

Course Descriptor

Last Edition: 5 May 2020	Version No. 20.2
---------------------------------	-------------------------

1. Course Title:	Software Quality											
2. Course Code:	INFSWQ01-A INFSWQ21-A											
3. Course Team:	Babak Basharirad Ahmad Omar											
4. Rationale and Synopsis:	Quantity and importance of data entrusted to web applications is growing, and programmers need to learn how to secure them. Traditional network defences, such as firewalls, fail to secure web applications. This course introduces some of these potential risks and helps students to better understand web application vulnerabilities, thus enabling them to properly defend organizations web assets.											
5. Year and OP offered:	Year 2 / OP 4											
6. Prerequisite:	Web											
7. Credit Value:	4 EC											
8. Student Learning Time (SLT) [hours]												
L = Lecture T = Tutorial P = Practical V = Virtual Learning A = Assessment O = Other	Face to Face						Guided Learning	Ind. Learning	Total Learning Time			
	L	T	P	V	A	O	Total					
	21			-	-	-	21	91	112			
9. Learning outcomes:	<p>On completion of this module, students will be able to:</p> <ol style="list-style-type: none"> 1) Understand web application security and its importance. 2) Understand common mistakes of coders and vulnerabilities of web applications. 3) Explain how code developers' mistakes may be exploited to the benefit of the attackers and how to prevent these attacks. 4) Build secure web applications using secure coding practices. 											
10. Assessment:												
	Learning Outcomes for Assessment											
Final Exam	<input checked="" type="checkbox"/>	100 % (Final Grade)			LO 1	<input checked="" type="checkbox"/>	LO 2	<input checked="" type="checkbox"/>	LO 3	<input checked="" type="checkbox"/>	LO 4	<input checked="" type="checkbox"/>
Assignment	<input checked="" type="checkbox"/>	Pass/Fail			LO 1	<input type="checkbox"/>	LO 2	<input checked="" type="checkbox"/>	LO 3	<input checked="" type="checkbox"/>	LO 4	<input checked="" type="checkbox"/>

11. Content of the module and the SLT per topic [hours]:			
Week	Topics	Class	Ind.
1	Introduction <ul style="list-style-type: none"> ▪ HTTP <ul style="list-style-type: none"> - Requests and Responses - Referer Header - Caching - Cookies ▪ Sessions <ul style="list-style-type: none"> - Session hijacking ▪ HTTPs 	3	13
2	Passing Data to Subsystems <ul style="list-style-type: none"> ▪ Introduction to Subsystems and Metacharacters ▪ SQL Injection <ul style="list-style-type: none"> - Avoiding SQL injection ▪ Shell Command Injection <ul style="list-style-type: none"> - Avoiding shell command injection 	3	7
3	User Input <ul style="list-style-type: none"> ▪ Introduction to Input <ul style="list-style-type: none"> - User-generated Input - Server-generated Input ▪ Input Validation ▪ Handling Invalid Input 	3	7
4	Output Handling: The Cross-site Scripting Problem <ul style="list-style-type: none"> ▪ Introduction to Cross-Site Scripting (XSS) <ul style="list-style-type: none"> - XSS-based Session Hijacking - Text Modification ▪ The Problem ▪ The Solution 	3	7
5	Web Trojans <ul style="list-style-type: none"> ▪ Introduction ▪ The Problem ▪ The Solution 	3	7
6	Review and Exam Tips	3	7
7	Review and Exam Tips	3	7
Total SLT (hours)		21	56

12.	References and Supporting Materials: Main Reference(s): 1. Title: Innocent Code: A Security Wake-Up Call for Web Programmers 1st Edition Author(s): Sverre H. Huseby Pub. Year: 2004 Additional Reference(s): 1. Title: Web Application Security, A Beginner's Guide. Author(s): Bryan Sullivan, Vincent Liu Pub. Year: 2011 2. Title: Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast Author(s): Paco Hope, Ben Walther Pub. Year: 2008
------------	--