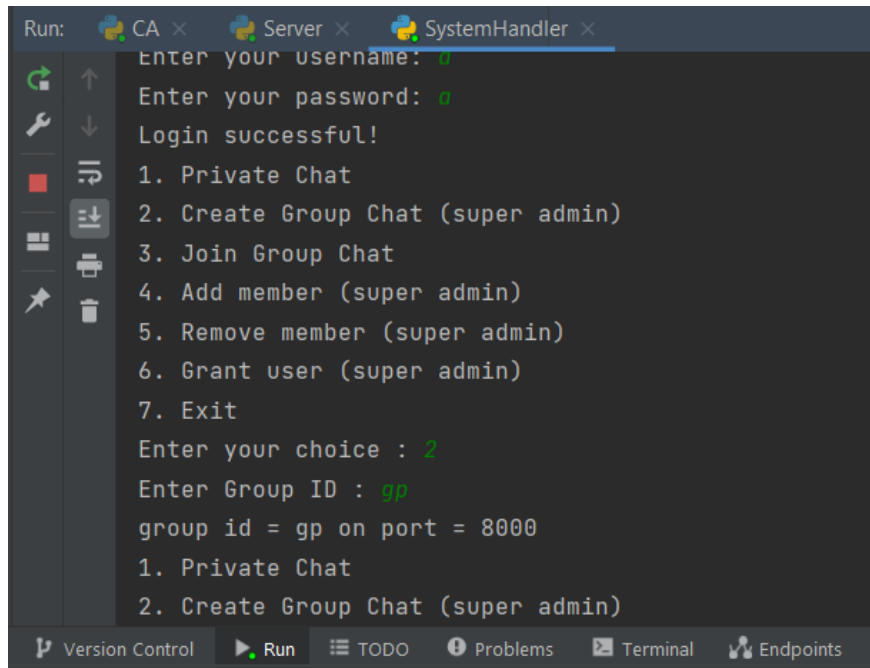
برای خاتمه چت باید عبارت end تایپ شود.

```
Run: CA x Server x SystemHandler x
2. Receive Message
Enter your choice : 2
b : hi
hey
a (you) : hey
end
a (you) : end
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : |
```

```
Run: SystemHandler x
Enter your choice : 1
Enter the ID you want to chat with : a
hi
b (you) : hi
a : hey
a : end
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : |
```

(2) Create group chat

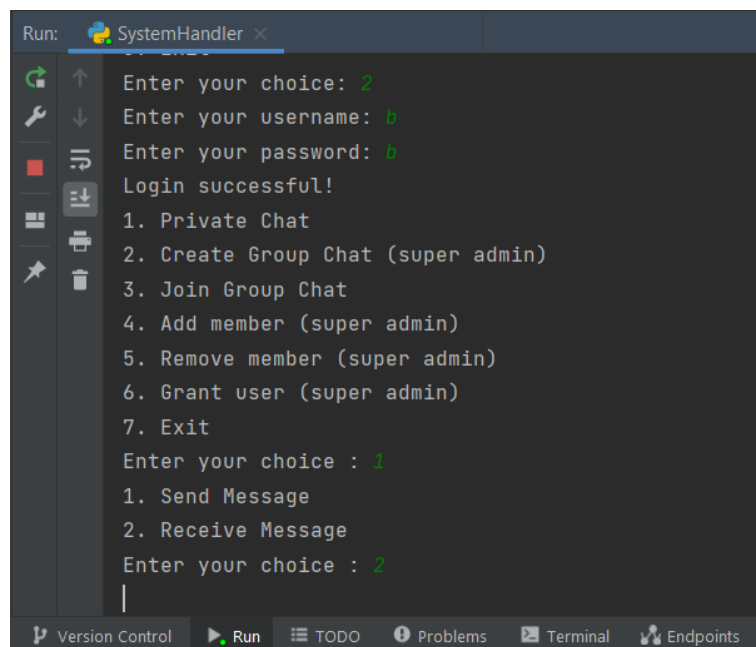
ساخت گروه فقط توسط کاربر با دسترسی **superadmin** امکان پذیر است. ابتدا نام دلخواه برای گروه را وارد می کنیم و بعد از اینکه گروه ساخته شد پیامی شامل اسم گروه و پورتی که گروه بر روی آن ساخته شده نمایش داده می شود و مجدداً منوی قبلی نمایش داده می شود.



```
Run: CA x Server x SystemHandler x
Enter your Username: a
Enter your password: a
Login successful!
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 2
Enter Group ID : gp
group id = gp on port = 8000
1. Private Chat
2. Create Group Chat (super admin)
```

