به نام خدا



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

توسط: ابراهیم کیانی فلاورجانی

شماره دانشجویی : 993623036

**شرح پروژه:**

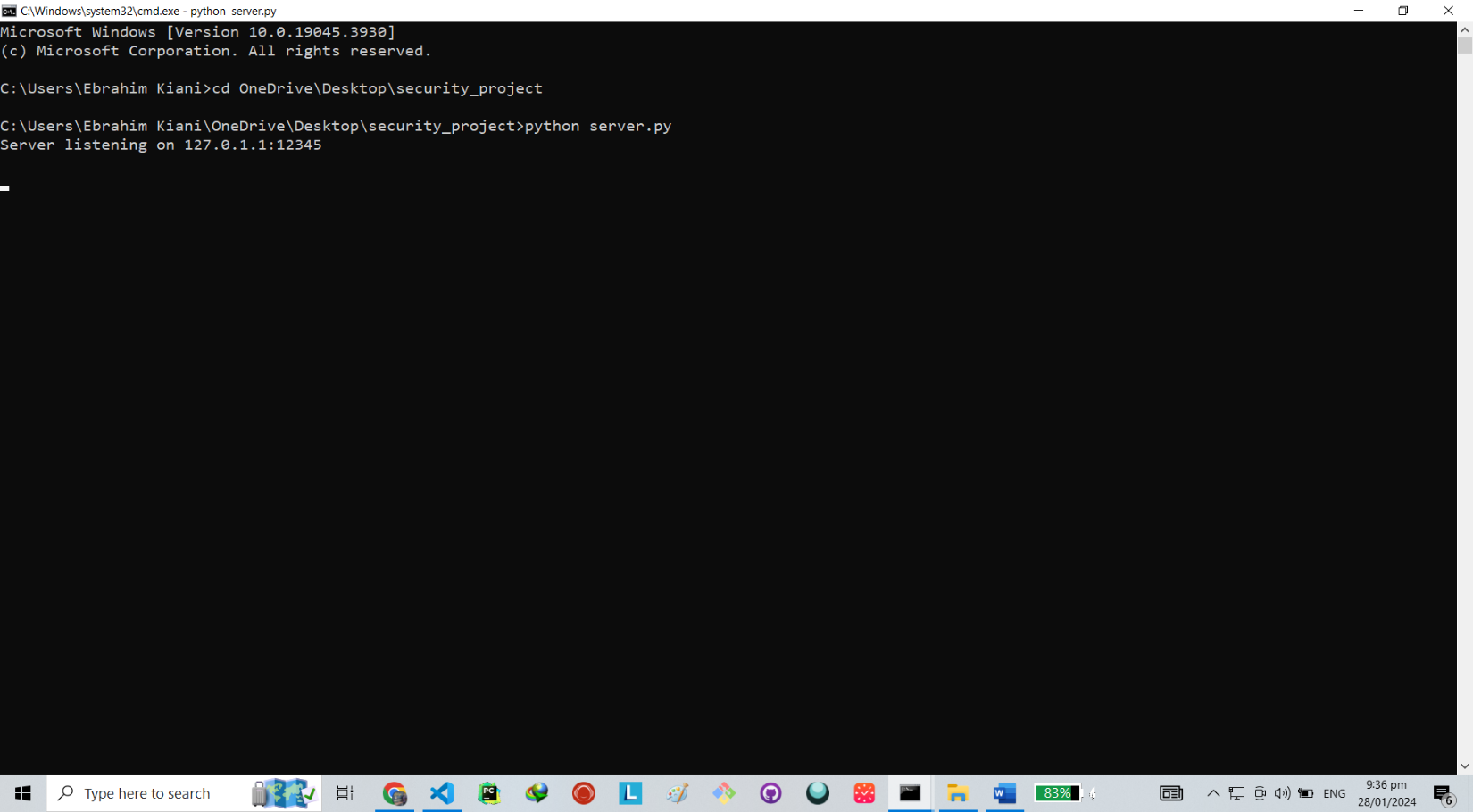
پروژه شامل سه فایل است. یک فایل شامل یک دیتا بیس خالی، و دو فایل دیگر به زبان پایتون است.

