Application Development and Security
APDS7311/w
MODULE OUTLINE 2024
(First Edition: 2019)

The Independent Institute of Education (Pty) Ltd is registered with the Department of Higher Education and Training as a private higher education institution under the Higher Education Act, 1997 (reg. no. 2007/HE07/002). Company registration number: 1987/004754/07.

Table of Contents

Introduction

Welcome to the module Application Development and Security. The greatest challenge we face today is hacking and cybercrime. Software does not know that the data it is processing over the Internet is sensitive. Hence, it is important that applications developed be designed on the sensitivity and confidentiality of the data they are processing. Recent inclinations show that a multi-factor authentication method enables safer authentication, authorisation, and protection of data in storage. This module aims to helps you understand the most common threats against web applications today and learn a wide variety of security techniques to help you build web applications that prevent these attacks from being successful.

Using this Module Outline

This module outline has been developed to **support your learning**. Please note that the content of this module is on Learn as well as in the prescribed material. You will not succeed in this module if you focus on this document alone.

- This document does not reflect all the content on Learn, the links to different resources, nor the specific instructions for the group and individual activities.
- Your lecturer will decide when activities are available/open for submission and when these submissions or contributions are due. Ensure that you take note of announcements made during lectures and/or posted within Learn in this regard.

This Module on Learn

Learn is an online space, designed to support and maximise your learning in an active manner. Its main purpose is to **guide and pace** you through the module. In addition to the information provided in this document, you will find the following when you access Learn:

- A list of prescribed material;
- A variety of additional online resources (articles, videos, audio, interactive graphics, etc.) in each learning unit that will further help to explain theoretical concepts;
- Critical questions to guide you through the module's objectives;
- Collaborative and individual activities (all of which are gradable) with time-on-task estimates to assist you in managing your time around these;
- Revision questions, or references to revision questions, after each learning unit.

Kindly note:

- Unless you are completing this as a distance module, Learn does **not** replace your contact time with your lecturers and/or tutors.
- APDS7311 is a Learn module, and as such, you are required to engage extensively with the content on the Learn platform. Effective use of this tool will provide you with opportunities to discuss, debate, and consolidate your understanding of the content presented in this module.
- You are expected to work through the learning units on Learn in your own time – especially before class. Any contact sessions will therefore be used to raise and address any questions or interesting points with your lecturer, and **not** to cover every aspect of this module.
- Your lecturer will communicate **submission dates** for specific activities in class and/or on Learn.

Icons Used in this Document and on Learn

The following icons are used in all your modules on Learn:

Icon	Description
Objectives	A list of what you should be able to do after working through the learning unit.
Prescribed Work	Specific references to sections in the prescribed work.
ThinkAbout	Questions to help you recognise or think about theoretical concepts to be covered.
Active Learning	Sections where you get to grapple with the content/ theory. This is mainly presented in the form of questions which focus your attention and are aimed at helping you to understand the content better. You will be presented with online resources to work through (in addition to the textbook or manual references) and find some of the answers to the questions posed.
Connect the dots	Opportunities to make connections between different chunks of theory in the module or to real life.
That is life!	Real life or world of work information or examples of application of theory, using online resources for self-exploration.

REMEMBER:

You need to log onto Learn to:

- Access online resources such as articles, interactive graphics, explanations, video clips, etc. which will assist you in mastering the content; and
- View instructions and submit or post your contributions to individual or group activities which are managed and tracked on Learn.