برای اینکه یک کاربر به گروه اضافه شود، این کاربر باید **login** کرده باشد و در حالت **private chat** و در حالت **receive message** قرار داشته باشد. علت اینکه کاربر باید در حالت **receive message** باشد این است که باید اطلاعات گروه و سرتیفیکت ادمین گروه برای کاربری که به گروه قرار است اضافه شود، ارسال شود.

یک سناریو برای ساخت گروه و اضافه کردن اعضا:



```
Run: SystemHandler x
Enter your choice: 2
Enter your username: b
Enter your password: b
Login successful!
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 1
1. Send Message
2. Receive Message
Enter your choice : 2
|
```

لاگین کردن کاربر **b** و قرار گرفتن در حالت **receive message** از اپشن **private chat**

```
Run: CA x Server x SystemHandler x
Enter your password: 
Login successful!
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 2
Enter Group ID : gp
group id = gp on port = 8000
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 4
Enter group ID you want to add member to it : gp
Enter member ID you want to add : b
```

اضافه کردن b به گروه gp توسط ادمین گروه با انتخاب گزینه add member

```
Run: SystemHandler x
6. Grant user (super admin)
7. Exit
Enter your choice : 1
1. Send Message
2. Receive Message
Enter your choice : 2
added to group id = gp on port = 8000
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : |
```

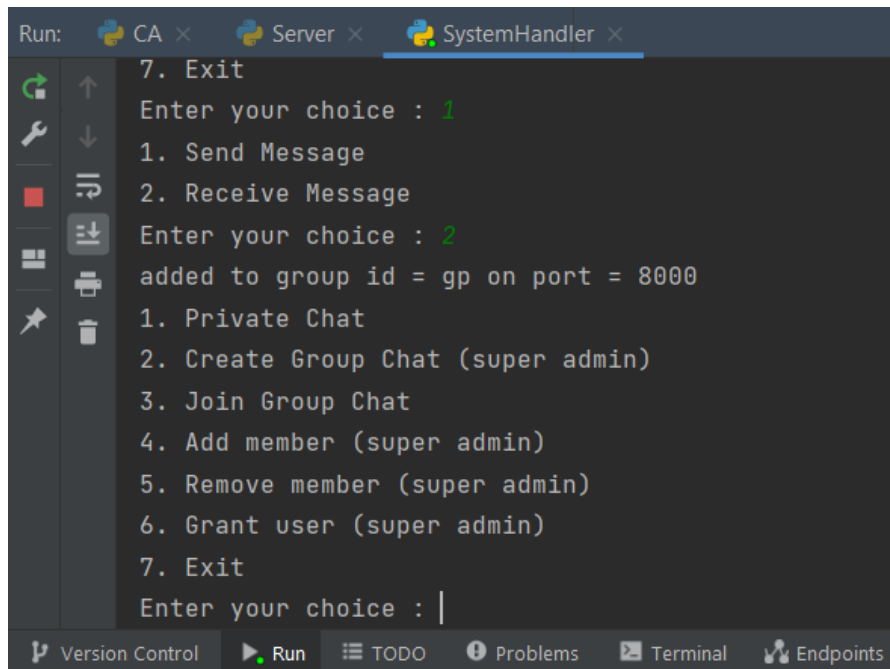
به کاربر b اعلام می شود که به گروه gp اضافه شده است


```
Run: CA x Server x SystemHandler x
Enter your choice: 2
Enter your username: c
Enter your password: c
Login successful!
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 1
1. Send Message
2. Receive Message
Enter your choice : 2
|
```

