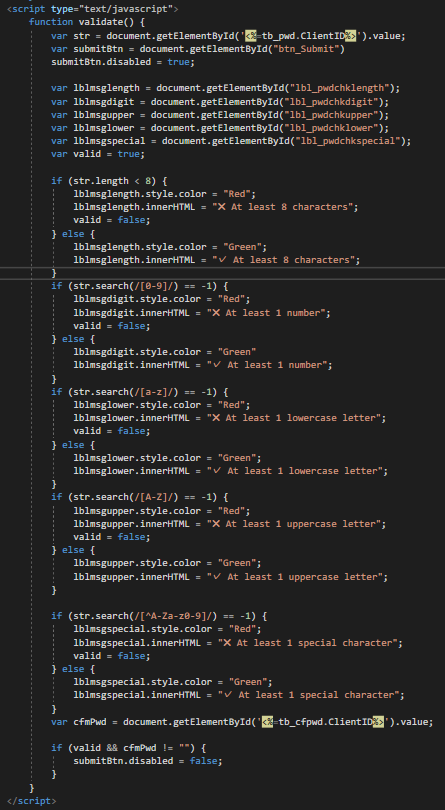
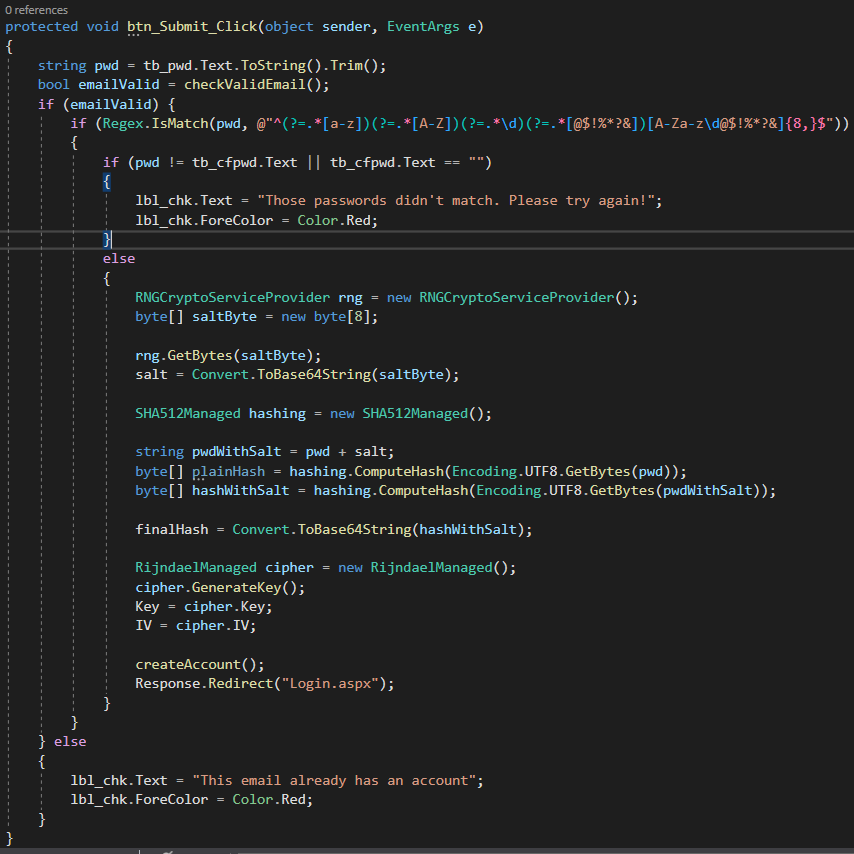
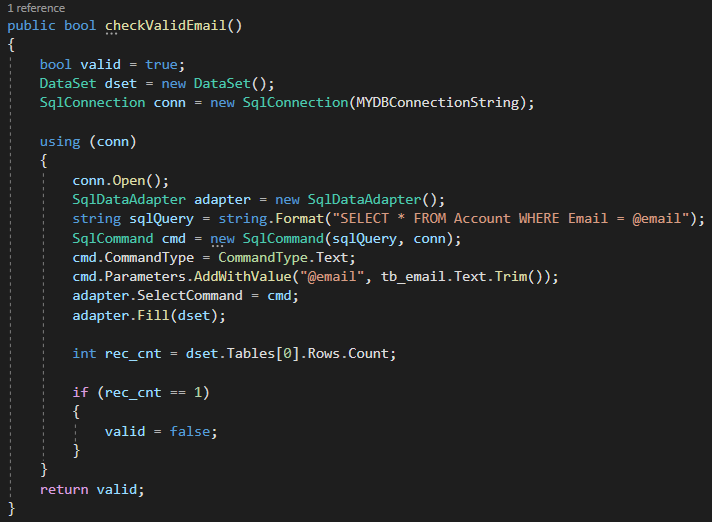
**IT2163 - Application Security Assignment Report**

