به نام خدا

دانشگاه اصفهان

University of Isfahan

پروژه پایانترم درس مبانی امنیت سایبری تاریخ: 1402/11/8

توسط: ابراهیم کیانی فلاورجانی

شماره دانشجویی : 993623036

شرح پروژه:

این یک مینی پروژه شبیه ساز لاگین کاربر **(احراز اصالت قوی)** با استفاده از پروتکل لمپورت است است که با برنامه نویسی سوکت و پایتون نوشته شده است.

پروژه شامل سه فایل است. یک فایل شامل یک دیتا بیس خالی، و دو فایل دیگر به زبان پایتون است.

برای این پروژه دو فایل رابط گرافیکی و فایل نصبی (exe) مربوط به آنها اضافه شده است.

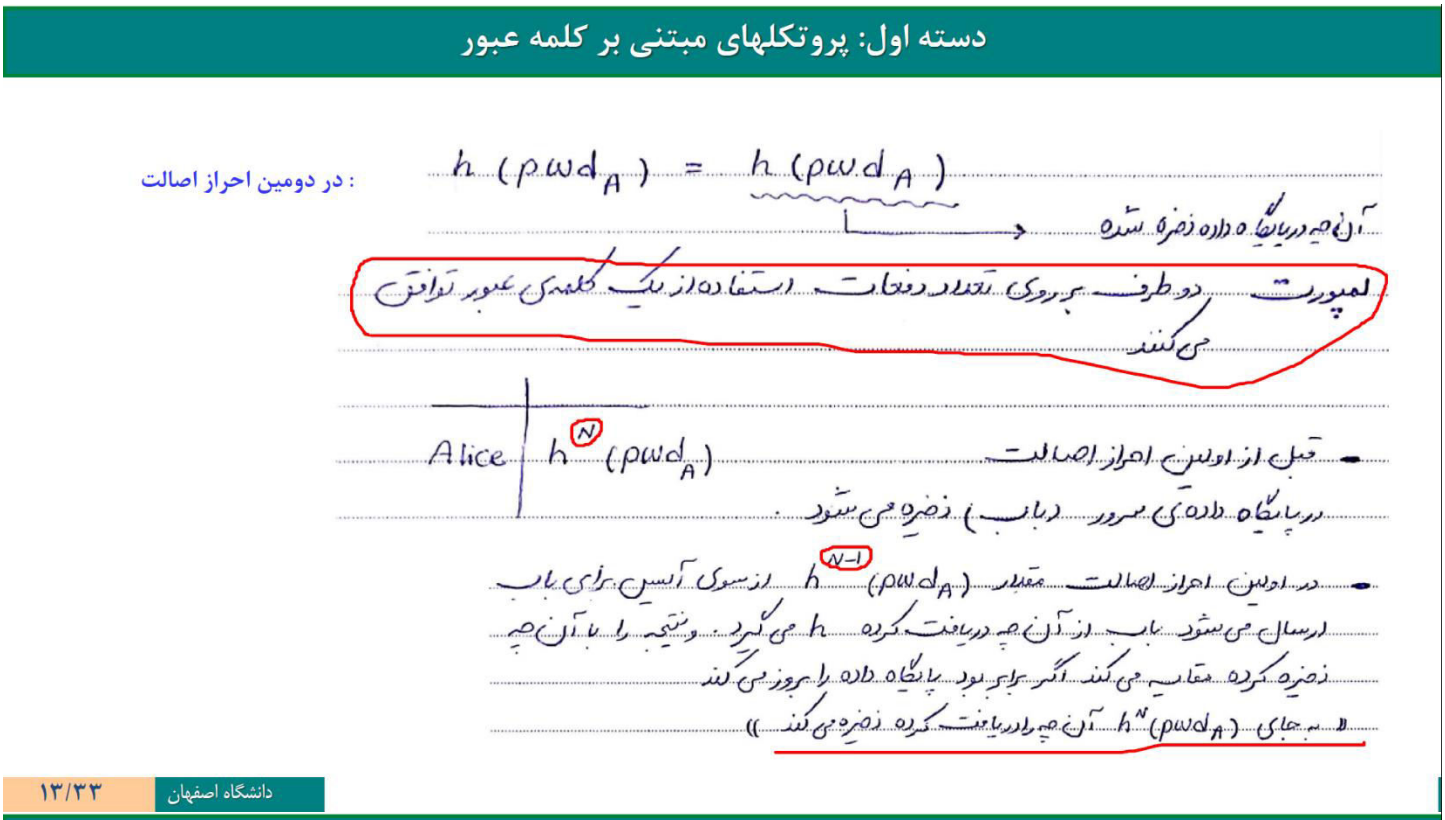
یک فایل پایتون به عنوان سرور و فایل دیگر به عنوان بخش کلاینت در نظر گرفته شده اند.

