

CCY4104 Web Security**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY2001 & CCS2305	4	7/8	2	--	2	3

COURSE AIM

To get the students to:

- Understand The fundamentals of web and browser security
- Know the guidelines for building secure web applications.
- Understand the security aspects of the web technologies
- Explore web vulnerabilities, web browser design flaws, and some advanced web privacy topics.

COURSE WEEKLY CONTENTS

- 1 Course Aim, Course outline, and introduction to web security
- 2 How the Internet works
- 3 How browsers work, HTTPS and its limitations
- 4 What are the latest emerging attacks facing the Internet?
- 5 Static and dynamic resources and tools critical in solving common web vulnerabilities.
- 6 7th week Assessment
- 7 Same origin policy and web attacker model. Injection flaws and Cross-site scripting
- 8 Injection Flaws (II): XSS (contd.), SQL Injection, OS Command Injection, HTTP Header Injection
- 9 Authentication flaws and request authentication flaws
- 10 Insecure Web Logic: Logic Flaws, HTTP Pollution, HTTP Parameter Tampering
- 11 Cookie Flaws and Server Misconfiguration
- 12 12th week Assessment
- 13 Attacks on User Interfaces
- 14 New web security defence techniques.
- 15 Projects Presentations

STUDENT GRADING & ASSESSMENT

Weeks	Exams	Assign.	Quizzes	Reports	Present.	Lab.	Total
1 to 7	←		3 0	M A R K S		→	30
8 to 12	←		2 0	M A R K S		→	20
1 to 15	←		1 0	M A R K S		→	10
16 or 17	Final Exam						40

REFERENCES

Textbook	Malcolm McDonald, Web Security for Developers, No Starch Press
----------	--