Secure Software Development – Seminar 2: Scrum Security Review

Contents:

- Announcements
- What is required for the assignment?
- An Outline Approach
- N-tier vs. MVC
- Integrating Code
- Seminar 2 Questions

Announcements:

- UK Daylight Saving Time – 27.03.2022 → Time changing

What makes an App Secure?

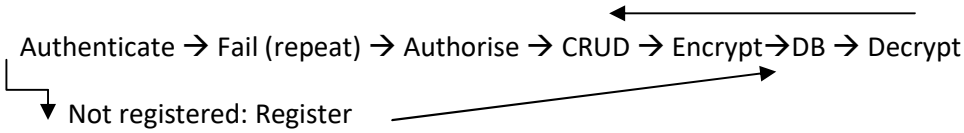
- Design
- Code – Style & Language Selection
- Testing

➔ Most important is the Design. Every Language can be more or less secure based of the structure and design. But Python has some approaches which increase the security like the way it handles with strings. Testing is important and can improve the security drastically, but just testing in the end arises to huge problems in terms of effectiveness.

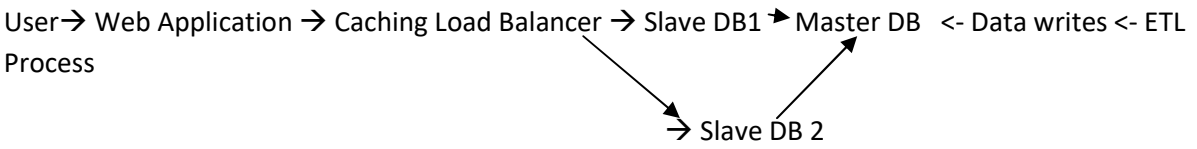
Design Review:

- What will your App do? –Authorisation and Authentication are the kernel aspects beside of storing and CRUD functions.
- What effect will the different customer profile (CERN, Dutch Police, ISS) have? – Amount of data traffic, structure of organisation, design of web interface
- What kind of App is it? (Arch Design)
- Planning:
- Brooks' rule of thumb for estimating the completion time of software projects:
- → 1/3 time for planning
- → 1/6 time for coding
- → 1/4 time for component tests
- → 1/4 time for system test with all components in hand

Outline Approach:



N-tier – Example Diagram for Course Text



- Functionality Separated into tiers
- May be physical partitions or not
- Firewalls may segregate tiers
- Common tiers include presentation, business and data
- E.g. operational data stores

MVC – Model-View-Controller (aka MVT – model-view-template)

Model → updates → View → sees → User → uses → Controller → manipulates

- Evolved from Smalltalk
- Used in Web frameworks – Rails & Django
- Model = data/database
- Controller = app/business logic
- View = presentation layer
- Django calls controllers ‘views’ and views ‘templates’ – somewhat confusing

➔ This approach allows to separate the task in the team. The downside however is to get an understanding with Django.

Code integration possibilities: Classes - CLI, MVC - Django, Flask

Next Seminar:

- Sharma, A. & Bawa, R.K. (2020) Identification and Integration of Security Activities for Secure Agile Development. International Journal of Information Technology.
- Some say that people are the biggest risk for cyber security.
- Select five terms from ISO/IEC Standard 27000 Section 3 Terms and Definitions and write a 300 – word blog post on how people can manage to overcome cyber security attacks from the inside.