هر دو فایل از برنامه نویسی سوکت پایتون بهره مندی شده اند. و زمانی که این فایل ها اجرا شوند ، آنها از طریق آپی و پورت مشخص شده در هر فایل به یکدیگر متصل شده اند.

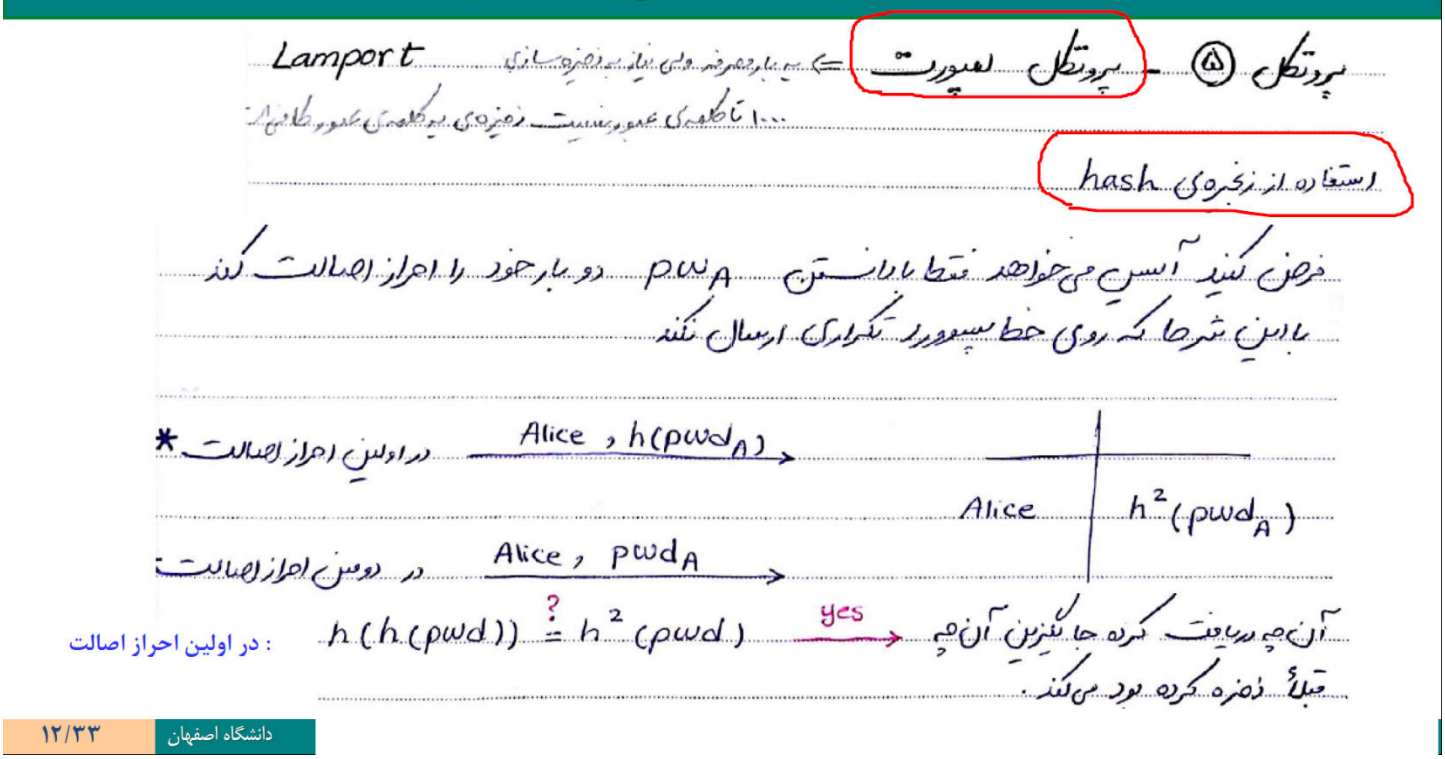
فایل سرور از دیتابیس مشخص شده برای ذخیره نام کاربری و رمز کاربر کاربر استفاده میکند.

