به نام خداوند جان و خرد

تمرین تحویلی امتیازی

درس مهندسی نرم افزار 2

گروه سوم

علیرضا زارع زین آبادی ۹۹۳۱۰۲۲

امیرفاضل کوزه گر کالجی ۹۹۳۱۰۹۹

رضا فرح‌بخش ۹۹۳۱۰۷۴

محمدحسین ساعدی ۹۹۳۱۰۲۵

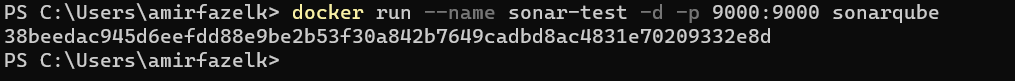
بخش پیاده سازی اول

مرحله اول)

**سوال اول**

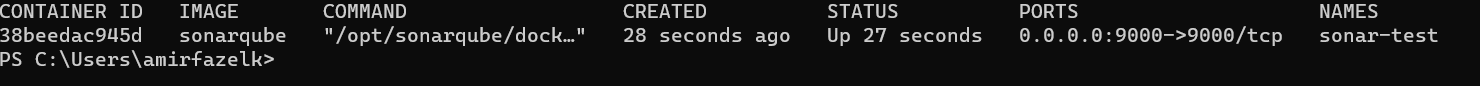
Sonarqube، ابزار پیشرو برای بازرسی مداوم کیفیت کد و امنیت پایگاه های کد شما و هدایت تیم های توسعه در طول بررسی کد است. SonarQube با پوشش 27 زبان برنامه‌نویسی، در حالی که با خط لوله نرم‌افزار موجود شما جفت می‌شود، راهنمایی‌های اصلاحی واضحی را برای توسعه‌دهندگان برای درک و رفع مشکلات و به طور کلی برای تیم‌ها ارائه می‌کند تا نرم‌افزار بهتر و ایمن‌تری را ارائه کنند.

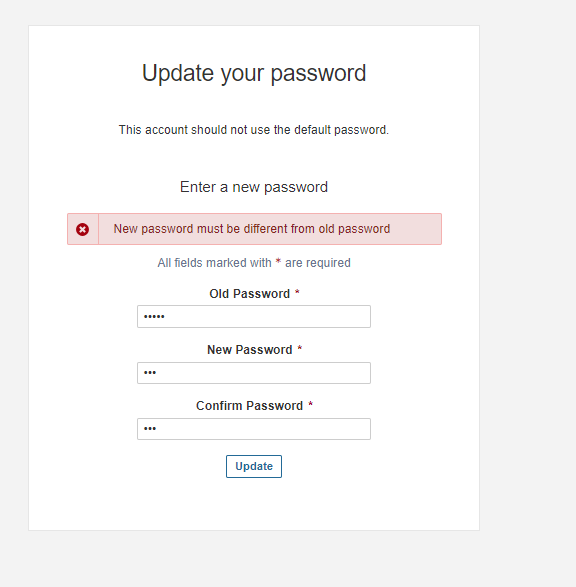
**سوال دوم**



مرحله دوم)

