Seminar 1 Notes

* Use academic referencing in blog post.
* Recommended preparing ePortfolio now.

**Weakness of security in Waterfall**

* Security provisioned at a single point in the development cycle
  + May not accommodate all the needs of the development team has

**Weakness of security in Agile**

* May not know all the requirements at the beginning
  + Don’t have a complete perspective of what we need in terms of security

**OWASP Proactive Controls**

* C1: Define security requirements
* C2: Leverage security frameworks and libraries
* C3 Secure database access
* C4: Encode and escape data
* C5: Validate all inputs
* C6: Implement digital identity
* C7: Enforce access controls
* C8: Protect data everywhere
* C9: Implement security logging and monitoring
* C10: Hanle all errors and exceptions

**Design document Assignment**

* Say these are the vulnerabilities within the system and these are the approaches that we’re going to use to protect against those vulnerabilities being exploited (OWASP Proactive Controls)
* What are you going to do with monitoring information?
* UML diagrams can go in appendix or main body of design document to support design

**Security in Agile Lifecycle**

* Sec Dev Checklist
* Training
* Data Flow Diagram
* Threat Modelling
* Security Architecture Review
* Code Analysis
* Dependency Analysis
* Dynamic Security Test
* Pen Testing
* Vulnerability management and patching
* Security User stories

**Peer review guidance**

* Give your peers something to think about for the summary post

**UML advice**

* Use swimlanes
* Misuse cases gives attention to hacker

**Blog post**

* Psychology profiles of people who attack
  + Demographic
  + Late teens male high intelligence with some personal issues
* Personality tests to get a job
* Personality traits to interact with people
* Training
* Social Engineering targeting the vulnerable
* Do you have a single administrator or multiple people (single point of failure)
* Work factor by sulture and Schroeder
  + Have lots of additional layers of security
* Human Error
* Access Management
* Risk Assessment
* Competency checks
* Policies