Module Resources	
Prescribed Material (PM) for this Module	• *Ma*nico, J. and Detlefsen, A. 2015. *Iron-Clad Java: Building Secure Web Applications* ISBN: 978-0-07-183589-3 • IIE Lab Guide
Recommended Readings, Digital and Web Resources	Please note that a number of additional resources and links to resources are provided throughout this module on the Learn platform and YouTube. You are encouraged to engage with these, as they will assist you in mastering the various objectives of this module. They may also be useful resources for completing any assignments. You will not, however, be assessed under examination conditions on any additional or recommended reading material. LU1 – https://www.youtube.com/playlist?list=PL480DYS-b_kfJ7MT686huYMim_TDLdmEe LU2 – https://www.youtube.com/playlist?list=PL480DYS-b_keOuyyhkQ0H9duso5Qb7J8Z LU3 – https://www.youtube.com/playlist?list=PL480DYS-b_kf4CQNnFg4ei87DuIcnSmX6 LU4 - https://www.youtube.com/playlist?list=PL480DYS-b_keCxFKiFtfwwXwA-i9nkROC LU5 – https://www.youtube.com/playlist?list=PL480DYS-b_kemSMc2KaD2eWhhHpqqYfBs LU6 – https://www.youtube.com/playlist?list=PL480DYS-b_ke_APxXgB-0FKPrlUHwEXtf LU7 – https://www.youtube.com/playlist?list=PL480DYS-b_kf4CRUsWjpjhmSRVxVTFMzl LU8 – https://www.youtube.com/playlist?list=PL480DYS-b_kcXNkaKQcFv_hsxbbM8Ebu0 LU9 – https://www.youtube.com/playlist?list=PL480DYS-b_kdoELASDjF_paSsE1k-4D8U
Module Overview	You will find an overview of this module on Learn under the *Module Information* link in the Course Menu.
Assessments	Find more information on this module's assessments in this document and on the Student Portal.

Module Purpose
The purpose of this module is to provide you with a solid grounding in web application security. It covers authentication and authorisation, session management, as well as database and file security. Vulnerability detection and secure development are important focus of this module.

Module Outcomes	
MO1	Demonstrate familiarity with compliance and operational security.
MO2	Identify threats and vulnerabilities in programming code.
MO3	Create applications that adhere to application security requirements and regimen.
MO4	Apply access control and identity management to software systems.

Assessments

Integrated Curriculum Engagement (ICE)	
Minimum number of ICE activities to complete	4
Weighting towards the final module mark	10%

Formatives	Part 1	Part 2
Total marks	100	100
Weighting	25%	30%
Duration	10 hours	12 hours
Learning Units covered	LU1–2	LU1–4

Summative	Portfolio of Evidence (POE)
Weighting	35%
Duration	15 hours
Total marks	100
Learning Units covered	All

Assessment Preparation Guidelines	
Format of the Assessment	Preparation Hints
Part 1	
This assessment will assess your understanding of Learning Unit 1 to 2.	• Ensure that you work through all the relevant activities, exercises, and revision questions on Learn and in your textbook. • Pay attention to the instructions and to the mark allocations of each question to ensure that you can meet the requirements. • Make sure that you have mastered the objectives in Learning Units 1 to 4.
Part 2	
The assessment will assess your ability to integrate and apply the content in Learning Units 1 to 4.	• Read through the prescribed chapters and content for Learning Units 1 to 3 and ensure that you have engaged before you proceed with your coding. • Remember to analyse all elements required and ensure that your task meets the requirements. • Improve the quality of your task by using the provided rubric and addressing any areas of concern prior to submitting it for marking.
Portfolio of Evidence (PoE)	
The PoE will consist of Task 1, Task 2, and further activities to complete the PoE. All learning units will be assessed in the PoE and reflections on your learning will be included.	• Ensure that you work through all the activities, exercises, and revision questions on Learn and consult your textbook. • Include the tasks as submitted, together with your lecturer's feedback and your corrected tasks based on the feedback received. • Include the reflection of your learning. • Complete other activities included in the PoE.

Module Pacer

Code	Programme	Contact Sessions	Credits
APDS7311	ADA1, BCA3; BCIS3	52	15
APDS7311w	ADA1w	12	
Learning Unit 1	Introduction to Web Application Security		

Overview:

In this chapter, you learn about the inner workings of the HTTP protocol, the use of intercepting proxies to tamper with requests, and review a variety of HTTP security response headers. You will be introduced to security fundamentals. It begins by examining the current challenges in web application security and why they are so difficult to achieve. It then describes information security in more detail to illustrate why it is important. Please work through all the themes on Learn, together with the relevant sections of your prescribed source/s.

Please work through all the themes on Learn, together with the relevant sections of your prescribed source/s.