**سوال سوم**

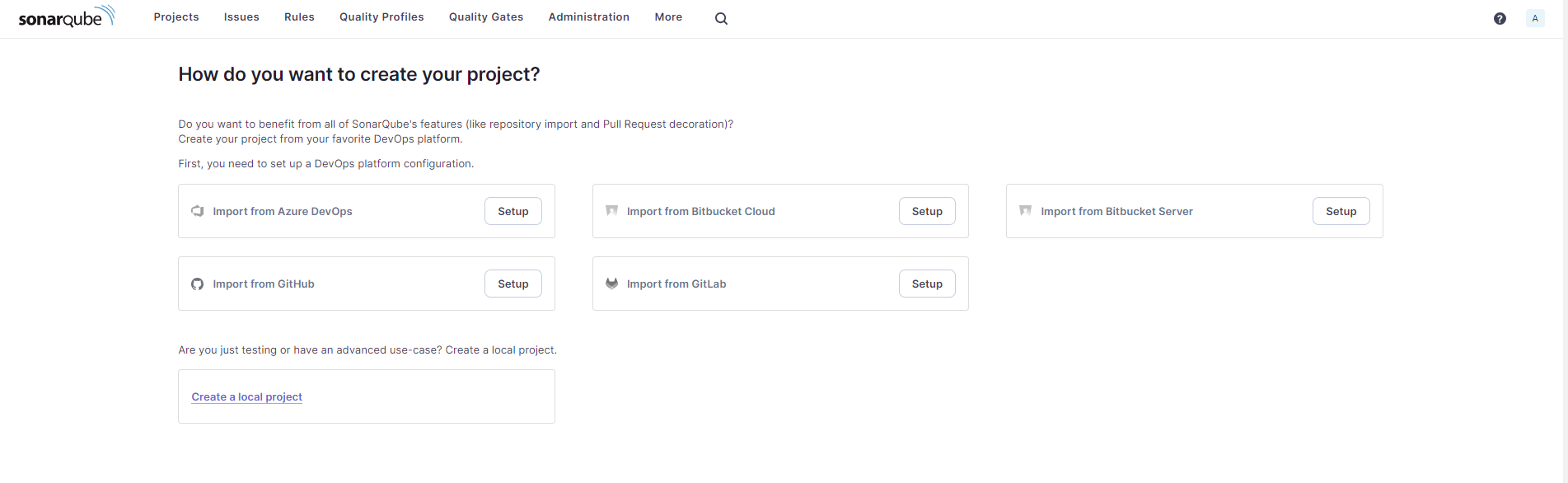


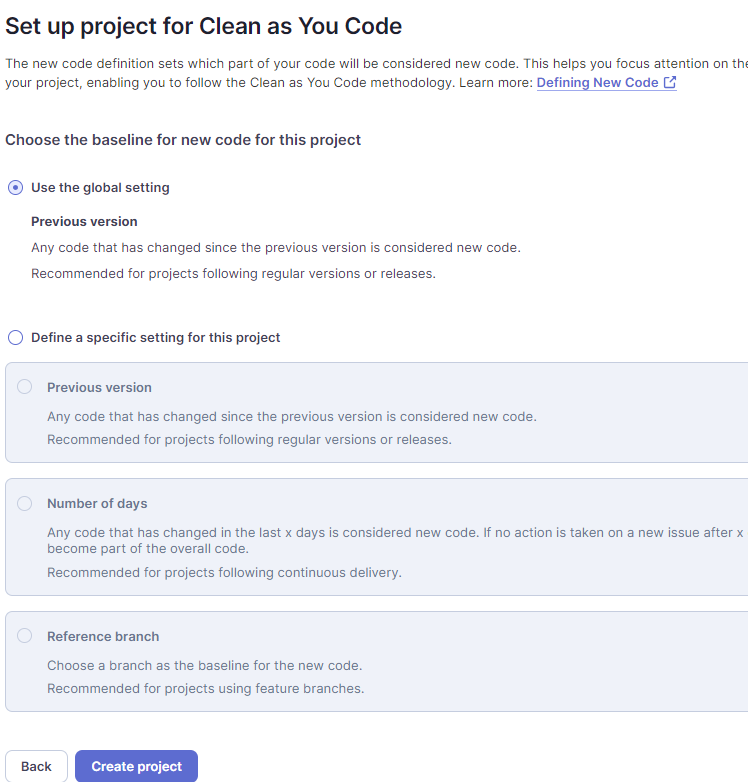
مرحله سوم)

