مهندسی اینترنت

تمرین شماره‌ی نهم

مدرس: رامتین خسروی

موعد تحویل: دوشنبه ۳ خرداد ۱۳۹۵

مقدمه

در این تمرین قصد داریم به پروژه Authentication، Authorization و به طور کلی برخی نیازمندی‌های امنیتی را اضافه کنیم.

بیان مسأله

در این تمرین پروژه‌ی شما باید موارد زیر را پشتیبانی کند:

۱- Authorization:

سیستم باید شامل نقش‌های کاربر معمولی، مدیر سیستم (Admin)، متصدی امور مالی و صاحب شرکت باشد. هر کدام از این سه نقش می‌توانند وظایفی را انجام دهند.

الف- کاربر معمولی: کاربر معمولی می‌تواند بعد از ورود به سیستم وظایف زیر را انجام دهد:

درخواست افزایش یا کاهش اعتبار

درخواست خرید و فروش سهام

مشاهده‌ی وضعیت بازار

مشاهده‌ی صفحه‌ی پروفایل خود (صفحه‌ی پروفایل علاوه بر اطلاعات شخصی، شامل اطلاعات سیستمی مانند میزان اعتبار وسهم‌های خریداری‌شده و همچنین درخواست‌های منتظر تأیید است.)

ب- متصدی امور مالی: متصدی امور مالی می‌تواند بعد از ورود به سیستم وظایف زیر را انجام دهد:

تأیید درخواست‌های منتظر تأیید افزایش و کاهش اعتبار

تأیید خرید و فروش‌هایی که ارزش مالی معامله‌ی آن‌ها از حد مجاز بیشتر است

مشاهده‌ی وضعیت بازار

مشاهده‌ی صفحه‌ی پروفایل خود (اطلاعات شخصی)

پ- صاحب شرکت: صاحب شرکت بعد از ورود به سیستم می‌تواند وظایف زیر را انجام دهد:

اضافه کردن نماد جدید و قرار دادن آن را برای فروش

مشاهده‌ی وضعیت بازار

مشاهده‌ی صفحه‌ی پروفایل خود (اطلاعات شخصی و همچنین اطلاعات سیستمی وضعیت نمادهای خود شامل حالت نماد، خریداران و درصد سهام هر کدام)

ت- مدیر سیستم: مدیر سیستم علاوه بر وظایف کاربر معمولی، متصدی امور مالی و صاحب شرکت می‌تواند وظایف زیر را انجام دهد:

مشخص کردن حد مجاز برای ارزش مالی معاملات که ارزش‌های بالاتر از آن نیاز به تأیید دارد

تأیید نماد جدید اضافه شده برای ورود به بازار خرید و فروش

مشاهده‌ی گزارش درخواستی (گفته‌شده در پروژه‌ی قبلی)
نقش دادن به دیگر کاربران
مشاهده‌ی پروفایل دیگر کاربران
گرفتن Backup (به شکل گفته شده در پروژه‌های قبلی) از پروژه

دقت کنید که هر کاربر می‌تواند چند نقش داشته باشد. برای مثلا یک کاربر که نقش صاحب شرکت را دارد برای خرید سهام از نمادهای مختلف باید نقش کاربر داشته باشد.

۲- Authentication:

سیستم باید دارای Login کاربران بر اساس نام کاربری و پسورد باشد. همچنین کاربرهای جدید نیز می‌توانند در سیستم ثبت‌نام کنند. (کاربر تازه‌ثبت‌نام‌شده کاربر معمولی محسوب می‌شود و تنها مدیر سیستم است که می‌تواند نقش آن را عوض کند.) فرم ثبت‌نام کاربران باید شامل اطلاعاتی چون نام، نام خانوادگی، پست الکترونیکی، نام کاربری، پسورد و تکرار آن باشد. همچنین در ابتدا کار همیشه سیستم دارای یک کاربر با نقش مدیر سیستم است.

۳- مسائل امنیتی: از حملات CSRF جلوگیری شود. همچنین سیستم باید عاری از SQL-Injection باشد.

نکات پایانی:

- نکات مطرح شده در تمرینات قبلی
- صفحه‌ی مدیر سیستم نباید از صفحه‌ی باقی کاربران با نقش‌های دیگر جدا باشد بلکه باید در یک صفحه و با سطح دسترسی‌های مختلف باشد.
- Validationهای لازم و کافی بر روی تمامی فرم‌ها و اطلاعات حاضر در پروژه باید به درستی انجام شود.
- پروژه‌ی شما از جهت واسط کاربری باید قابل قبول باشد. همچنین نمایش هر نیازمندی گفته‌شده باید صفحه نمایش مناسبی داشته باشد. (برای مثال منوهای نقش‌های مختلف، پنل مدیریت)
- پیام‌های بروز خطا یا نتیجه‌ی موفق باید به درستی و به‌نحوی قابل قبول به کاربر سیستم نمایش داده‌شود.
- هسته‌ی مرکزی بورس باید دقیقا مانند همان چیزی که در تمرین‌های قبل گفته شده‌است کار کند.
- هرگونه فرض منطقی برای سیستم که در چارچوب فرضیات گفته‌شده در مسئله باشد قابل قبول است.