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

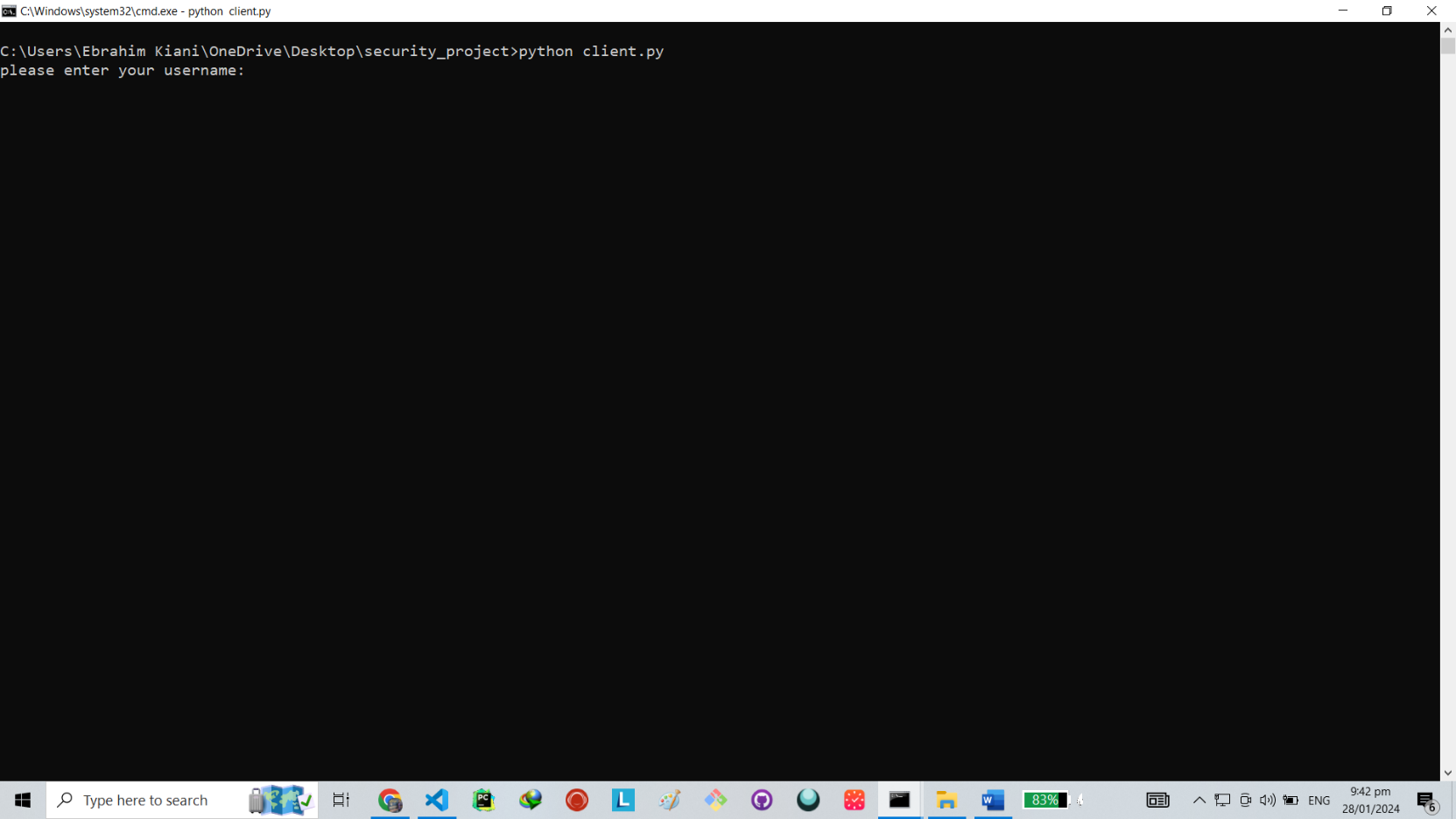
هر دو فایل از برنامه نویسی سوکت پایتون بهره مندی شده اند. و زمانی که این فایل ها اجرا شوند ، آنها از طرییق آپی و پورت مشخص شده در هر فایل به یکدیگر متصل شده اند.

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

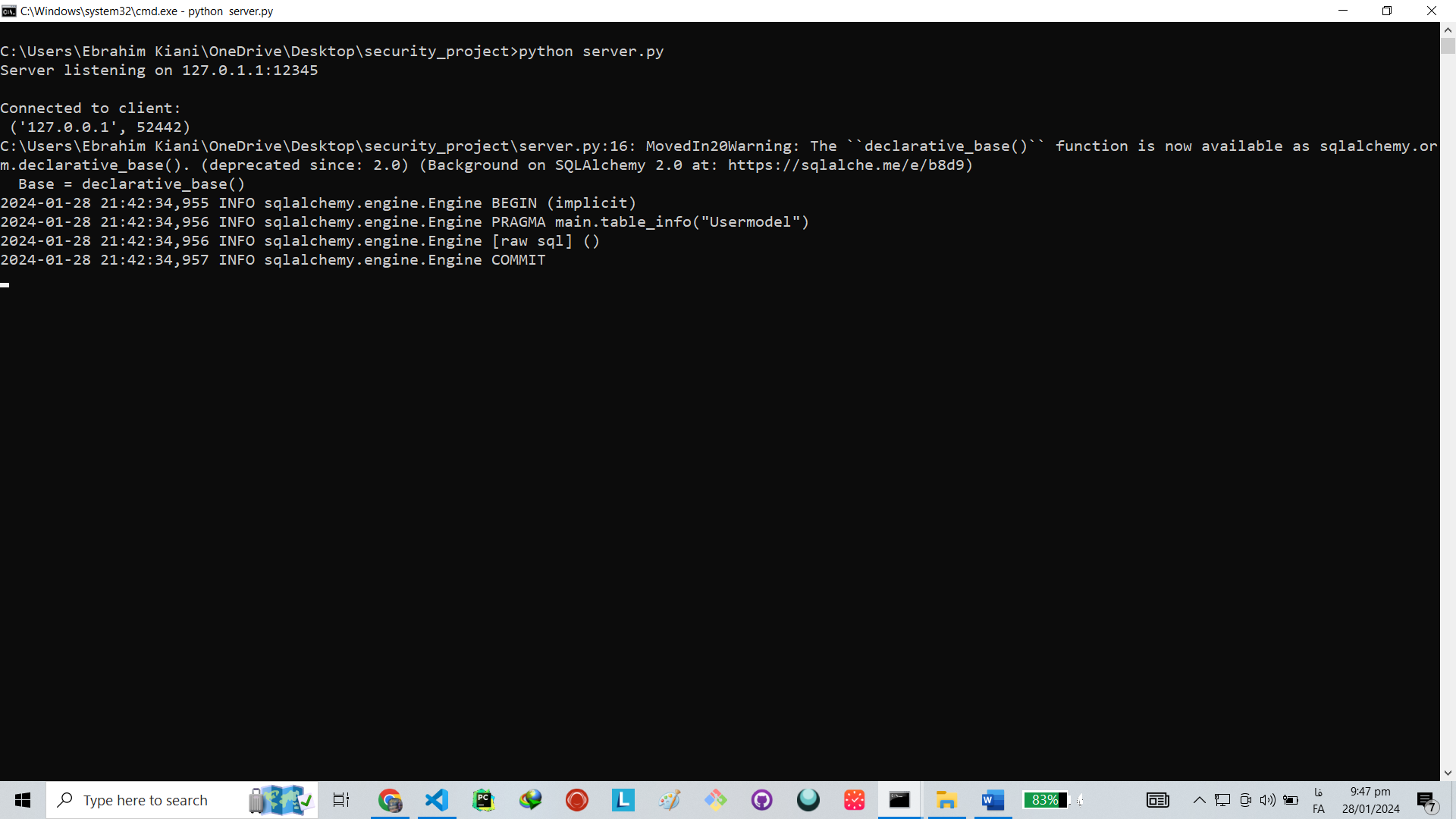
من در هر دو فایل رمز کاربر را عدد 1234 به صورت قرار دادی گذاشته ام که مثلا قبلا توسط کاربر و سرور در یک کانال امن رد و بدل شده است.

برای اجرای پروژه ابتدا فایل سرور در یک ترمینال باید اجرا شود به صورت زیر:

اکنون فایل کلاینت را در ترمینال دیگر باز میکنیم:



اما در سوی دیگر در سرور مشاهده میکنیم که سرور با موفقیت به کلاینت متصل شده و پیغام اتصال را میدهد و اعلان میکند که در حال شنیدن از کلاینت مد نظر است.



اکنون میخواهیم نام alice را برای کاربر انتخاب کنیم و تعداد 5 عدد لاگین را به فایل کلاینت بدهیم. در شکل زیر مشاهده میکنید.

A computer screen with a black screen

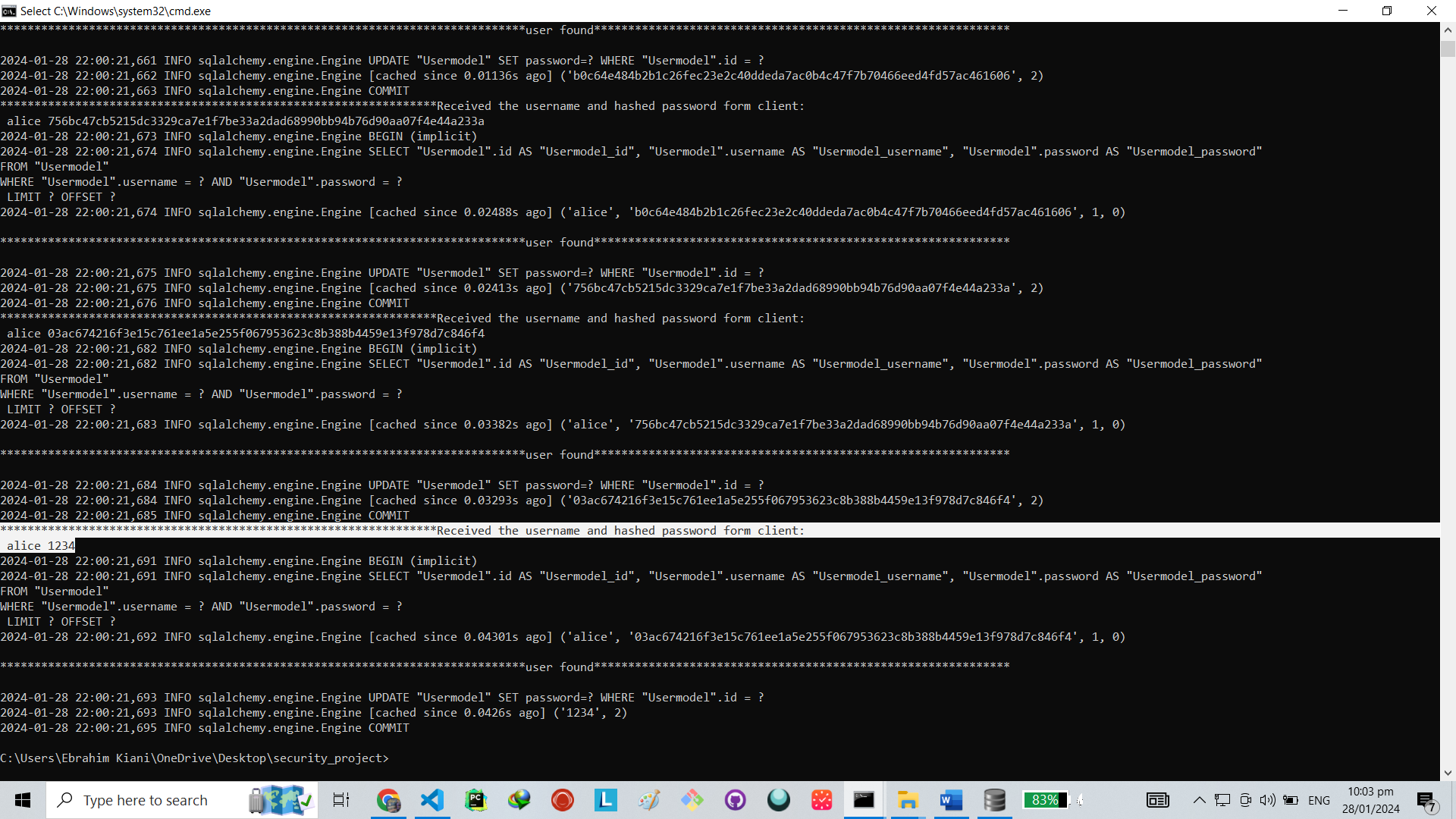
Description automatically generatedپس از زدن دکمه اینتر در بخش کلاینت، سرور 5 بار رمز کاربر را هش کرده و سپس در سرور ذخیره میکند.

سپس کاربر 5 بار لاگین میکند و هر بار یک بار کمتر رمز خود را هش میکند و برای سرور میفرستد. سرور نیز در هر بار رمز کاربر را یک بار هش کرده و سپس بررسی میکند که آیا کاربر معتبر است یا خیر. اگر معتبر بود رمز کاربر را در دیتا بیس همان چیزی قرار میدهد که کاربر برایش فرستاده بود و سپس منتظر لاگین بعدی کاربر میشود.

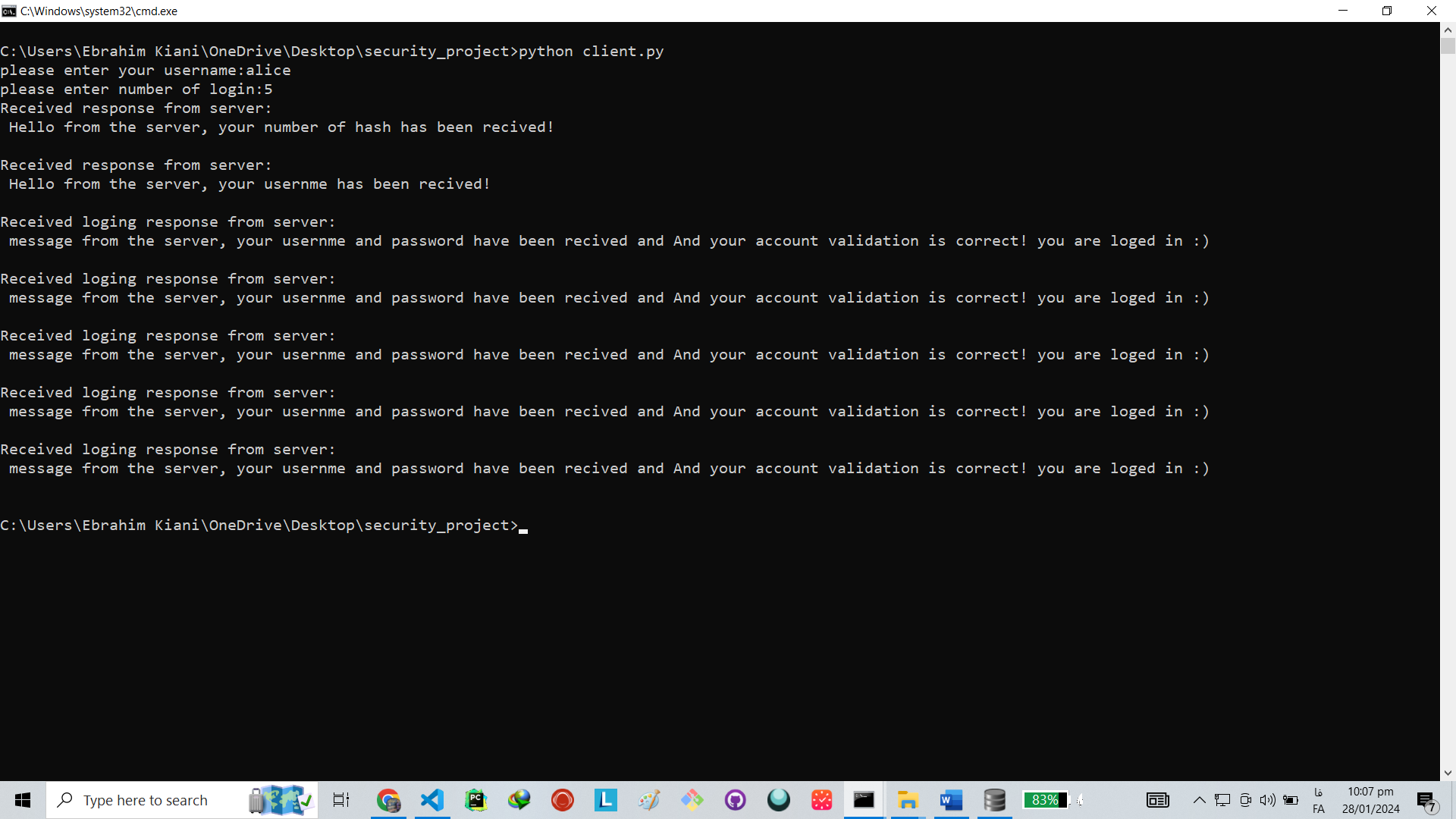
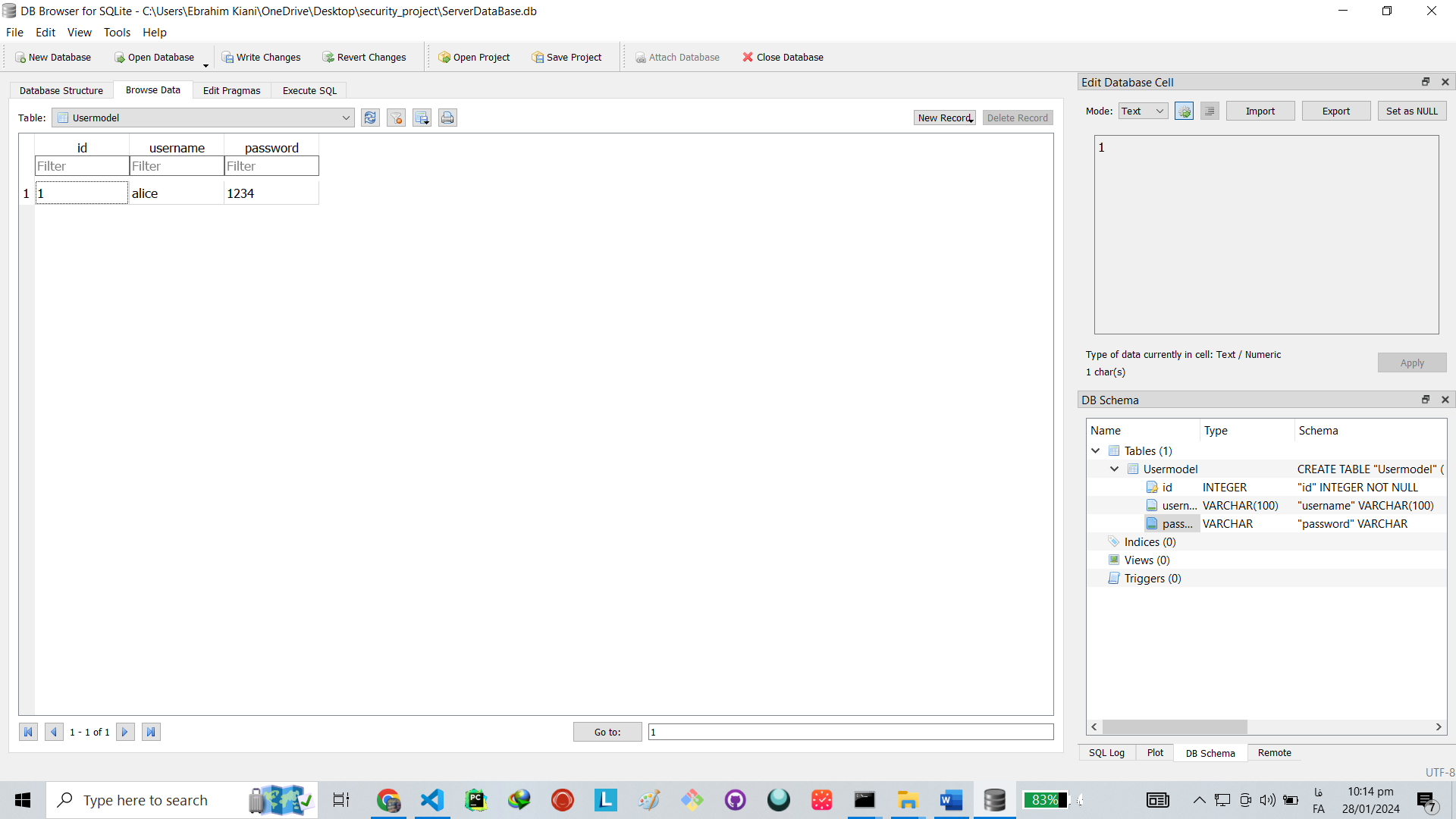
این کار همان 5 بار که داده بودیم تکرار میشود تا به خود رمز 1234 کاربر برسیم.

بدین ترتیب ذنجیره هش اجرا شده و در هر بار رمز های متفاوتی از طریق سوکت برای سرور ارسال میشود.

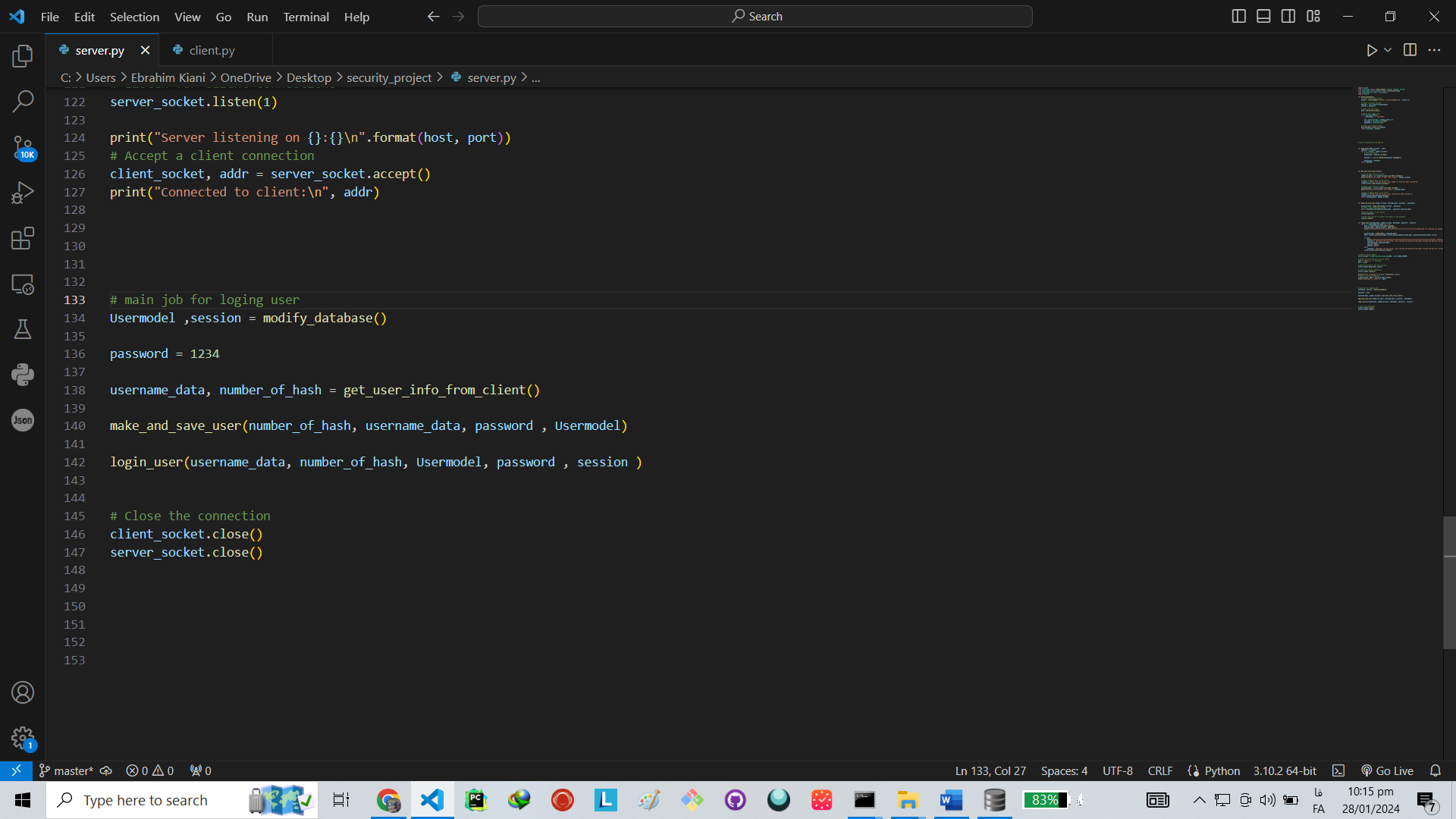
همانطور که در بخش سرور مشاهده میکنیم.

کاربر 5 بار اطلاعاتش توسط کلاینت دریافت شده و لاگین شده تا اینکه بالاخره به رمز اصلی کاربر برسد و ان را ذخیره سازی کند.(در عمل نباید رمز اصلی در دیتا بیس نمایش داده شود و باید هش آخر قرار داده شود ولی در اینجا برای نشان دادن صحت عمل پروژه، در آخر به رمز اصلی رسیده ام)

و اما در فایل کلاینت اکنون مشاهده میکنیم که:

کاربر 5 بار لاگین موفقیت آمیز داشته که هر بار رمزش یکی کمتر هش شده و برای سرور ارسال شده است و سرور در پاسخ به کلاینت فهمانده است که او لاگین شده است! در فایل دیتا بیس به صورت زیر مشاهده میکنیم که اخرین لاگین کاربر در دیتابیس ثبت شده است.

منطق میانی کد سرور:



A screenshot of a computer

Description automatically generatedو همینطور منطق پیاده شده در کد کلاینت:

در هر دو فایل کامنت ها و تابع های مدنظر را به صورت خوانا قرار داده ام و کافیست به صورت یک نگاه سطحی بررسی کنید تا منطق آن را به طور واضح درک کنید.