**سوال چهارم**

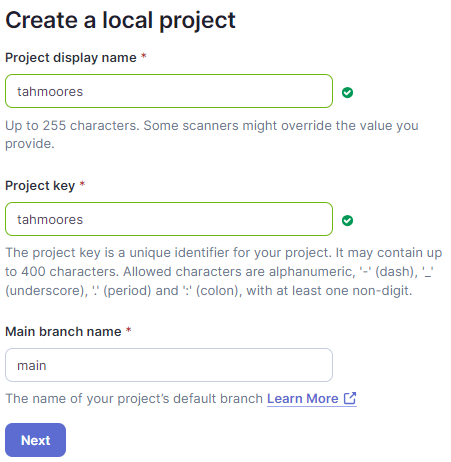
پس از وارد کردن اطلاعات صفحه تغییر رمز کاربری نشان داده می‌شود:

در ادامه صفحه اولیه به مانند زیر می‌باشد:



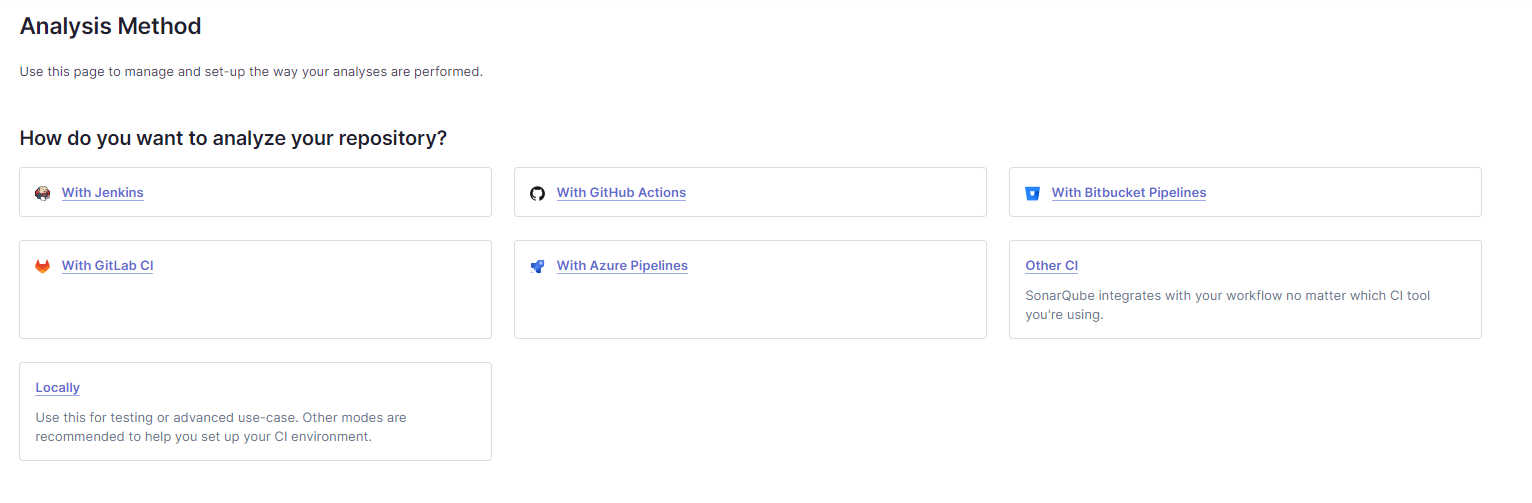
مرحله چهارم)

پروژه جدیدی را به صورت لوکال می‌سازیم:



مرحله پنجم)

در این مرحله نیز، طبق گفته دستور کار، لوکال را به عنوان نحوه آنالیز کد مشخص می‌کنیم