لاگین کردن کاربر c و قرار گرفتن در حالت receive از ایشن private chat

```
Run: CA x Server x SystemHandler x
7. Exit
Enter your choice : 4
Enter group ID you want to add member to it : gp
Enter member ID you want to add : b
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 4
Enter group ID you want to add member to it : gp
Enter member ID you want to add : c
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : |
```

اضافه کردن کاربر c به گروه gp توسط ادمین گروه



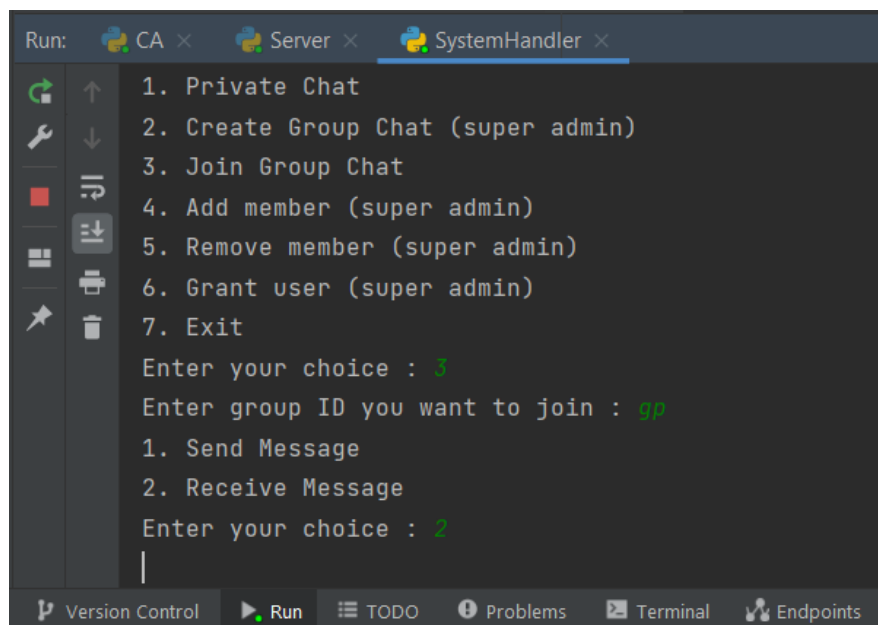
```
Run: CA x Server x SystemHandler x
7. Exit
Enter your choice : 1
1. Send Message
2. Receive Message
Enter your choice : 2
added to group id = gp on port = 8000
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 3
```

به کاربر c اعلام می شود که به گروه gp اضافه شده است.

3) Join group chat

این گزینه برای چت کردن در گروه است. کاربر بعد از انتخاب این گزینه باید انتخاب کند که در کدام گروه می خواهد چت کند و بعد مشخص کند که می خواهد پیام بدهد یا پیام دریافت کند (receive message/send message).

زمانیکه یک کاربر گزینه دریافت پیام را انتخاب می کند تا رسیدن اولین پیام امکان ارسال پیام ندارد اما به محض اینکه اولین پیام را دریافت کند این کاربر هم امکان ارسال پیام خواهد داشت. مورد بعدی این است که چند کاربر همزمان امکان انتخاب گزینه send message را دارند.



```
Run: CA x Server x SystemHandler x
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 3
Enter group ID you want to join : gp
1. Send Message
2. Receive Message
Enter your choice : 2
```

کاربر a مشخص می کند که می خواهد در گروه gp در حالت گیرنده باشد

```
Run: SystemHandler x
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 3
Enter group ID you want to join : gp
1. Send Message
2. Receive Message
Enter your choice : 1
```

کاربر b مشخص می کند که در گروه gp می خواهد پیام ارسال کند

```
Run: CA x Server x SystemHandler x
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 3
Enter group ID you want to join : gp
1. Send Message
2. Receive Message
Enter your choice : 2
```

کاربر c مشخص می کند که در گروه gp می خواهد پیام دریافت کند

```
Run: SystemHandler x
Enter your choice : 1
hi every body
b (you) : hi every body
a : hello
c : hey
c : end

1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : |
```

