1. Replay Attacks

تهدید: دریافت پیام‌های رد و بدل شده میان سرور و کلاینت و فرستادن پیام‌های ضبط شده به سمت سرور برای ایجاد اختلال در روند کاری سرور.

راه حل تدبیر شده : رمزگذاری کردن پیام‌ها توسط SSL که به وسیله‌ی Spring انجام میشود. کلید رمزگذاری برای این عملیات در دایرکتوری Resources و در پوشه‌ی keystore قرار دارد.

2. Improper Inputs

تهدید: طول ورودی بسیار بزرگ باشد و مهاجم سعی در کند کردن سرور یا از کار انداختن ان را دارد.

راه حل تدبیر شده : دیتابیس Sql با توجه به محدودیت‌های اعمال شده بر ان مانع از ذخیره‌ی اطلاعات بسیار طویل. و اخطار مناسب را به کلاینت میدهد.

تهدید: فرستادن اطلاعات اشتباهی که سرور هنگام برخورد با ان‌ها دچار اختلال شده و کارایی خود را از دست بدهد.

راه حل تدبیر شده : اگر فرمت اشتباه ورودی جزو 21 اکسپشن طراحی شده باشد. سرور با استفاده از ان‌ها اخطار مناسب را به کلاینت میدهد و به کار خود ادامه میدهد. اما اگر خطا جزو 21 اکسپشن طراحی نباشد. سرور اسپرینگ از خطاهای موجود در خود استفاده کرده و اخطار مناسب را به کلاینت میدهد و به کار خود ادامه میدهد.(مهاجم تحت هیچ شرایطی نمیتواند با استفاده از اطلاعات نامناسب سرور اسپرینگ را از کار بیندازد.)

3. SQL INJECTION

تهدید : دادن اطلاعات مخرب برای دسترسی غیرمستقیم به دیتابیس سرور.

راه حل تدبیر شده : JPA کنترل Query زدن را از برنامه نویس میگیرد به طوری که وارد کردن Query کاملا توسط JPA انجام میشود. و در JPA، Query هایی که ممکن است باعث دسترسی مهاجم به دیتابیس شوند به طور خودکار حذف میشوند. و در نتیجه این مشکل کاملا توسط JPA هندل میشود.

4. Brute Force

تهدید: فرستادن درخواست‌های مکرر برای دسترسی به رمز کاربردهای مختلف به صورت تصادفی و اتوماتیک.

راه حل تدبیر شده : هنگام ورود کاربر یا ثبت نام کاربر جدید یک سوال ریاضی از طرف سرور به سمت کلاینت فرستاده میشود. و جواب این سوال در سمت سرور چک میشود. این کار مانع از فرستادن درخواست‌های مکرر به سمت سرور برای پیدا کردن رمز کاربران به صورت تصادفی
این قسمت در بخش RegisterMenuController برای کلاینت و در بخش AuthenticationController در بخش سرور قابل مشاهده است.
و همینطور اگر تعداد درخواست‌ها از حدی بیشتر باشد همان سیستم DoS جلوی ارتباط بیشتر با سرور را میگیرد.

5. Denial Of Service (DoS)

تهدید: مهاجم سعی دارد با فرستادن درخواست‌های مکرر سرور را از کار بیندازد.

راه حل تدبیر شده : در کلاس Interceptor هر درخواست اطلاعاتش مانند ای پی و تایم درخواست ذخیره شده، و اگر تعداد درخواست‌ها در مدت معینی از مقدار معینی بیشتر شود. سرور دیگر جوابی به کلاینت تا سپری شدن مدت زمان تعیین شده نمیدهد.

6. Broken Authentication

تهدید: دسترسی مهاجم به دیتابیس و پیدا کردن رمز عبور کاربران یا توانایی رمزگشایی پسوردهای رمزنگاری شده به دلیل ضعیف بودن الگوریتم انتخاب شده.

راه حل تدبیر شده : همه‌ی پسوردها با استفاده از SHA-256 هش شده‌اند. و برای چک کردن پسورد هش ان پسوردها چک میشود.

تهدید : توانایی استخراج لیست یوزرنیم‌ها از اکسپشن‌های فرستاده شده از طرف سرور. و استفاده از ان‌ها برای لاگین کردن بدون پسورد.

راه حل تدبیر شده : هنگام لاگین کردن اگر فیلدی غلط پر شود. سرور هیچ اطلاع اضافی به کلاینت نمیدهد. و فقط خبر از اشتباه بودن یک فیلد را میدهد.

تهدید : استفاده از توکن‌های افراد دیگر برای استفاده از اکانت دیگران بدون لاگین کردن.

راه حل تدبیر شده : بخاطر استفاده از SSL مهاجم قادر به شنود اطلاعات رد و بدل شده میان سرور و کلاینت نخواهد بود و نمیتواند به توکن فرد دیگری دسترسی پیدا کند. و توکن به دلیل هش شدن توسط توسط SHA-256 به هیچ مهاجمی قابلیت حدس زدن ان را نمیدهد.