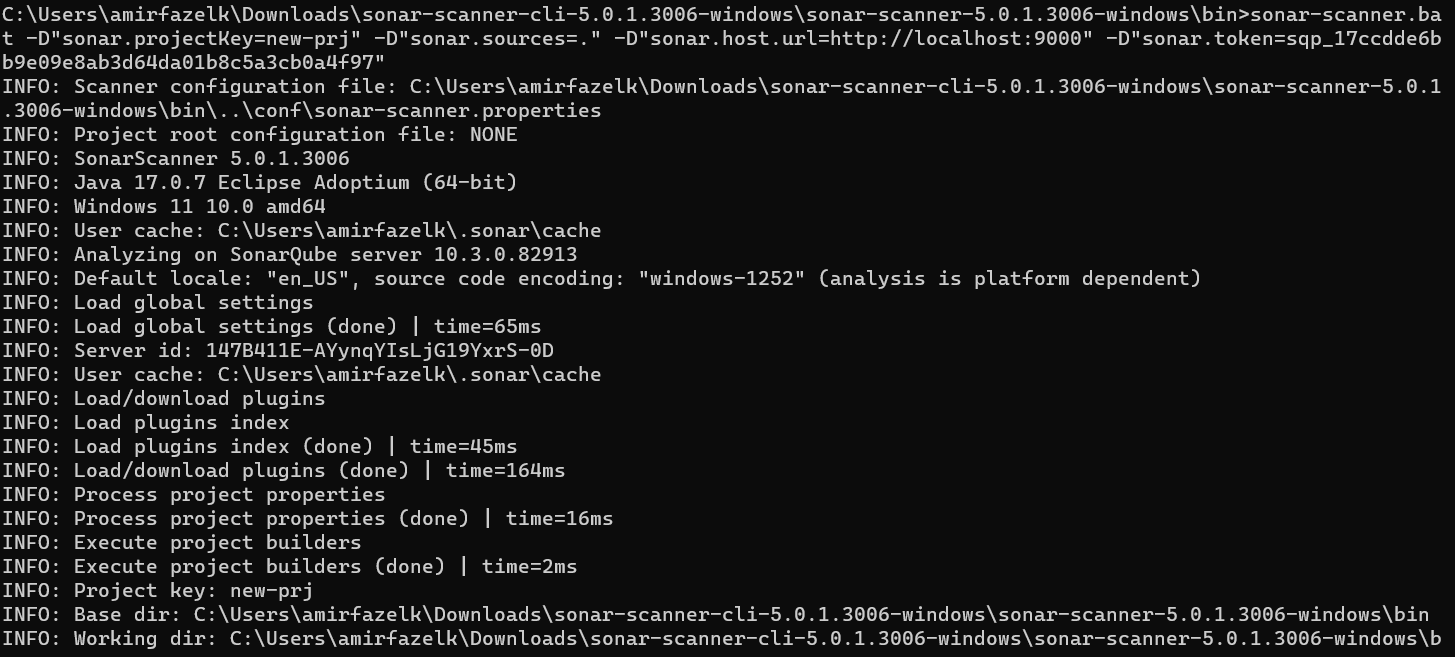


مرحله ششم)

در این مرحله با انتخاب یک نام، توکن درخواستی را تولید می‌کنیم.

مرحله هفتم)

در این مرحله، ابزار sonarscanner را نصب کرده، و دستور داده شده توسط خود برنامه را اجرا می‌کنیم.



**سوال پنجم**

با مراجعه به لینک داده شده در دستورکار و نصب نسخه مورد نظر sonarscanner بر اساس سیستم عامل خود، آن را نصب می‌کنیم.

