گزارش اقدامات امنیتی

1 - در وهلة اول ، برای افزایش قدرت امنیتی لایه بالایی پروژه ، سراغ اعتبار سنجی های پروژه رفتیم و تمامی اعتبار سنجی ها را دوباره بررسی و بعضا قوی تر از قبل کردیم . به عنوان مثال به اعتبار سنجی ها محدودیت تعداد کاراکتر اضافه کردیم تا دچار مشکلات حافظه نشویم . در بخش ایمیل ، کاربران را محدود به استفاده از سرویس گوگل کردیم تا ایمیل های نامعتبر دریافت نشود . برای رمز کاربر هم ، کاربر را وادار به استفاده از حروف کوچک ، بزرگ و اعداد و علائم نگارشی کردیم و همچنین رمزگزاری نمی تواند کمتر از 8 کاراکتر باشد تا مبادا مهاجمان سایبری بتوانند با دیکشنری ها و لیست های رمز های استفاده شده و ... به سیستم نفوذ کنند.

2 - قدم بعدی برای حفظ امنیت کاربران ، رمزگزاری اطلاعات است . به این منظور ، رمز های کاربران hash و salt شده است که برای امنیت بیشتر salt ، برای هر رمز salt به صورت شانسی تولید می شود و فقط طول مشخص دارد و پس از اضافه شدن این پیشوند ، رمز ها بر اساس الگوریتم مشخصی تغییر می کنند و ذخیره می شوند

3 – اقدام بعدی ، blacklisting و محدود کردن تلاش های یک کاربر برای ورود است تا از حملات brute force و Dos جلوگیری شود که برای این منظور ، IP هایی که در مدت زمان کم ، بیش از تعداد مشخصی تلاش ناموفق داشته باشند ، به لیست سیاه سیستم اضافه می شوند و درخواست های این IP ها در جا رد می شوند

4 – نهایتا ، آخرین اقدام مربوط به بستن برنامه قبل از خارج شدن است که برای این منظور ، تابعی برای وقتی کاربر علامت ضربدر بالای صفحه را می زند صدا می شود که خود به خود کاربر را از برنامه خارج می کند