شرح لمپورت:

دسته اول: پروتکلهای مبتنی بر کلمه عبور



دسته اول: پروتکلهای مبتنی بر کلمه عبور



دسته اول: پروتکلهای مبتنی بر کلمه عبور

لمپورت ... دو طرف بر روی تعداد دفعات استفاده از یک کلمه‌ی عبور توافق می‌کنند

Alice	$h^{N}(pwd_A)$

- قبل از اولین احراز اصالت در پایگاه داده‌ی سرور (باب) ذخیره می‌شود.

- در اولین احراز اصالت مقدار $h^{N-1}(pwd_A)$ از سوی آلیس برای باب ارسال می‌شود. باب از آن چه دریافت کرده h می‌گیرد و نتیجه را با آن چه ذخیره کرده مقایسه می‌کند. اگر برابر بود پایگاه داده را بروز می‌کند «به جای $h^{N}(pwd_A)$ آن چه را دریافت کرده ذخیره می‌کند»

دسته اول: پروتکلهای مبتنی بر کلمه عبور

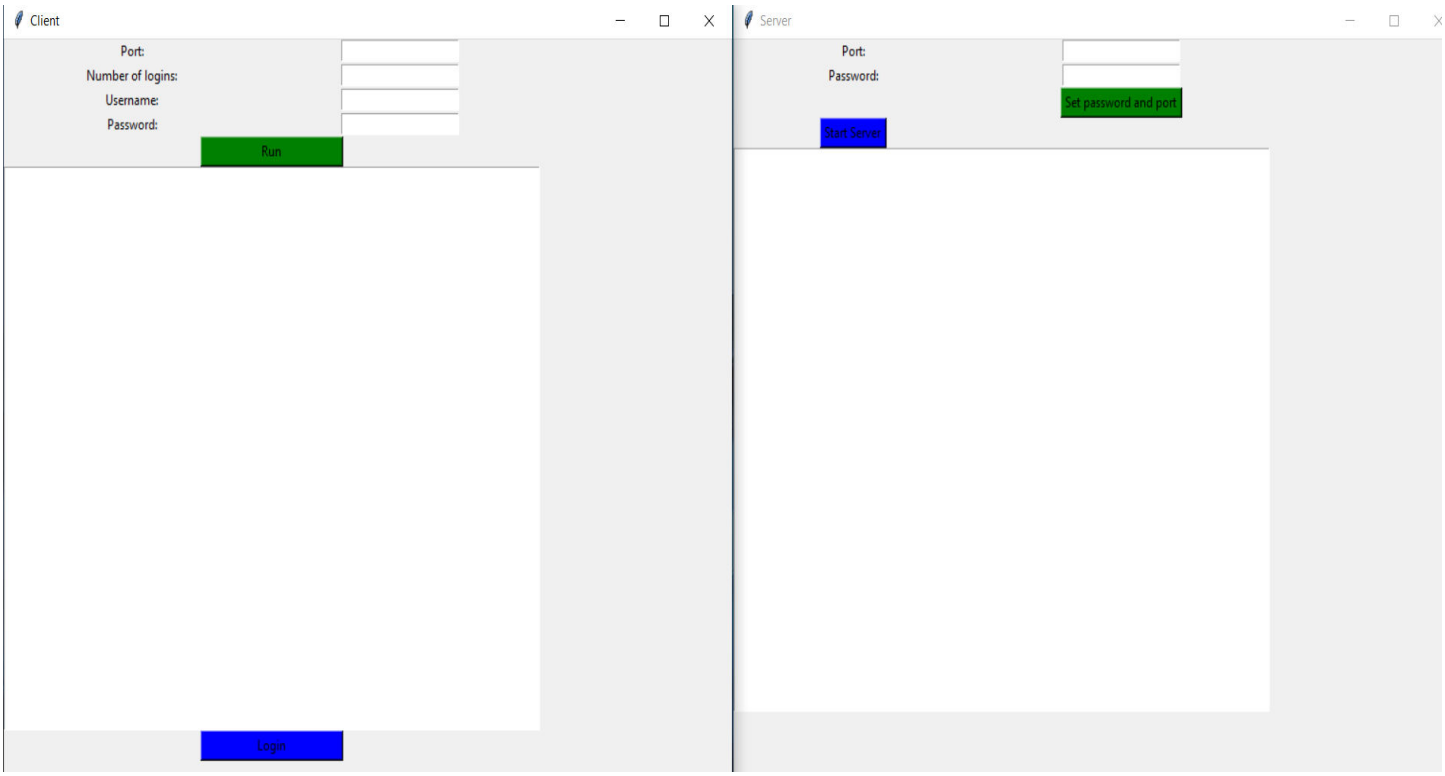
Alice, $h^{N-i}(pwd_A)$ →

- در iامین احراز اصالت

Alice	$h^{N-i+1}(pwd_A)$

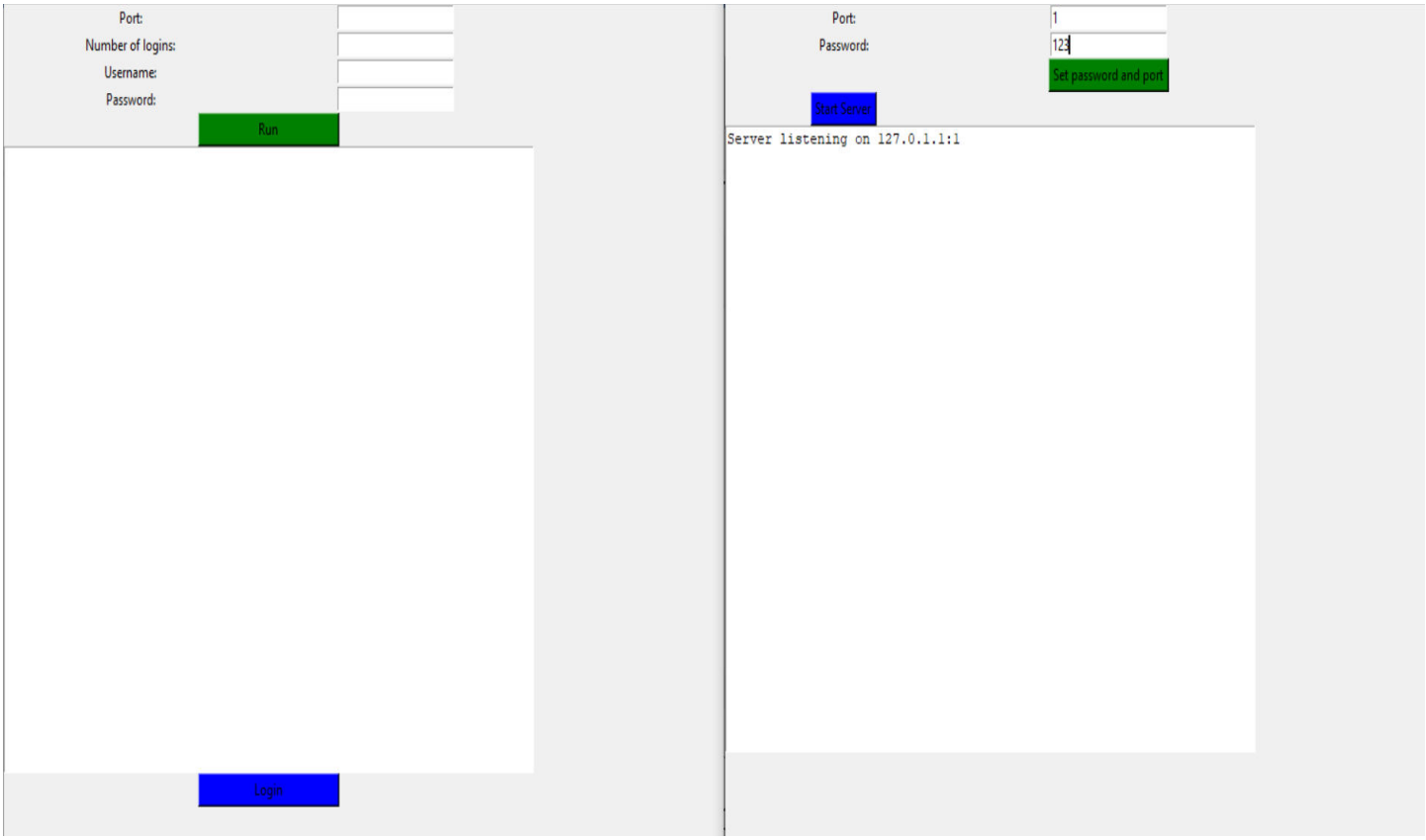
اجرای پروژه:

برای اجرای پروژه باید دو فایل client_GUI.exe و server_GUI.exe موجود در پوشه setup_files را در دایرکتوری دلخواه باز کنید.