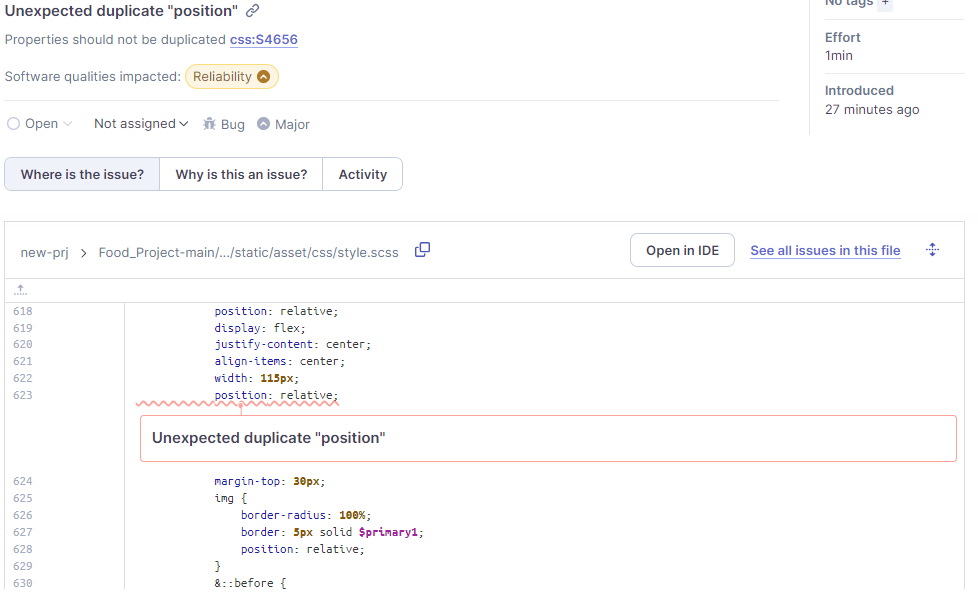
برای آنالیز کردن بیلد های برنامه های مان نیاز به یک اسکنر داریم. در sonarqube هم از اسکنر sonarscanner استفاده می‌شود تا بتوان بیلد های برنامه توسعه یافته مان را اسکن کرد.

مرحله هشتم)

**سوال ششم**

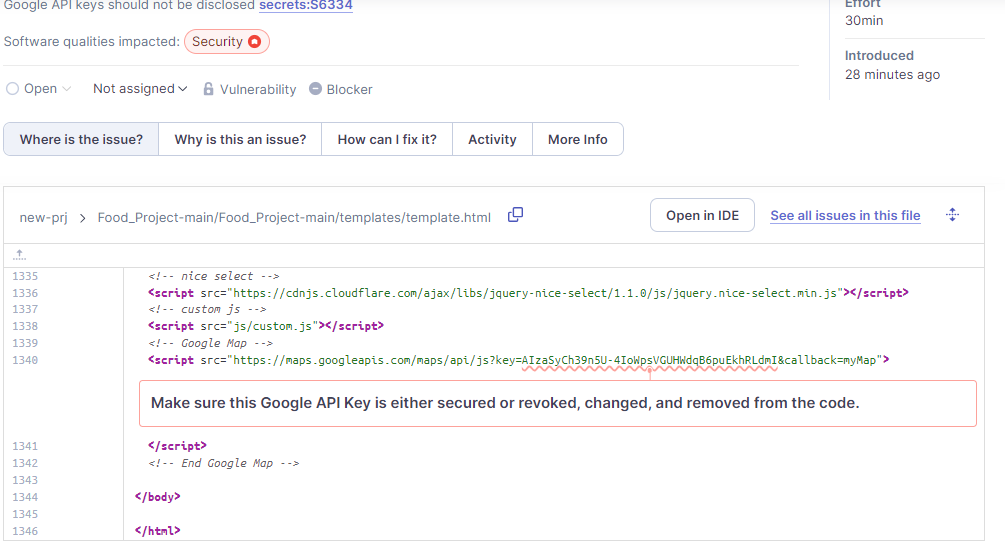
Bugs:

تعداد خطاهای درون کدی که باعث ایجاد خطا در رفتار برنامه هنگام اجرا می شود. تعداد این مورد برابر با 26 می‌باشد.