کاربر b پیام خود را ارسال می کند و از الان هر دو کاربر a و c هم می توانند پیام ارسال کنند

```
Run: CA x Server x SystemHandler x
Enter your choice : 2
b : hi every body
a : hello
hey
c (you) : hey
end
c (you) : end

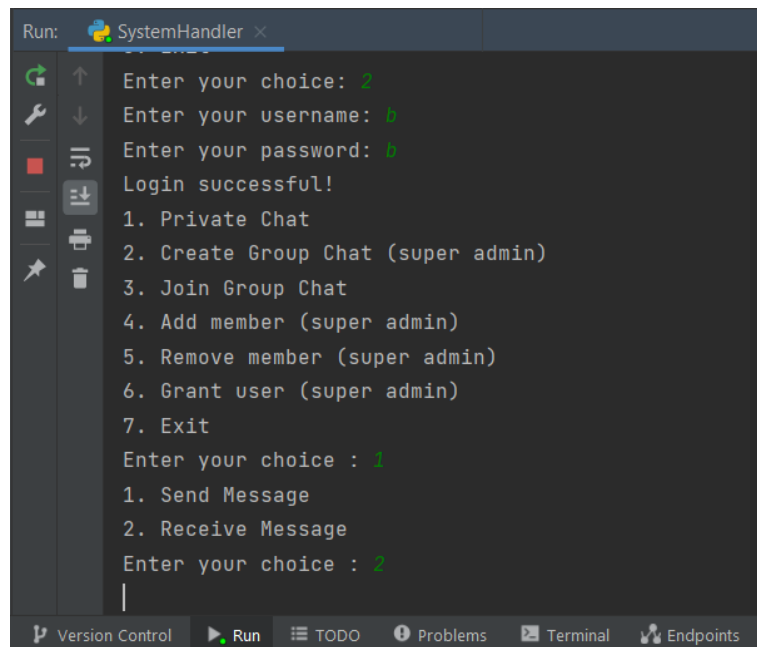
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : |
```

```
Run: CA x Server x SystemHandler x
Enter your choice : 2
b : hi every body
hello
a (you) : hello
c : hey
c : end

1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : |
```

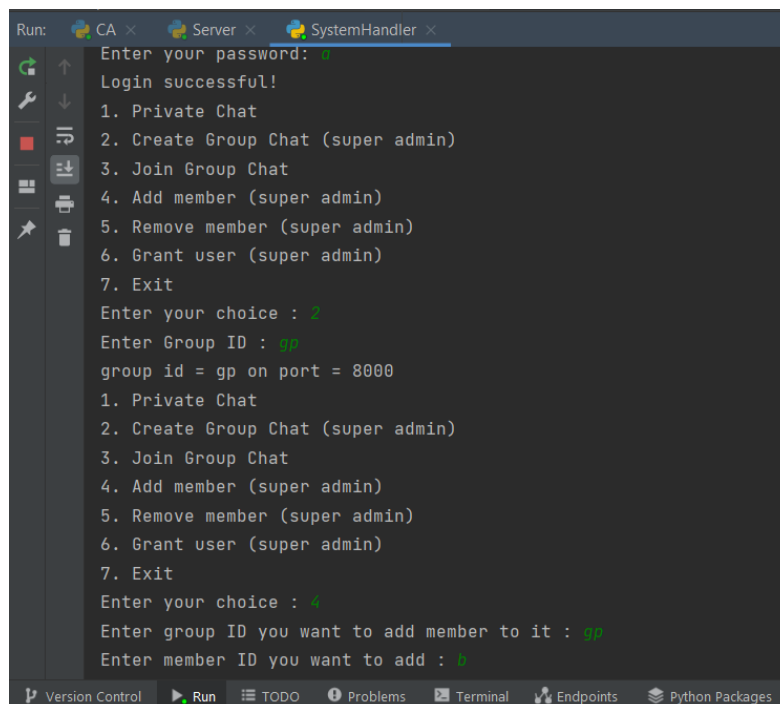
4) Add member

اضافه کردن اعضا به گروه توسط ادمین انجام می شود و برای این کار، کاربر مورد نظر باید در حالت receive message از اپشن private chat باشد.



```
Run: SystemHandler x
Enter your choice: 2
Enter your username: b
Enter your password: b
Login successful!
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 1
1. Send Message
2. Receive Message
Enter your choice : 2
|
```