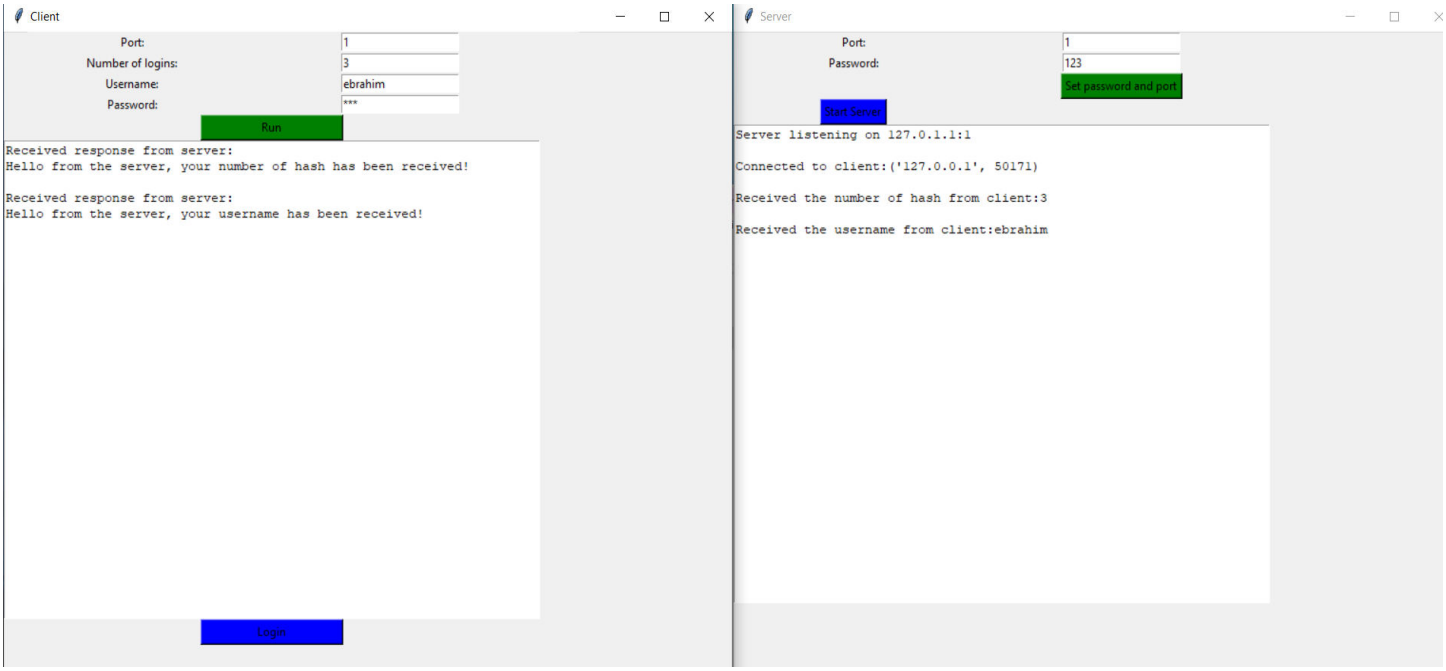
دو فایل باز شده شبیه ساز های کلاینت و سرور هستند.

حال اول باید در سرور یک پورت را به صورت عدد قرار داده و سپس یک رمز قرار دادی قرار دهیم و کلید Set password and port را فشار داده و سرور را با فشار دادن کلید Start Server اجرا کنیم.



اکنون سرور پیغام میدهد که بر هاست 127.0.1.1 و پورت 1 در حال اجرا است.