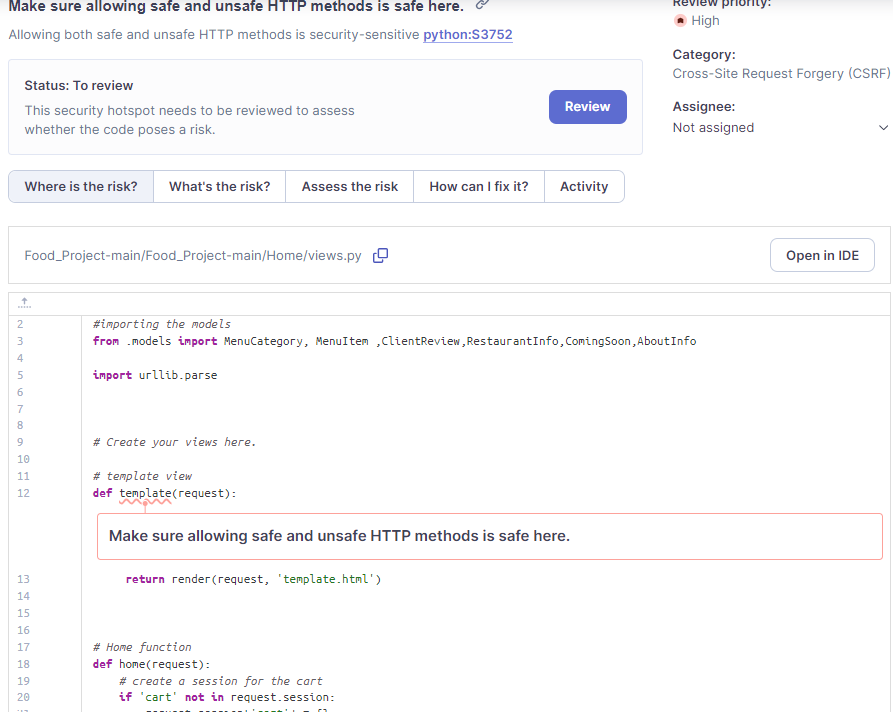
Vulnerabilities:

این مورد نشان دهنده آسیب پذیری های درونی سیستمی است. تعریف دقیق تر آن، عبارت است از ویژگی یا نقطه ضعف سیستم که ممکن است از آن علیه خودمان سو‌استفاده شود. تعداد این مورد برابر با 2 است.

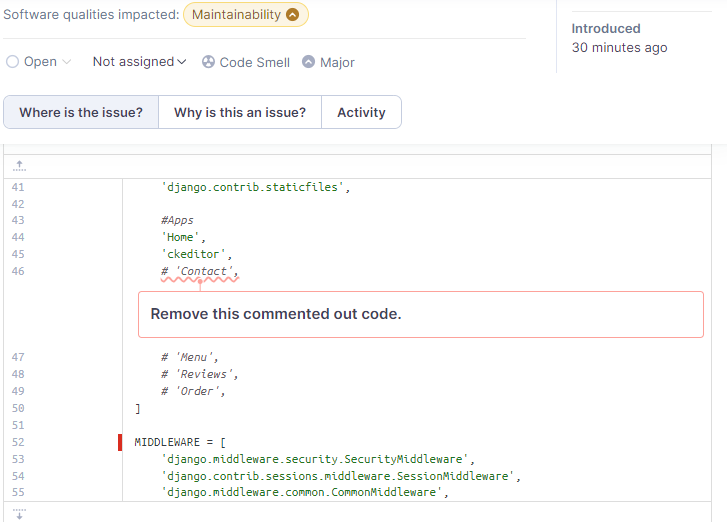
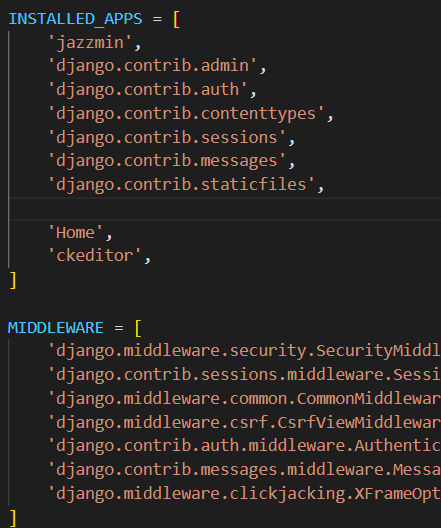