لاگین کردن کاربر b و قرار گرفتن در حالت receive message از اپشن private chat

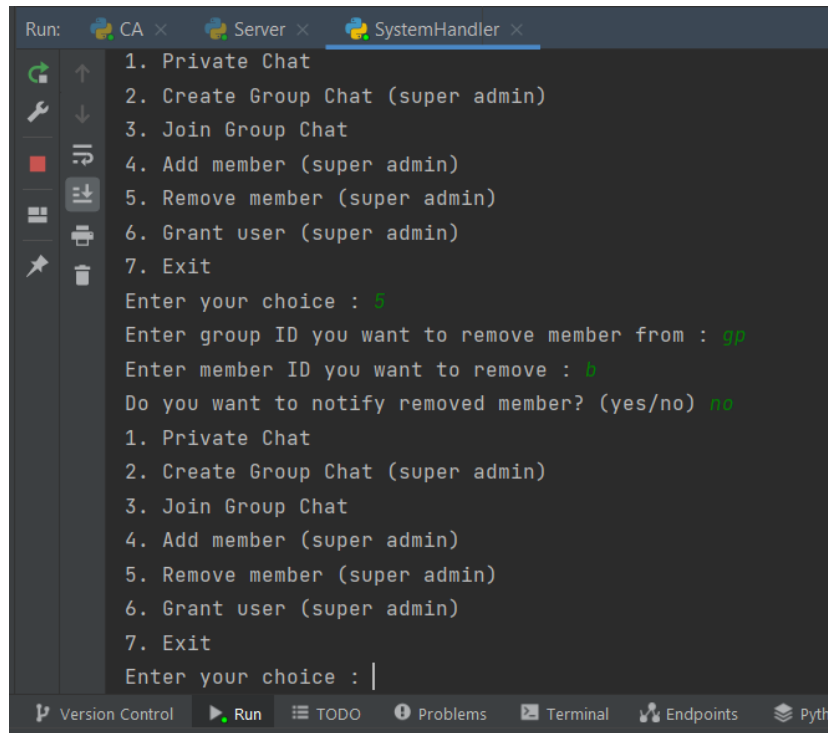


```
Run: CA x Server x SystemHandler x
Enter your password: gp
Login successful!
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 2
Enter Group ID : gp
group id = gp on port = 8000
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 4
Enter group ID you want to add member to it : gp
Enter member ID you want to add : b
```