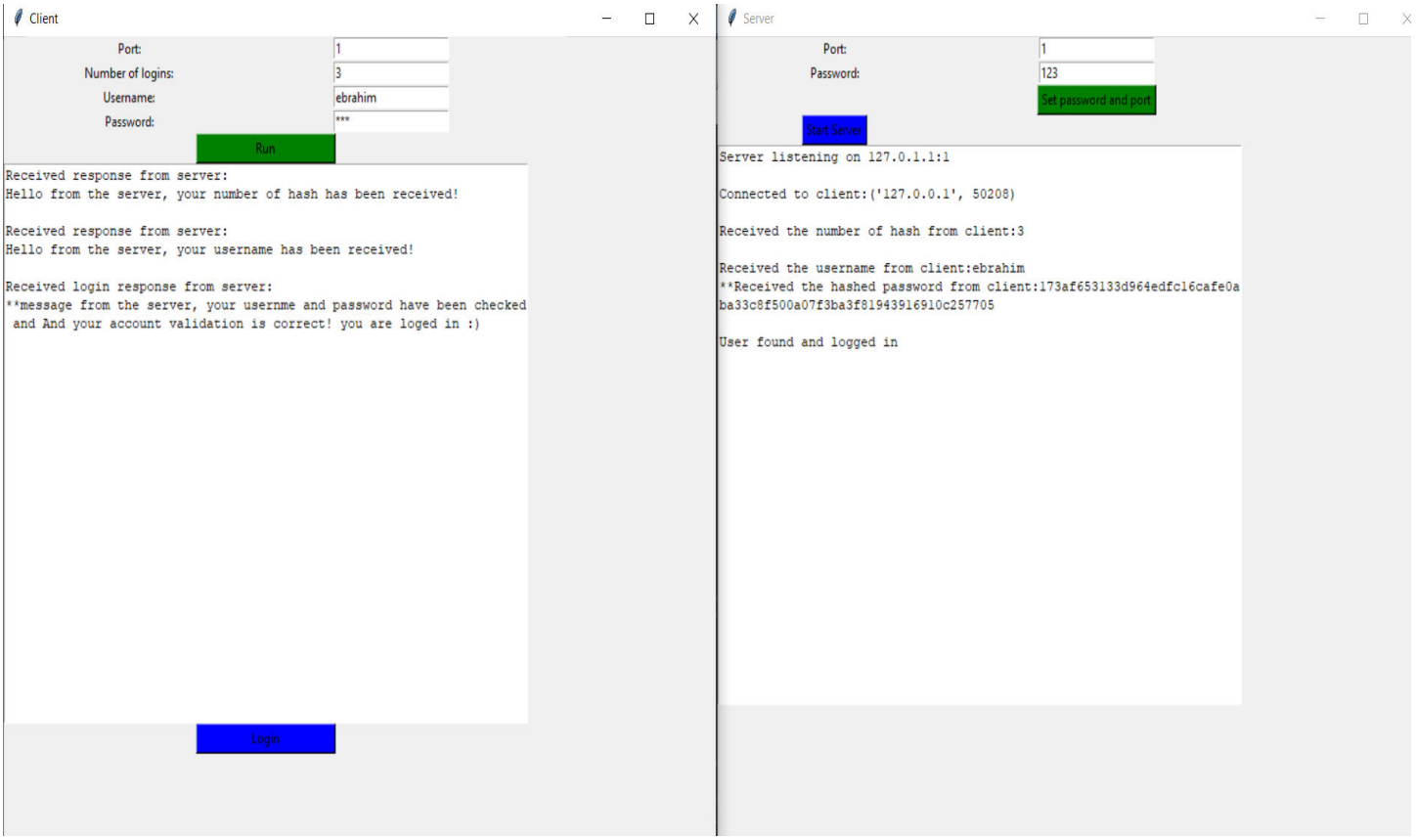
در مرحله بعدی به سراغ بخش کلاینت میرویم و شماره پورت سرور و تعداد لاگین که قرار است انجام بدهیم و نام کاربری دلخواه و رمز قرار داده شده را انتخاب کرده و اجرای کلاینت را با فشار دادن کلید Run انجام میدهیم.



