Secure Software Development

Team Meetings for Team 4

Notes:

Date	14 Sep 2021	Meeting ID	7
Attendees	Andrey Smirnov; Taylor Edgell; Michael Justus;		

Agenda

- ▪ Review Technical Report

Minutes of Meeting

Review Technical Report

The team reviewed the document and agreed we will trim down the content before submission. Current word count is around 1150.

Security considerations: OWASP

- *XML External Entities* - not appliable because we don't leverage XML
- *Insecure deserialization* - not applicable because we don't leverage deserilization only encryption and decryption.
- *Security misconfiguration* - is not clear right now.
- Hard and soft locks. Soft wil be a time duration, hard lock will be a full lockout where Admin must be notified.
- How will we handle the monitoring? Monitoring is all about the "right now", so perhaps we print out a simple message that notifies that a user is performing an action. Expectation is that monitoring is not a requirement, however a background task might be suitable. We can lever a single thread that is raised when an action occurs.

- Logging can be a singleton class, but can be a simple case of look at the important security path and call into a single log class.

Technical Overview

- We won't just throw an API on top of the existing business logic. We will expose a single set of functionality, for example, "Login".
- We should leverage Flask as the API hosting server
- We can add an API block next to the CLI block.
- The implementation is not a full API solution, rather an add-on.

Required Tools

- All good with this section.

Technical Challenges

- All good with this section. We might remove the lack of access modifiers in Python.

References

- All good with this section.

Other Discussion Points

- Should we expand more on testing for example, explicit mention of the tests we're going to do?
  - o Just show *some* evidence of unit testing. Python does not really have integration testing tool.
  - o Maybe mention **what** we're going to tests in terms of *sensitive* parts, or equivalence testing, key values of key functionality.

Report Changes

- We added a Privacy consideration section to deal with GDPR. This is weird to deal with in the solution in that we're dealing with *security* and not so much the *data*.