اضافه کردن b به گروه gp توسط ادمین گروه با انتخاب گزینه add member

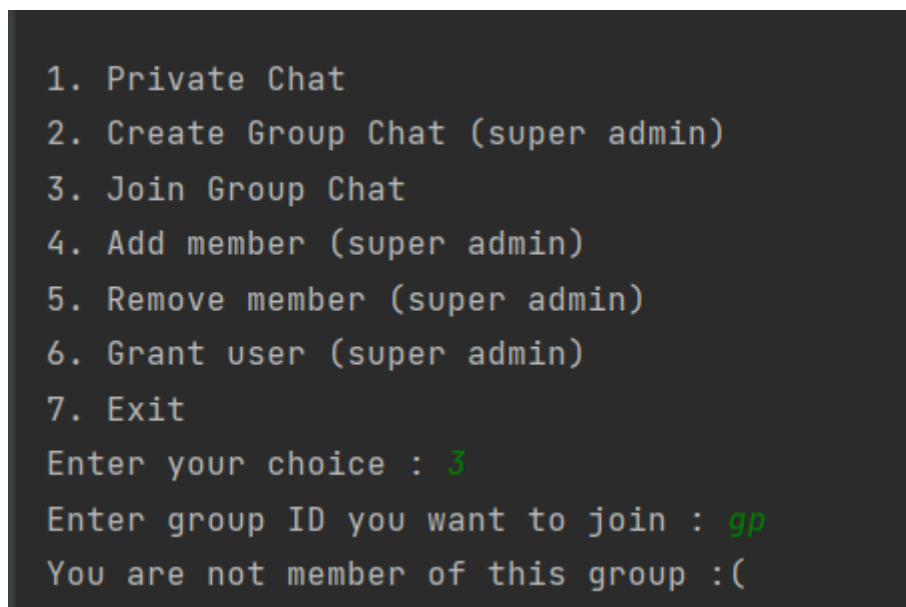
5) Remove member

باید اسم گروهی که می خواهیم عضوی را از آن حذف کنیم وارد کرده و بعد ایدی کاربری که می خواهیم از گروه ریمو کنیم را وارد کرده. در اینجا superadmin می تواند انتخاب کند که به کاربر ریمو شده اعلام شود که از گروه حذف شده یا نه.



```
Run: CA x Server x SystemHandler x
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 5
Enter group ID you want to remove member from : gp
Enter member ID you want to remove : b
Do you want to notify removed member? (yes/no) no
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : |
```

B توسط سوپرادمین از گروه حذف می شود

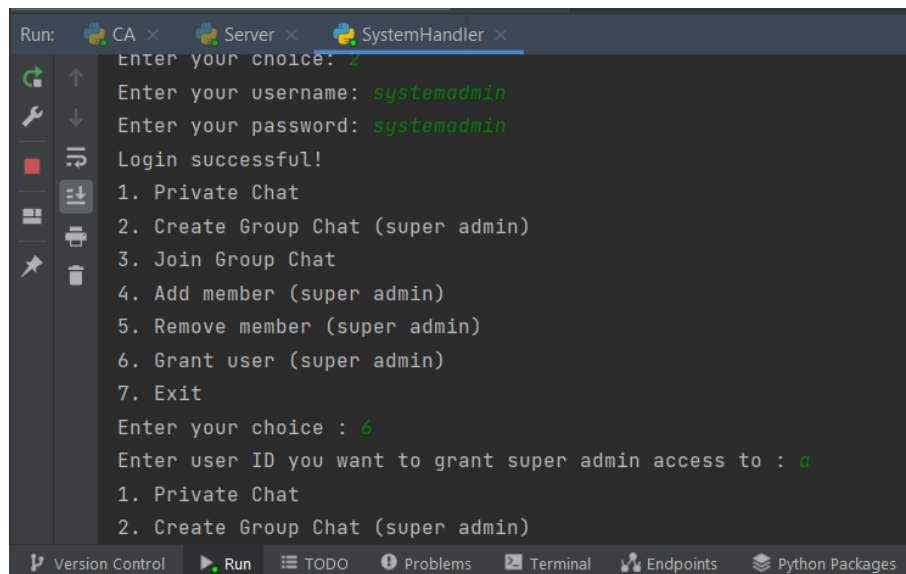


```
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 3
Enter group ID you want to join : gp
You are not member of this group :(
```

چون b دیگر عضوی از گروه gp نیست، نمی تواند در گروه پیام ارسال کند.

6) Grant user:

در این قسمت سیستم ادمین می تواند دسترسی سوپرادمین را به کاربر مدنظر اعطا کند.



```
Run: CA x Server x SystemHandler x
Enter your choice: 6
Enter your username: systemadmin
Enter your password: systemadmin
Login successful!
1. Private Chat
2. Create Group Chat (super admin)
3. Join Group Chat
4. Add member (super admin)
5. Remove member (super admin)
6. Grant user (super admin)
7. Exit
Enter your choice : 6
Enter user ID you want to grant super admin access to : 0
1. Private Chat
2. Create Group Chat (super admin)
```

7) Exit:

دستور خروج از برنامه.