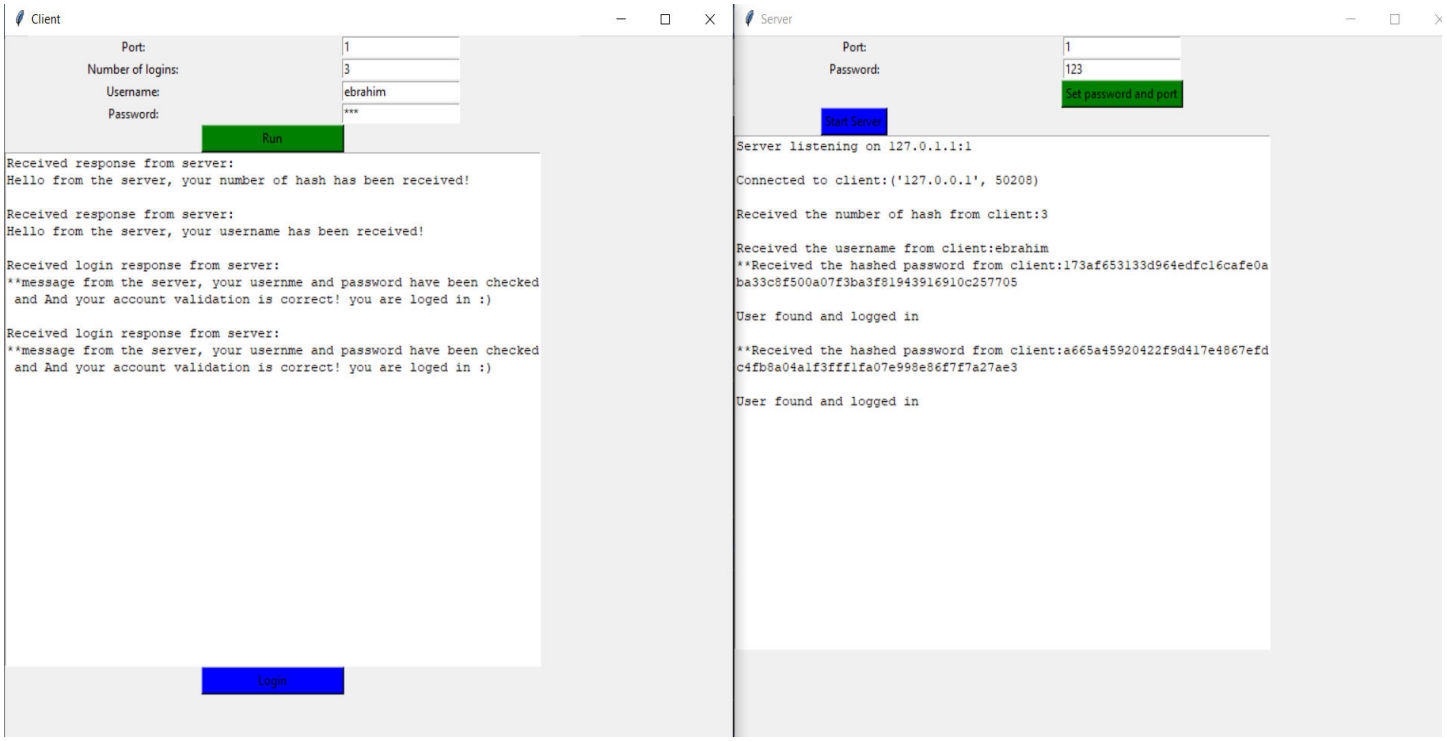
همانطور که در تصویر مشاهده کردیم کلاینت به سرور متصل شده و اطلاعات کلاینت به سرور ارسال شده و سرور علاوه بر نشان دادن اطلاعات یک فیدبک به کلاینت هم میدهد.

اکنون میتوان لاگین کرد، فراموش نکنید که با توجه به اینکه تعداد لاگین قرار دادی را سه بار قرار داده ایم پس رمز ما دو بار هش شده و هر بار یک هش کمتر از تعداد هش های سرور برای سرور ارسال میشود و سرور با هش کردن رمز دریافتی احراز اصالت را انجام میدهد.