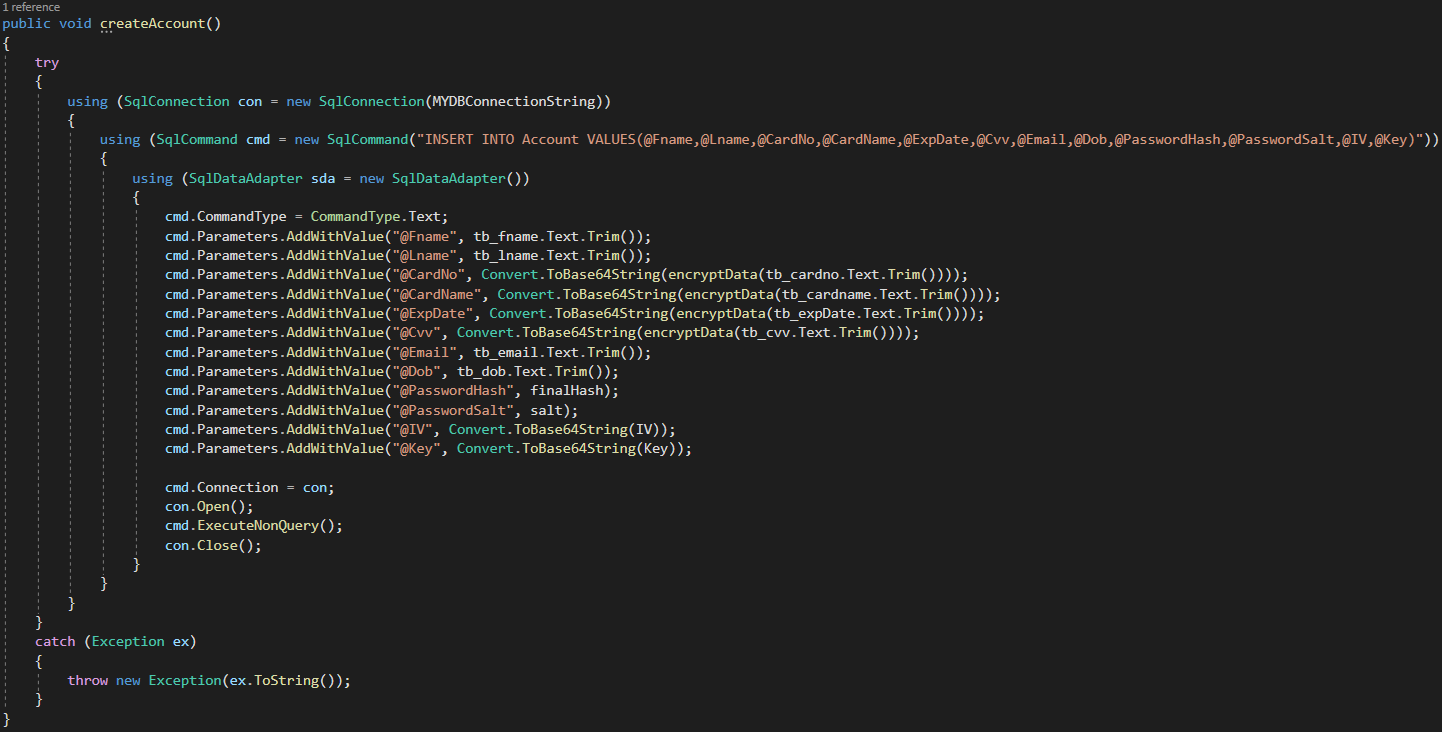
* Set Strong password
  + Perform password complexity checks
  + Offer feedback to user on password.
  + Implement both Client-based and Server-based checks.



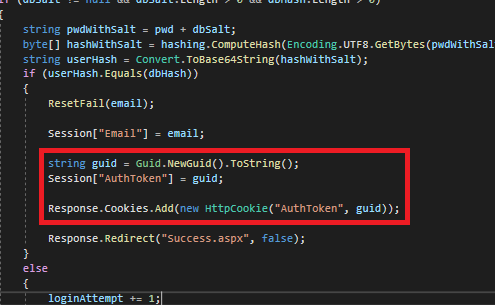


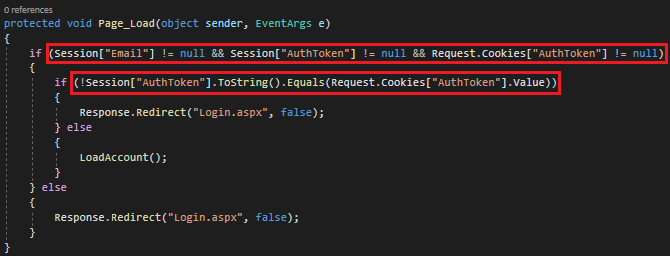


* Securing user data and passwords
  + Implement Password Protection
  + Encryption (Credit card to be encrypted)

