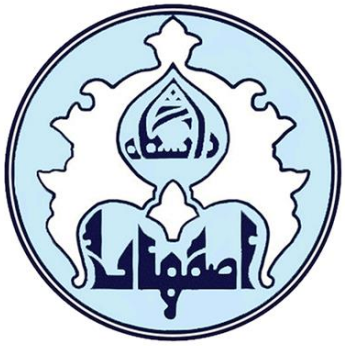
به نام خدا



پروژه پیاده سازی احراز هویت از طریق Lamport

استاد درس:

حسین تهامی

تهیه کننده: زهرا منصوری

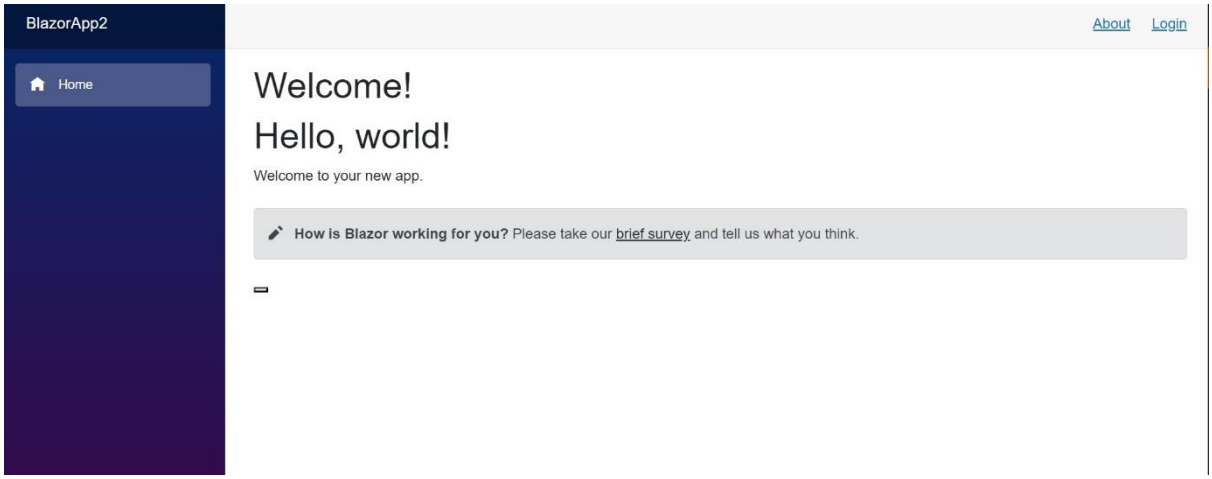
زمستان ۱۴۰۲

توضیحات اولیه:

این پروژه ا طریق فریم ورک asp .net برای قسمت بک اند، فریم ورک Blazor برای فرانت اند و sql Server برای دیتابیس و ذخیره داده ها استفاده شده است، که در ادامه توضیحات مرتبط داده میشود:

مراحل انجام احراز هویت را بررسی میکنیم:

۱- در زیر صفحه اصلی برنامه قبل از احرا هویت کاربر قابل مشاهده است:

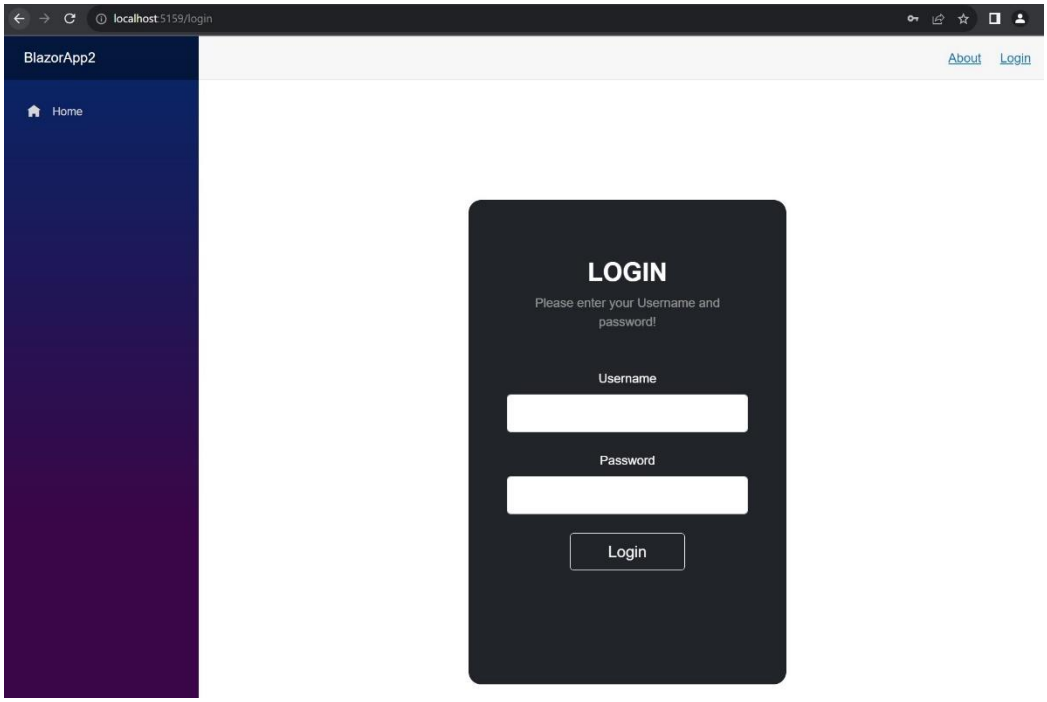


و داده های ذخیره شده در جدول کاربران به صورت زیر است:

(کاربر admin رمز ۱۱۱۱ را در هنگام ثبت نام وارد کرده است که یک بار هش شده و در ستون پسورد ذخیره شده و n که نشان دهنده شماره نوبتی است که کاربر میخواهد وارد سایت شود)

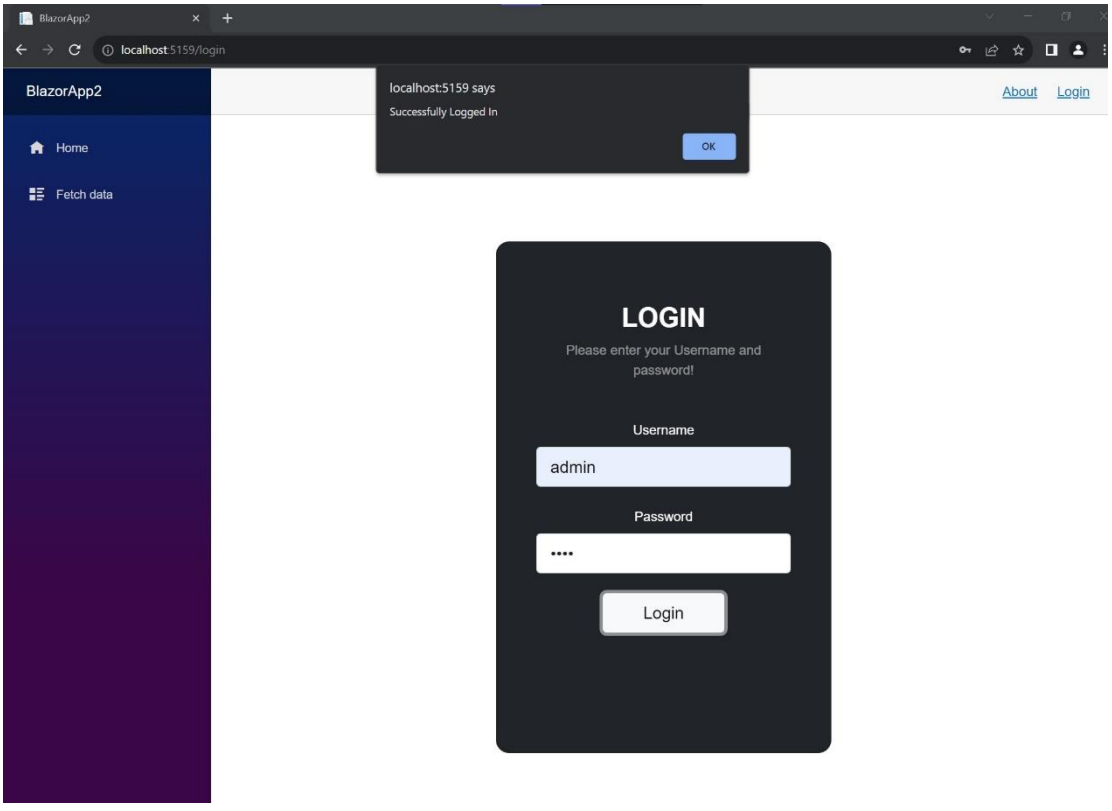
	ID	UserName	Password	Role	n
▷	bf2f-f6aa5fbeefbb	admin	ed18b67948fd...	Administrator	9
	fbe11cfc-933d-...	user	c22d5e599c66...	User	10
	NULL	*NULL*	*NULL*	*NULL*	*NULL*