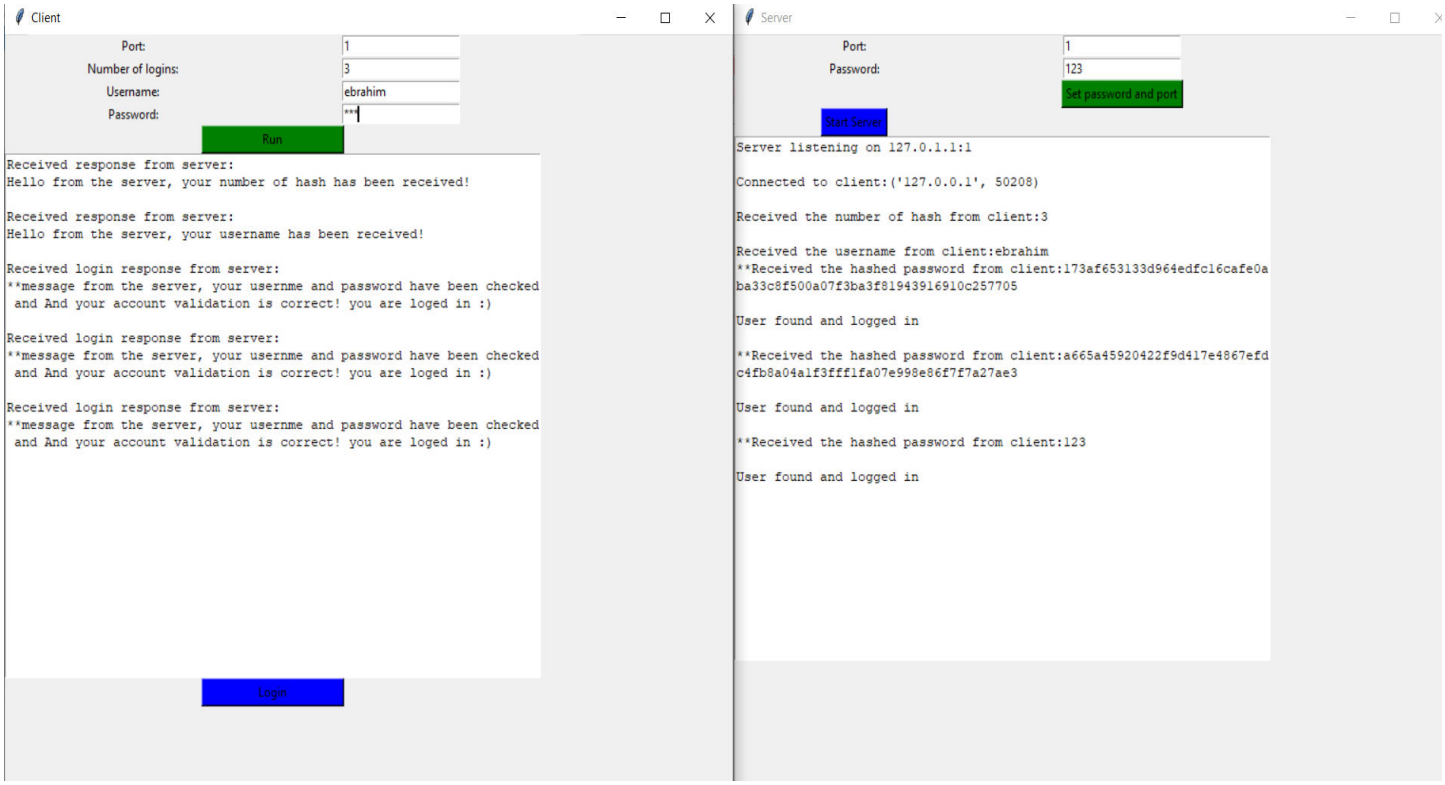
مراحل سه بار لاگین کردن کلاینت را با سه بار فشردن کلید لاگین در بخش کلاینت مشاهده میکنیم. لاگین اول:



لاگین دوم:



لاگین سوم (آخر):



همانطور که در لاگین آخر مشاهده میکنیم سرور در پایان رمز اصلی کاربر را دریافت میکند.البته این امر درست نیس و باید اخرین هش رمز در دیتابیس ذخیره شود ولی در اینجا برای صحت انجام کار رمز اصلی در دیتابیس باقی خواهد ماند.

	id	username	password
	Filter	Filter	Filter
1	71	ebrahim	123

در پایان هر چقدر بر روی کلید لاگین کلیک کنید مشاهده میکنید که دیگر نمیتوانید لاگین کنید زیرا همه شانس های لاگین خود را از دست داده اید. و کلاینت پیغام:

You used all your chances to login

را نمایش میدهد.