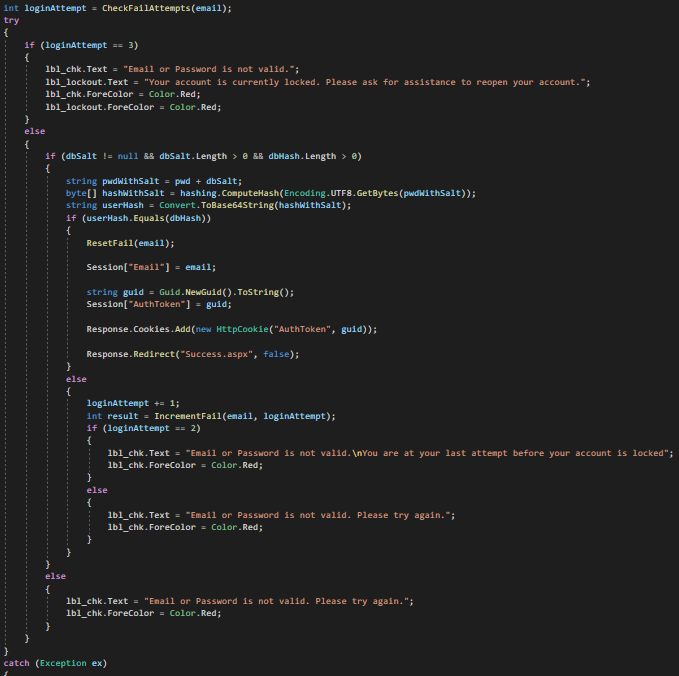


* Login
  + Avoid Session fixation attack

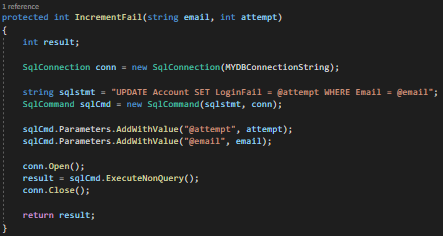


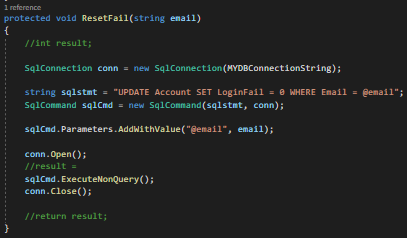


* + Account Lockout after 3 login failures

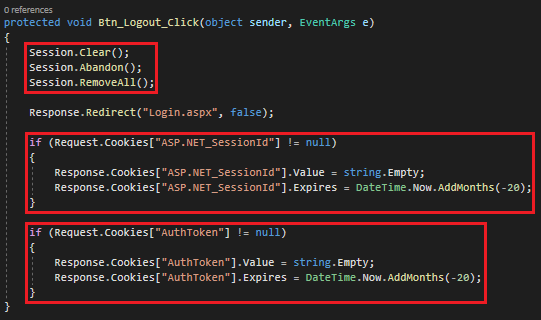




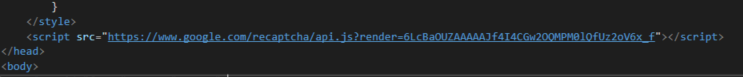


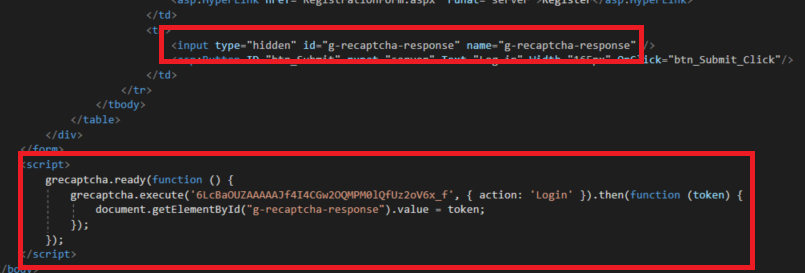


* + Proper and clean logout

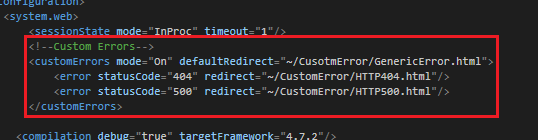


* Anti-bot
  + Implement Google reCaptcha v3 service

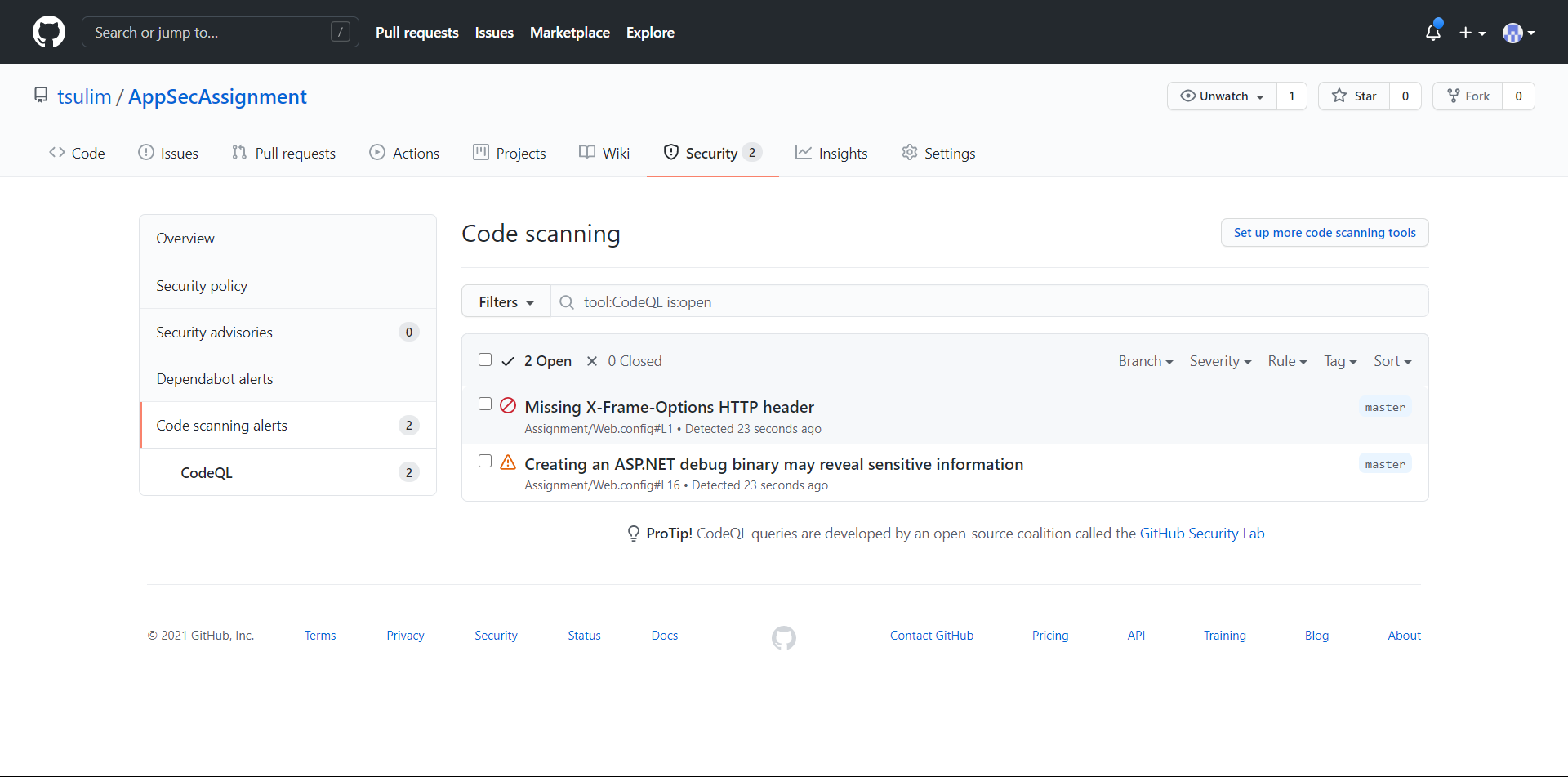




* Proper Input Validation
  + Prevent SQLi and XSS and perform proper input filtering, validation and verification (e.g email)
* Proper Error handling
  + Graceful error handling on all pages (including 404, 403 error pages etc)



* + Provide test cases in our report
* Software Testing
  + Use external tools to perform software testing:
    - snyk.io souce code scanner in Github
    - Arachni
    - Zap



* + Explain remediation effort based on pen-test report.

1. Set the X-Frame-Options HTTP header to DENY, to instruct web browsers to block attempts to load the site in a frame.
2. “Debug” flag should be set to false, or removed completely

* Advanced Features
* Account Policies
  + Automatic account recovery after lockout.
  + Avoid password reuse (max 2 password history)
  + Change password
  + Minimum password age (cannot change password within 5 mins from the last change of password)
  + Maximum password age (must change password after 15 mins)
* Presentation
  + Present web app to your tutor and explain your
  + programming codes.
  + Working prototype with database
  + Error free demo
* Report
  + Create a report to explain how the above security features were implemented.