۲. با کلیک کردن روی login در قسمت نوبار وارد صفحه ورود میشویم:



از آنجایی که کابر admin برای اولین بار است که وارد سایت میشود باید ۹بار از مقدار ۱۲۳۴ هش گرفته و آن را در فرم وارد کند.

(دزسمت بک‌اند از مقدار ورودی هش گرفته میشود و با مقدار ستون پسورد در دیتابیس مقایسه میشود، همانطور که در تصویر مشخص است در ساید بار بعد از احراز هویت یک گزینه جدید با عنوان Fetch data اضافه شده و ستون پسورد با مقدار جدید جایگزین میشود)



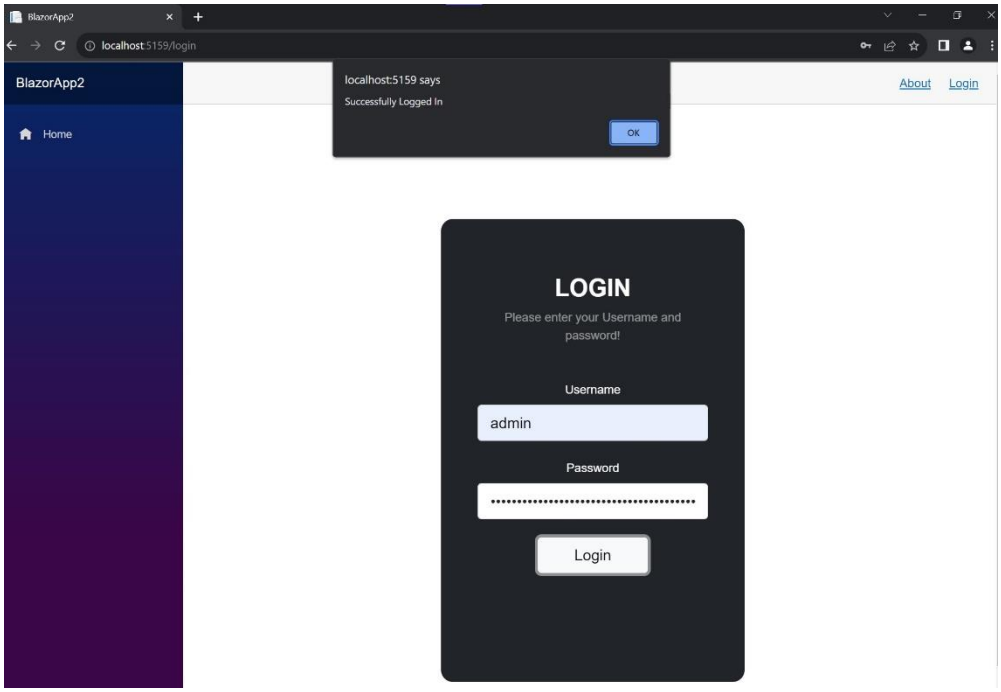
۳- در گام بعدی فرض میکنیم میخواهیم دوباره با کاربر admin وارد شویم دو حالت وجود دارد یا کاربر میداند که بار چندمی است که میخواهد وارد شود و درواقع چالشی که با آن روبرو است چیست یا اینکه نمی‌داند:

در حالت اول: کاربر با توجه به دانشش به تعداد n-i-1 از رمز اصلی هش میگیرد و سپس طبق قبل پس از زدن login از ورودی هش گرفته میشود و با مقدار ذخیره شده در دیتابیس مقایسه میشود:

اینبار i=2 است پس باید Hash(p)^8 را محاسبه کنیم:

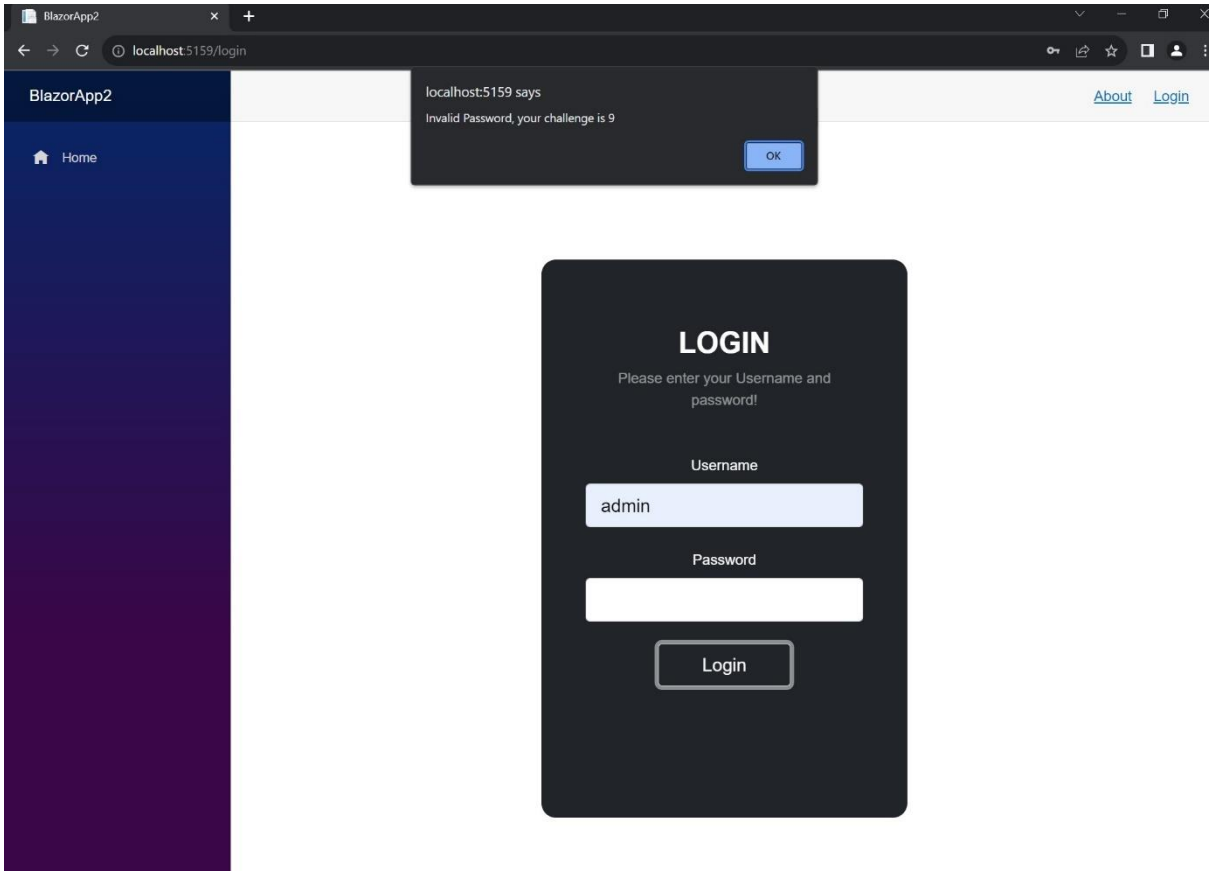
```
6c3a3172fbec5eb14f10386c8ed17b6c83c91d42590b49eb62fca8e28daa75c3
```

سپس با وارد کردن هش بدست آمده احراز هویت کامل میشود:



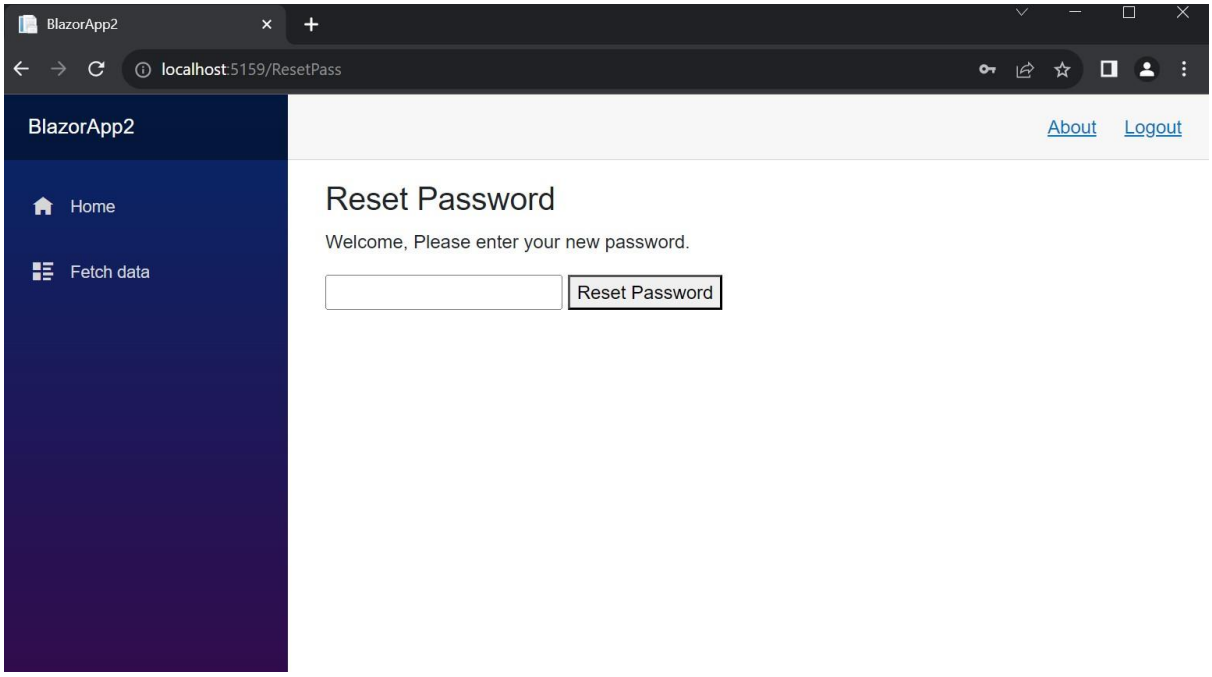
در حالت دوم اگر کاربر از مقدار n آگاه نباشد، اگر تنها فیلد نام کاربر را وارد کند شماره چالش و در واقع مقدار n به

او داده می‌شود:



۴- حالت بعدی که باید درنظر بگیریم این است که مقدار i به ۱ برسد.باید پسورد جدیدی توسط کاربر تعیین

شود:



داده های دیتابیس نیز بصورت زیر تغییر میکنند:

(مقدار n دوباره ۱۰ شده به این معنی که کاربر هنوز از این رمز عبور جدید برای ورود استفاده نکرده است.)

	ID	UserName	Password	Role	n
	7a3f4867-31b7...	admin	ed18b67948fd...	Administrator	10
	fbe11cfc-933d-...	user	c22d5e599c66...	User	10
	NULL	*NULL*	*NULL*	*NULL*	*NULL*

نکته۱: مقدار i در ستون nدیتابیس ذخیره شده است.

نکته۲: مقدار n برای کاربران بطور پیش فرض ۱۰ در نظر گرفته شده است.

نکته۳: برای هش کردن از روش SHA256 استفاده شده است.

منابع استفاده شده:

https://www.cs.cornell.edu/courses/cs513/2005fa/NL11Lamport.html

https://lamport.azurewebsites.net/pubs/password.pdf