Rotterdam University of Applied Sciences

School of Communication, Media and Information Technology

Course Descriptor

Last Edition:	12 February 2019	**Version No.**	20.2

1.	**Course Title:**	Web Application Security (WAS)
2.	**Course Code:**	INFANL01-9
3.	**Course Team:**	Babak Basharirad Jannes Bloemendal 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 Semester offered:**	Year 2 / Sem 1
6.	**Prerequisite:**	Introduction to Web Programming
7.	**Credit Value:**	3 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			-	3	-	24	56	80

9. Learning outcomes:

On completion of this module, students will be able to:

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			
Class Test	☐	- %	LO 1 ☐	LO 2 ☐	LO 3 ☐	LO 4 ☐
Final Exam	☒	100 %	LO 1 ☒	LO 2 ☒	LO 3 ☒	LO 4 ☒
Assignment	☐	- %	LO 1 ☐	LO 2 ☐	LO 3 ☐	LO 4 ☐

* regardless of assessment type, students need to obtain 50% of marks for each LO to successfully pass the module.

11. Content of the module and the SLT per topic [hours]**:**

Week	Topics	Class	Ind.
1	**Introduction** ▪ HTTP – Requests and Responses – Referer Header – Caching – Cookies ▪ Sessions – Session hijacking ▪ HTTPs	**3**	**7**
2	**Passing Data to Subsystems** ▪ Introduction to Subsystems and Metacharacters ▪ SQL Injection – Avoiding SQL injection ▪ Shell Command Injection – Avoiding shell command injection	**3**	**7**
3	**User Input** ▪ Introduction to Input – User-generated Input – Server-generated Input ▪ Input Validation ▪ Handling Invalid Input	**3**	**7**
4	**Output Handling: The Cross-site Scripting Problem** ▪ Introduction to Cross-Site Scripting (XSS) – XSS-based Session Hijacking – Text Modification ▪ The Problem ▪ The Solution	**3**	**7**
5	**Web Trojans** ▪ Introduction ▪ The Problem ▪ The Solution	**3**	**7**
6	**Review and Exam Tips**	**3**	**7**
7	**Review and Exam Tips**	**3**	**7**
8	**Exam and Assignment Submission** ▪ Written Exam	**3**	**7**
Total SLT (hours)		**24**	**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 Security Testing Cookbook: Systematic Techniques to Find Problems Fast **Author(s):** Paco Hope, Ben Walther **Pub. Year:** 2008
	2. Title: The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws **Author(s):** Dafydd Stuttard, Marcus Pinto **Pub. Year:** 2011