Learning Unit 1: Theme Breakdown		
Sessions: **1-2**	**Theme 1:** HTTP Security Considerations	**Prescribed Material (PM)**
Related Outcomes: MO001	• Motivate the importance of proxy server settings; • Discuss the threat of untrusted data; • Explain how HTTP drives web traffic.	PM1: Chapter 1
	Theme 2: Anti-Patterns and Positive Patterns	PM2: Chapter 1

	• Distinguish between the most common anti-patterns with reference to:
	  ○ Blacklist Input Validation;
	  ○ Lack of parameterized SQL;
	• Discuss security controls and the variety of positive defensive patterns;
	• Explain input validation as a programming technique.	

Learning Unit 2	Authentication and Session Management

Overview:

In this learning unit, we explore the security controls needed to build a complete secure login application. We learn techniques on how to stop attacks, such as brute force, username harvesting, and session theft.

Please work through all the themes on Learn, together with the relevant sections of your prescribed source/s.

Learning Unit 2: Theme Breakdown		
Sessions: 3-7	Theme 1: The Login Process	Prescribed Material (PM)
Related Outcomes: MO001 MO002	• Discuss the importance of the new registration requirements. • Discuss the nine steps of the login workflow,	PM: Chapter 2
	Theme 2: Attacks Against Authentication	PM: Chapter 2
	• Discuss the various ways of defence against authentication layer attacks. • Explain the significant risks of session hijacking and session fixation.	
	Theme 3: Cookies and Credential Security	PM: Chapter 2
	• Explain the dangers of storing sensitive data in cookies.	
	• Defend the importance of credential security.	PM: Chapter 2
	Theme 4: Multi-factor Authentication	
	• Explain the roles of multi-factor authentication.	PM Chapter 2:

Learning Unit 3	Identity and Access Control

Overview:

Access control, or authorisation, is the process of limiting users to access only the functionality and data that they are specifically permitted to use. In this learning unit, we explore application-specific access control that you, as a developer, need to build within your Java web applications. Even in a simple web application, access control appears at many layers.

Please work through all the themes and activities on Learn, together with the relevant sections of your prescribed source/s.

Learning Unit 3: Theme Breakdown		
Sessions: 8-10	Theme 1: Identity and Access Control	Prescribed Material (PM)
	• Apply different authorisation, authentication, and access control; • Explain the role of the core components of access. • Differentiate between vertical privilege escalation and horizontal privilege escalation.	PM: Chapter 3
Related Outcomes: MO002 MO003	Theme 2 Contextual Access Control	PM: Chapter 3

	• Explain how access control anti-patterns result in Design Flaws.
	• Discuss guiding principles to include positive access control patterns in access control mechanism.
	• Contrast RBAC and ABAC with regards to:
	  ○ implementation;
	  ○ functionalities;
	  ○ limitations;
	  ○ access control.
	• Explain how access control anti-patterns result in Design Flaws;
	• Discuss guiding principles to include positive access control patterns in access control mechanism.	

Learning Unit 4	Cross-Site Scripting Defense

Overview:

In this learning unit, you learn about cross-site scripting and how to use contextual output encoding when building user interface code. You also learn about HTML sanitisation techniques, safe use of JSON, and proper JavaScript usage for security.

Please work through all the themes and activities on Learn, together with the relevant sections of your prescribed source/s.

Learning Unit 4: Theme Breakdown		
Sessions: 11-20	Theme 1: Content Spoofing	Prescribed Material (PM)
	• Differentiate between content spoofing and reflected XSS.	PM: Chapter 4
Related Outcomes: MO002	Theme 2: Defending Against XSS	PM: Chapter 4

	• Discuss the factors to consider when choosing a defence strategy against XSS.
	• Motivate the use of:
	  ○ input validation;
	  ○ contextual output encoding;
	  ○ html validation and sanitisation;
	  ○ Secure JSON patterns.	

Learning Unit 5	Cross-Site Request Forgery Defense and Clickjacking

Overview:

This learning unit focuses on Cross-Site Request Forgery (CSRF) attacks that, as the name implies, trick the browser into making unauthorised requests on the victim's behalf, often without the victim's knowledge. This vulnerability is also called "session riding" because it often takes advantage of a legitimate user's existing authenticated session on the vulnerable site. We will first investigate the threats presented by cross-site request forgery and the techniques to combat it. In Theme 2, we will explore the main X-Frame-Options choices used to combat clickjacking.

Please work through all the themes and activities on Learn, together with the relevant sections of your prescribed source/s.

