

Seminar 1: Scrum Security review

Please carry out these activities before joining the seminar this week. Your answers will be discussed during the seminar.

Question 1

Create a 2-column multi-line table. In the left-hand column, include the software development stages of the Scrum agile life cycle approach to project management. In the right-hand column, describe the processes which you recommend are applied at each stage to ensure that secure software is produced at the end of the development. To support the preparation of your response, you can refer to the following literature:

Sharma, A. & Bawa, R. K. (2020) Identification and Integration of Security Activities for Secure Agile Development. *International Journal of Information Technology*.

SCRUM Step	Recommended Process
Pre requirement	Initial education <ul style="list-style-type: none"> • allows for understanding of system requirements • Can prep possible security weaknesses linked to reqs
Requirement phase	Agree on definitions and role matrix <ul style="list-style-type: none"> • Agreement on defs is crucial for agile teamwork/security development • Access control and authentication among the various roles required is an essential security element
Design	Security architecture and requirements inspection <ul style="list-style-type: none"> • Code with security in mind, though not all at once – this would be an iterative process • Requirements are also iterative, should therefore we checked along with sec architecture
Implementation	Follow coding rules, use security tools, conduct a static code analysis <ul style="list-style-type: none"> • Coding rules help reduce possible errors or weaknesses • security tools can help parse code errors/reinforce code security

	<ul style="list-style-type: none">• code analysis allows for faster bug/weakness detection
Testing	Dynamic analysis and penetration testing <ul style="list-style-type: none">• Dynamic analysis better reflects real-world code (mis)usage• Penetration testing can document bugs/weaknesses missed by initial testing
Release	Signing the code, incident response planning, and final security review <ul style="list-style-type: none">• Signing code adds to the level of validity of the product's security• incidents will happen – better to have a plan and look prepared than be caught out with a zero-day• final reviews make everything nice and neat