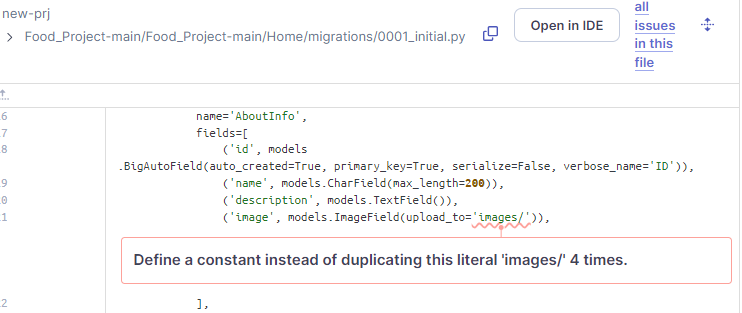
Security hotspots:

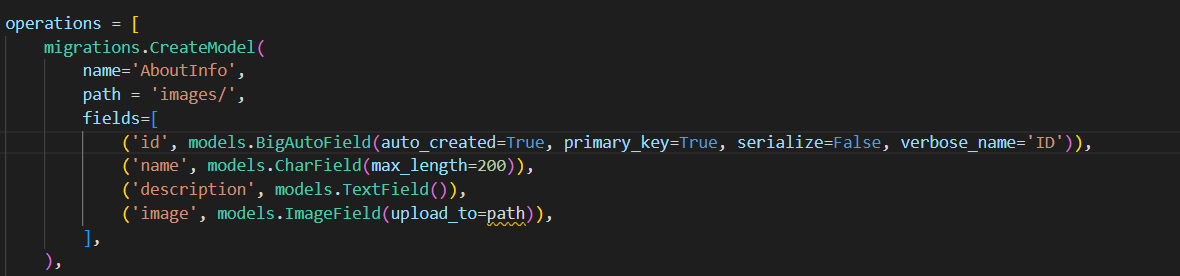
قطعه هایی از کد که به نا امنی حساس هستند و باید به صورت دستی بررسی شوند تا تشخیص داده شوند یک آسیب پذیری هستند یا نه. تعداد این مورد برابر است با 15.



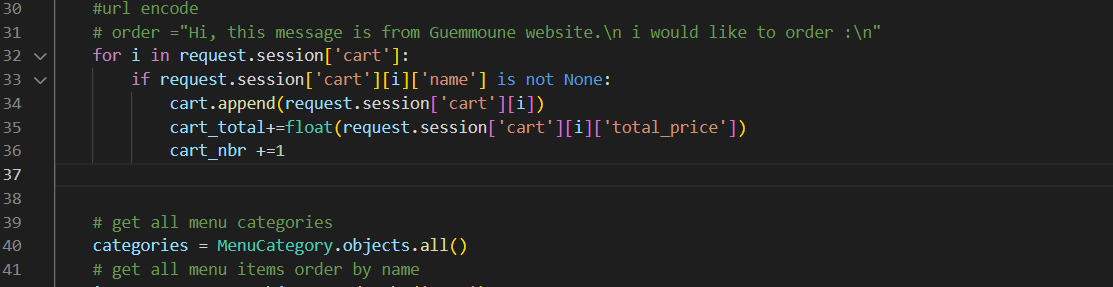
**سوال هفتم**

Code smell ،نتیجه برنامه نویسی ضعیف یا نادرست است. این مورد در کد برنامه اغلب می تواند به طور مستقیم به اشتباهات توسط برنامه نویس برنامه در طول فرآیند کدنویسی ردیابی شود. در ادامه به حل کردن برخی از code smell های برنامه داده شده می‌پردازیم:







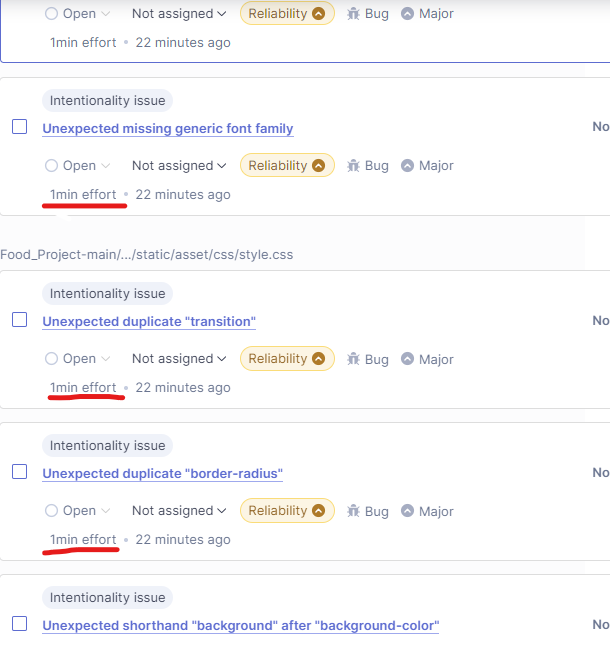


**سوال هشتم**

Vulnerability، آسیب پذیری ای است که قطعیت آن ثابت شده و مشخص است که امکان سو‌استفاده از آن جهت ضربه زدن به برنامه مان وجود دارد. در دست دیگر، security hotspot، بخشی از کد مان است که از نظر امنیتی حساس به حساب می‌رود و باید به صورت دستی بررسی شود تا آسیب پذیر بودن آن قطعه کد تایید یا رد شود.

**سوال نهم**

بدهی فنی هزینه ضمنی کار مجدد در آینده است که هنگام انتخاب یک راه حل آسان اما محدود به جای یک رویکرد بهتر که می تواند زمان بیشتری را ببرد. در ادامه برای محاسبه میزان بدهی فنی، مجموع میزان زمانی که این برنامه به ازای تمامی باگ های برنامه ما در نظر گرفته است را جمع می‌کنیم.



این مقدار برابر می‌شود با: 44 دقیقه. (این مسئله فقط در بخش باگ ها بررسی شده است.)

بخش پیاده سازی دوم

در این بخش با توجه به گفته دستور کار، باید یک برنامه تحت وب را با استفاده از افزونه سلنیوم تست کنیم. این افزونه مناسب برای ضبط کردن اقدامات پشت سر هم کاربر می‌باشد و آن ها را ذخیره می‌کند تا بتوان یک فعالیت خاص که شامل چندین قدم می‌شود را یک جا ذخیره و آن را چندین بار اجرا کنیم.

با توجه به تهیه یک فایل با نام sizzle.side که تمامی سناریو های خواسته شده در دستور‌کار را در‌بر می‌گیرد، همچنین نبود ویژگی های گرافیکی خاصی در این مورد پیاده سازی، موردی برای ثبت در این گزارش وجود ندارد و می‌توانید به فایل نام برده مراجعه و تست سناریو های مختلف را در آن مشاهده کنید.

در پس انجام این سناریو ها اما، برخی باگ هایی که عمدتا مربوط به تجربه کاربری می‌شد، مشاهده شدند که لیست زیر را تشکیل می‌دهند:

- not showing proper error message on invalid user

- not showing proper error message on wrong password

- not showing proper error message on empty cart, confirmation

- having to add the image again to the form while updating a food info

- having fixed value for the price input, unabling us to enter higher values

در ادامه با استفاده از برنامه تحت وب jira، با ایجاد پروژه ای جدید و منتشر کردن هر یک از این باگ ها، یک بک لاگ برای خود ساختیم، سپس به طور بسیار تصادفی هر یک از آیتم ها را به یکی از اعضای گروه، الصاق کردیم. نتیجه نهایی به مانند زیر می‌باشد:

