

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 استفاده میکند.

شرح لمپورت:

دسته اول: پروتکل‌های مبتنی بر کلمه عبور

در دومین احراز اصالت:

$$h(pwd_A) = h(pwd_A)$$

آنچه در پایگاه داده ذخیره شده

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

Alice	$h^N(pwd_A)$
-------	--------------

قبل از اولین احراز اصالت

در پایگاه داده‌ی سرور (باب) ذخیره می‌شود

در اولین احراز اصالت مقایسه $h^{N-1}(pwd_A)$ 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 دریافت کرده ذخیره می‌کند »

دسته اول: پروتکل‌های مبتنی بر کلمه عبور

Lamport

پروتکل ⑤ - پروتکل لمپورت

۱۰۰۰ تا کلمه عبور منحصبت ذخیره می‌کند و کلمه عبور را به سرور می‌فرستد

استفاده از زنجیره‌ی hash

فرض کنید آلیس می‌خواهد فقط با بابش pwd_A دوبار خود را احراز اصالت کند بابش شریک که روی خط بی‌سیم رمزنگاری ارسال کند

در اولین احراز اصالت * $Alice, h(pwd_A)$

Alice	$h^2(pwd_A)$
-------	--------------

در دومین احراز اصالت $Alice, pwd_A$

در اولین احراز اصالت: $h(h(pwd_A)) \stackrel{?}{=} h^2(pwd_A)$ yes → آن چه دریافت کرده جاگزین آن چه قبلاً ذخیره کرده بود می‌کند

دسته اول: پروتکل‌های مبتنی بر کلمه عبور

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

Alice | $h^{(N)}(pwd_A)$

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

در اولین اعزاز اصالت مقید $h^{(N-1)}(pwd_A)$ از سوی آیسین 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 دریافت کرده ذخیره می‌کند »

دسته اول: پروتکل‌های مبتنی بر کلمه عبور

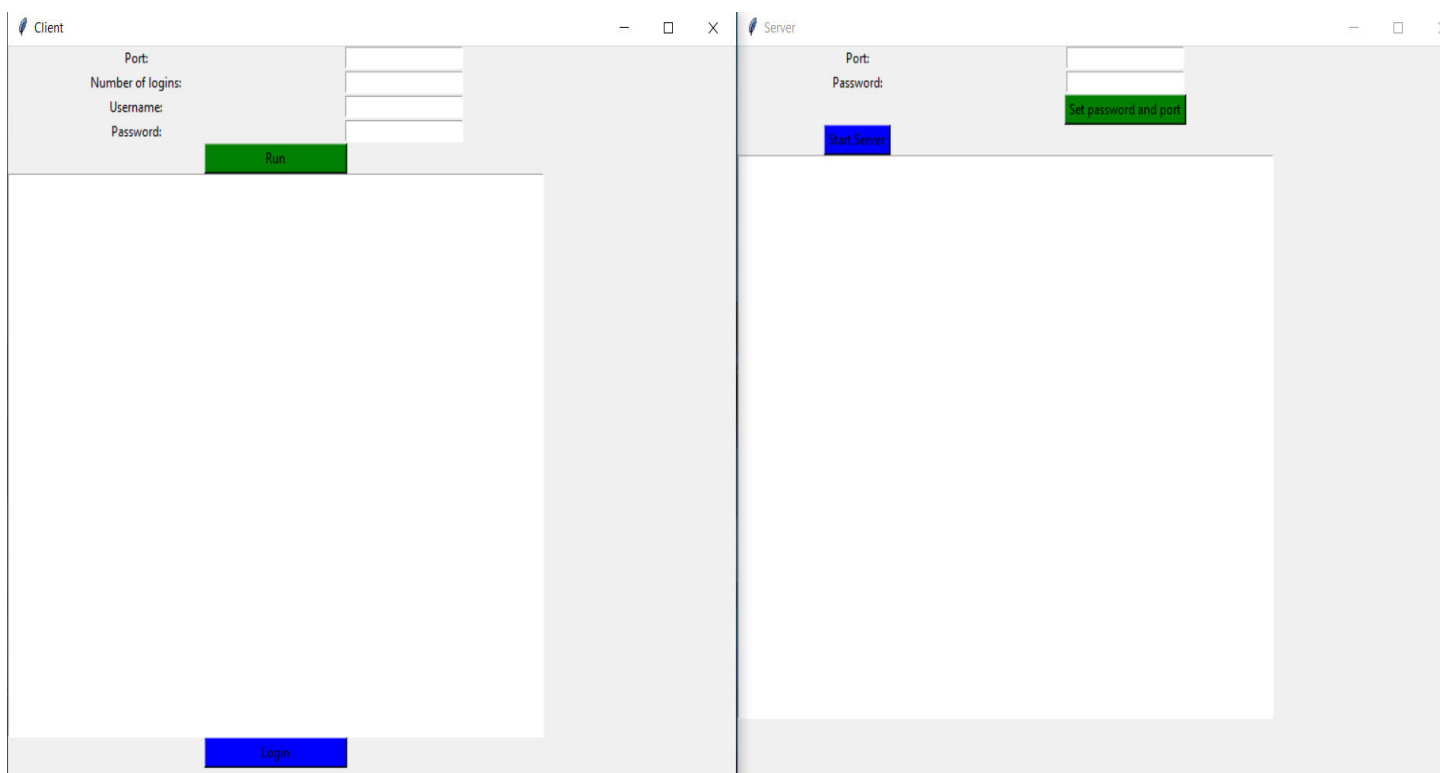
Alice, $h^{(N-i)}$ (pwd_A) →

در آیسین اعزاز 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.



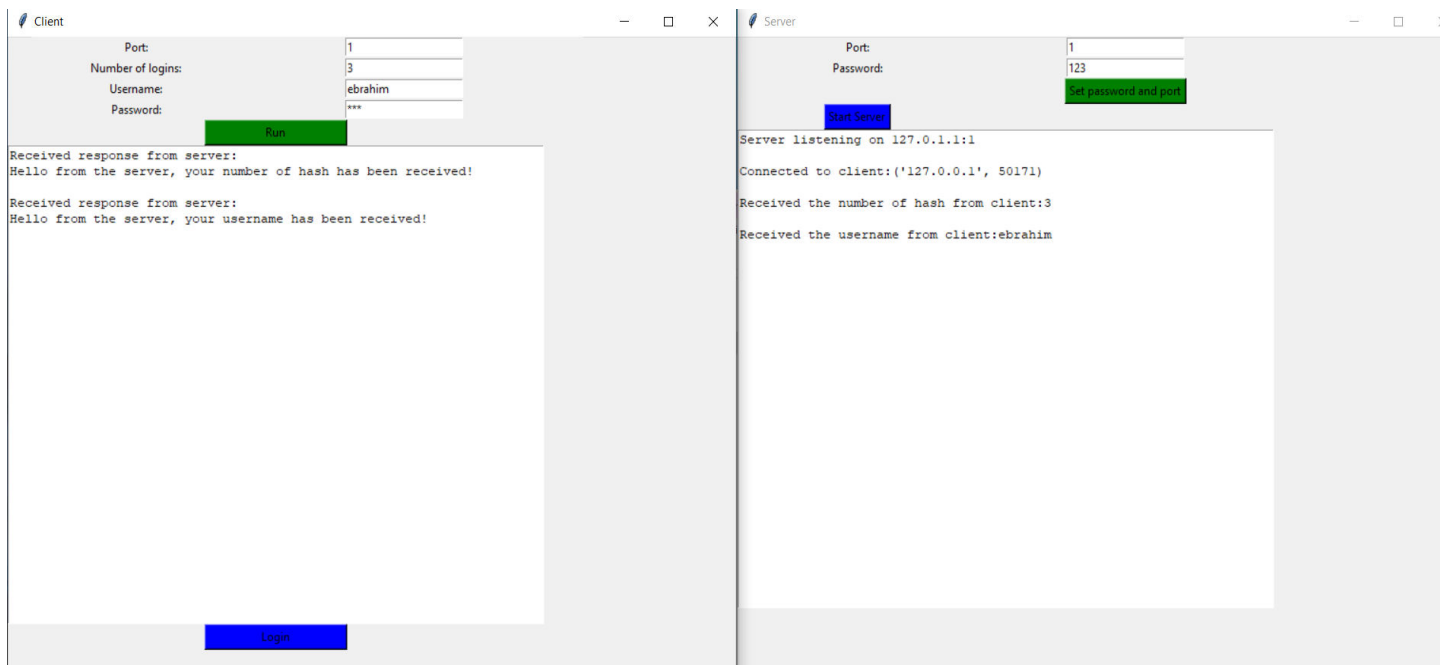
دو فایل باز شده شبیه ساز های کلاینت و سرور هستند.

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.

Port: Number of logins: Username: Password:	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	Port: Password:	<input type="text" value="1"/> <input type="text" value="123"/>
<input type="button" value="Run"/>		<input type="button" value="Set password and port"/>	
<input type="button" value="Login"/>		<input type="button" value="Start Server"/>	
		Server listening on 127.0.1.1:1	

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 هاش شده و هر بار یک هاش کمتر از تعداد هاش های سرور برای سرور ارسال میشود و سرور با هاش 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:

Client

Port:1

Number of logins:3

Username:ebrahim

Password:***

Run

Received response from server:
Hello from the server, your number of hash has been received!

Received response from server:
Hello from the server, your username has been received!

Received login response from server:
**message from the server, your usernme and password have been checked
and And your account validation is correct! you are logged in :)

Login

Server

Port:1

Password:123

Start Server

Server listening on 127.0.1.1:1

Connected to client:('127.0.0.1', 50208)

Received the number of hash from client:3

Received the username from client:ebrahim

**Received the hashed password from client:173af653133d964edfc16cafe0a
ba33c8f500a07f3ba3f81943916910c257705

User found and logged in

لاگین دوم:

Client

Port:1

Number of logins:3

Username:ebrahim

Password:***

Run

Received response from server:
Hello from the server, your number of hash has been received!

Received response from server:
Hello from the server, your username has been received!

Received login response from server:
**message from the server, your usernme and password have been checked
and And your account validation is correct! you are logged in :)

Received login response from server:
**message from the server, your usernme and password have been checked
and And your account validation is correct! you are logged in :)

Login

Server

Port:1

Password:123

Start Server

Server listening on 127.0.1.1:1

Connected to client:('127.0.0.1', 50208)

Received the number of hash from client:3

Received the username from client:ebrahim

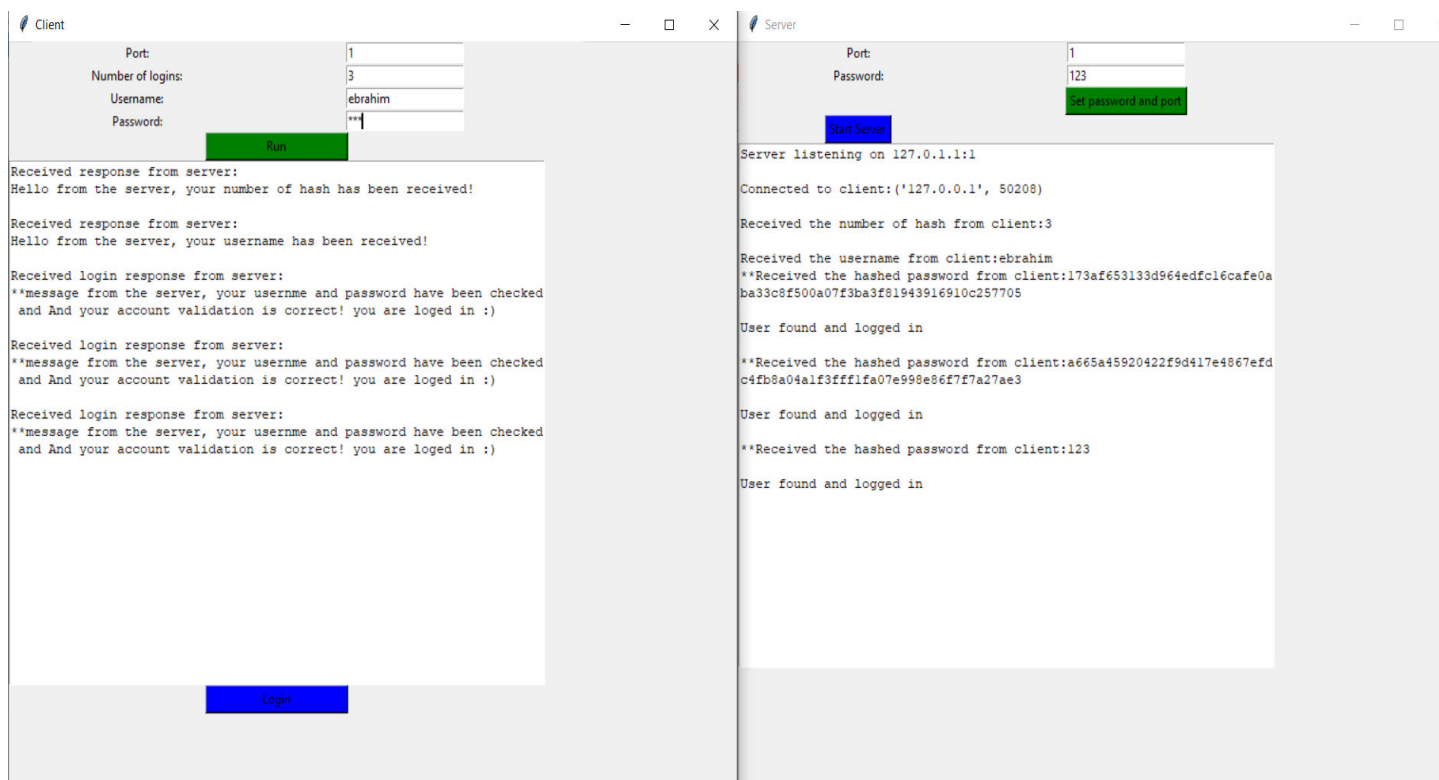
**Received the hashed password from client:173af653133d964edfc16cafe0a
ba33c8f500a07f3ba3f81943916910c257705

User found and logged in

**Received the hashed password from client:a665a45920422f9d417e4867efd
c4fb8a04a1f3fff1fa07e998e86f7f7a27ae3

User found and logged in

لاگین سوم (آخر):



همانطور که در لاگین آخر مشاهده میکنیم سرور در پایان رمز اصلی کاربر را دریافت میکند. البته این امر درست نیست و باید آخرین 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.