Learning Unit 5: Theme Breakdown		
Sessions: 21-25	Theme 1: How does Cross-Site Request Forgery work?	Prescribed Material (PM)
	• Explain the threats presented by cross-site request forgery with reference to suitable examples.	PM: Chapter 5
Related Outcomes: MO002 MO003	Theme 2: How to combat Cross-Site Request Forgery	PM: Chapter 5
	• Discuss the various techniques to combat cross-site request forgery.	
	Theme 3: Clickjacking	PM: Chapter 5
	• Distinguish between the main X-Frame-Options choices used to combat click jacking.	

Learning Unit 6	Protecting Sensitive Data

Overview:

In this learning unit, we cover techniques to keep data safe. Card numbers, ID numbers, and passwords are all sensitive information. Whether you are writing the data to a file, storing it in a database, or sending it across the network, your code needs to keep the information secure. You learn about ways in which cryptography can be used to protect data using different types of cryptography algorithms to encrypt and decrypt data. We will then examine cryptographic attacks in greater detail, as well as the use of digital certificates along with public key infrastructure to keep data secure on files and disks. We will end the unit with a look at the roles of different transport cryptographic algorithms and protocols in the security of transmitted data.

Learning Unit 6: Theme Breakdown		
Sessions: 26-30	Theme 1: Securing Data in Transit	Prescribed Material (PM)
Related Outcomes: MO003 MO004	• Discuss the general rules to protect against network-based threats; • Explain the steps necessary when using certificate chains; • Motivate the necessity for customised trust managers; • Discuss the role of protocol versions.	PM: Chapter 6
	Theme 2: Securing Data at Rest	PM: Chapter 6
	• Differentiate between various categories of cryptographic algorithms; • Explain how keysets are created and managed with KeyczarTool; • Explain the role of secure random numbers in security operations; • Identify capabilities for generating cryptographic random numbers.	

Learning Unit 7	SQL Injection Attacks

Overview:

In this learning unit, you learn to use query parameterisation and variable binding in order to prevent SQL injection. You will also learn how to protect stored procedures against SQL injection and implement configuration measures that can be taken to reduce the impact of SQL injection.

Please work through all the themes and activities on Learn, together with the relevant sections of your prescribed source/s.

Learning Unit 7: Theme Breakdown		
Sessions: 31-37	Theme 1: SQL Injection	Prescribed Material (PM)
Related Outcomes: MO002 MO003 MO004	• Explain the danger of SQL injection; • Defend the importance of query parameterization as an important technique to build secure websites; • Explain how to protect stored procedures against SQL injection.	PM: Chapter 7
	• Discuss configuration measures that can be taken to reduce the impact of SQL injection.	PM: Chapter 7

Learning Unit 8	Safe File Upload and File Input-Output

Overview:

In this learning unit, we will look at the ways in which they do so, focusing on attacks that target web-based servers and the applications that run on those devices. We will begin with a look at the roles of malware and learn techniques to safely perform file I/O operations in your application. You also learn how to build a secure file upload mechanism.

Please work through all the themes and activities on Learn, together with the relevant sections of your prescribed source/s.

Learning Unit 8: Theme Breakdown		
Sessions: 38-42	Theme 1: Anti-Patterns and Design Flaws	Prescribed Material (PM)
Related Outcomes: MO002 MO003 MO004	• Discuss design flaws to avoid for secure file handling; • Explain what is involved in building a secure file upload mechanism for web applications.	PM: Chapter 8
	Theme 2: Patterns of Attack	
	• Describe the necessary steps to safely upload files in an application.	PM: Chapter 8

Learning Unit 9	Logging, Error Handling, and Intrusion Detection

Overview:

In this learning unit, you learn how to use several third-party Java libraries for security-centric logging. We also review how to keep your code from revealing too much when errors occur. In addition, you learn several easy intrusion detection techniques to help alert you the moment your application is under attack.

Please work through all the themes and activities on Learn, together with the relevant sections of your prescribed source/s.

Learning Unit 9: Logging, Error Handling, and Intrusion Detection		
Sessions: 47-52	Theme 1: Logging and Safe Error Handling	Prescribed Material (PM)
MO003 MO004	• Discuss the requirements for effective logging to support software accountability; • Identify appropriate logging frameworks for security; • Discuss safe error-handling techniques for web applications.	PM: Chapter 9