روند برنامه:

زمانیکه گزینه register انتخاب می شود، هر کاربر private key خودش را می سازد و csr (دارای public key) را با استفاده از این private key آن را امضا می کند و برای CA ارسال می کند تا آن را امضا کند. این private key و csr مربوط به هر کاربر در یک فولدر با ایدی خود کاربر ذخیره می شود. بعد از اینکه CA، csr را امضا کرد، certificate حاصل را با ایدی خود کاربر در فولدر SecretFiles ذخیره می کند. در این فولدر علاوه بر certificate های کاربران، certificate خود CA، دیتابیس مربوط به اطلاعات کاربران (email + id + hashed password with salt + salt + role)، اطلاعات گروه ها (group id + admin + members) و private key مربوط به CA وجود دارد.

در چت خصوصی برای اینکه شخص a با شخص b ارتباط بگیرد باید شخص b در حالت listen (receive message) باشد و شخص a صراحتاً ایدی شخص b را وارد می کند و درخواست چت خصوصی با b را برای CA ارسال می کند. CA در پاسخ، certificate شخص b را برای a ارسال می کند. هنگامیکه اولین پیام از طرف a برای b ارسال می شود، شخص b برای اینکه بتواند پیام ها را رمز کند، certificate شخص a را از CA درخواست می کند.

در ابتدا شخصی که دارای سطح دسترسی سوپر ادمین است درخواست ایجاد گروه از CA با ایدی داده شده را می کند و اگر ایدی گروه تکراری نباشد، CA اطلاعات اولیه گروه شامل ایدی، پورت و certificate ادمین را برای این شخص ارسال می کند و ادمین برای اضافه کردن کاربران به این گروه باید پیامی شامل اطلاعات اولیه گروه را برای کاربر مدنظر ارسال کند (در این حالت کاربر مدنظر روی حالت listen (receive message in private chat) قرار دارد.

برای چت گروهی کاربران یکی از گروه هایی که در آن عضو هستند را انتخاب و در قالب فرستنده یا گیرنده در آن مشارکت می کنند.

برای حذف یک کاربر از یک گروه، ادمین ایدی گروه و ایدی شخص را وارد کرده و به دو صورت می تواند کاربر را حذف کند. اگر نیاز باشد که به کاربر اعلام کند باید کاربر روی حالت listen (receive message in private chat) قرار داشته باشد.

برای اعطای دسترسی، ابتدا نقش کاربری که می خواهد دسترسی را اعطا کند بررسی می شود اگر سوپر ادمین بود، نقش ایدی کاربری که وارد کرده به سوپر ادمین تغییر می یابد.

پیام هایی که از طرف کاربران برای CA فرستاده می شود دارای سه بخش flag request (نمایانگر نوع درخواست)، sender id و message است.

Flag request	Request
0	Sign csr
1	Private chat
2	Group chat

زمانیکه flag=0 است، محتوای message، csr کاربر است.

زمانیکه flag=1 است، محتوای message، ایدی کاربری است که کاربر درخواست certificate آن را دارد.

زمانیکه flag=2 است، محتوای message، ایدی گروه است.

Flag پیام هایی که از طرف CA برای client ارسال می شوند به صورت زیر می باشد:

flag	meaning
0	Waiting for csr
1	Success
2	Not super admin
3	Sender id not found
4	Recipient id not found
5	Repetitive group id

زمانیکه flag=1 است، درخواست کاربر با موفقیت پردازش شده و certificate و اطلاعات مربوطه ارسال می شود.

زمانیکه flag>1 است، نشان دهنده حالات خطاست.

پیام های رد و بدل شده بین کاربران که از سرور عبور می کنند به فرمت زیر است:

flag	Group member	Sender ID	Recipient ID	message	signature
------	--------------	-----------	--------------	---------	-----------

که در چت خصوصی، بخش message و signature رمز می شوند و در چت گروهی رمز نمی شوند.

flag	Used for	Group member
0	Private chat	–
1	Group chat message	–
2	Add user(admin)	Added user
3	Delete user(admin)	Removed user
4	Create group	admin
5	Delete user without notify	Removed user
6	voting	–
7	Send poll	–
8	Confidential voting	–