ITT Technical Institute

CS420

Application Security

Onsite Course

SYLLABUS

Credit hours: 4

Contact/Instructional hours: 50 (30 Theory Hours, 20 Lab Hours)

Prerequisite(s) and/or Corequisite(s):

Prerequisites: CS310 Programming in C++ or equivalent, CS400 Web Services and Applications or equivalent

Course Description:

This course emphasizes the importance of using safe programming practices by giving students a glimpse into the mind of the attacker. Key security technologies, such as cryptography and authentication are also discussed.

Syllabus: Application Security

Instructor:	_____
Office hours:	_____
Class hours:	_____

Course Description

This course emphasizes the importance of using safe programming practices by giving students a glimpse into the mind of the attacker. Key security technologies, such as cryptography and authentication, are also discussed.

Major Instructional Areas

1. The need for software security
2. Protection against security breaches in different applications
3. Methods to assess security vulnerabilities
4. Methods to secure authentication, authorization, and privacy

Course Objectives

1. Discuss the importance of software security goals.
2. Examine how attackers can discover vulnerabilities in software.
3. Develop strategies to mitigate common attack patterns.
4. Perform a threat analysis as part of risk management.
5. Design a secure authentication strategy for software security.
6. Design a secure authorization strategy for software security.
7. Assess the role of cryptography in application security.
8. Evaluate the risks inherent in client-side code.
9. Assess the risks associated with server-side code.
10. Employ steps to mitigate risks specific to web applications and web services.
11. Evaluate the steps to mitigate overflow attacks.

Course Outline

Note: All graded activities, except the Project, are listed below in the pattern of <Unit Number>.<Assignment Number>. For example, Labs: 2.1 refers to the first lab activity in Unit 2.

Unit	Activities

1— Software Security Introduction	• Content Covered:
	• *Application Security*:
	  ○ Chapter 1, "Introduction to Software Security"
	  ○ Chapter 2, "Guiding Principles for Software Security"
	  ○ Chapter 3, "The Web Is Different"
	• Course Project: Start Part 1
	• Labs: Pre-Lab, 1.1
	• Assignments: 1.1

2— Cryptography	• Read from *Application Security*:
	  ○ Chapter 4, "Cryptography Basics"
	  ○ Chapter 5, "Randomness and Determinism"
	• Read from Application Security Learning Packet:
	  ○ Using .NET Framework System.Security.Cryptography classes
	• Quizzes: 2.1
	• Course Project Part 1: Submit
	• Labs: 2.1
	• Assignments: 2.1

3— Authentication	• Read from *Application Security*:
	  ○ Chapter 6, "Password Authentication"
	  ○ Chapter 7, "Authentication"
	• Read from Application Security Learning Packet:
	  ○ Implementing Authentication in a .NET Windows Application
	  ○ Implementing Authentication in an ASP.NET Application
	• Read from *Microsoft SQL Server 2008 for Dummies*
	  ○ Chapter 16, "Protecting Your Data from Prying Eyes"
	• Quizzes: 3.1
	• Course Project Part 2: Submit
	• Labs: 3.1
	• Assignments: 3.1

4— Access Control and Privacy	• Read from *Application Security*:
	  ○ Chapter 8, "Access Control"
	• Read from *How to Break Web Software* PDF:
	  ○ Chapter 9, "Privacy"
	• Read from Application Security Learning Packet:
	  ○ Limiting Code Access
	• Quizzes: 4.1
	• Course Project Part 3: Submit
	• Labs: 4.1
	• Assignments: 4.1

5— Attack Patterns and	• Read from *Application Security*:

Unit	Activities
Auditing Software	○ Chapter 9, “On Open Source and Closed Source” ○ Chapter 10, “Auditing Software” ○ Chapter 11, “Attack Patterns” ○ Chapter 12, “Gathering Information on the Target” • Quizzes: 5.1 • Course Project Part 4: Submit • Labs: 5.1 • Assignments: 5.1
6— Exploiting Server Software	• Read from *Application Security*: ○ Chapter 13, “Exploiting Server Software” • Quizzes: 6.1 • Course Project Part 5: Submit • Labs: 6.1 • Assignments: 6.1
7— Database, Web Services, and Web Server Security	• Read from *Application Security*: ○ Chapter 14, “Database Security” ○ Chapter 15, “Attacking User-Supplied Input Data,” Attack 9, “SQL Injection,” pp. 388-394 ○ Chapter 16, “Attacking the Server” ○ Chapter 17, “Web Services” • Quizzes: 7.1 • Course Project Part 6: Submit • Labs: 7.1 • Assignments: 7.1
8— Client Software	• Read from *Application Security*: ○ Chapter 18, “Exploiting Client Software” ○ Chapter 19, “State-based Attacks” ○ Chapter 15, “Attacking User-Supplied Input Data,” Attack 8, “Cross-Site Scripting” and Attack 10, “Directory Traversal” pp. 380-388 and pp. 394-398 • Quizzes: 8.1 • Course Project Part 7: Submit • Labs: 8.1 • Assignments: 8.1
9— Malicious Input	• Read from *Application Security*: ○ Chapter 20, “Crafting (Malicious) Input” ○ Chapter 21, “Attacking the Client” • Quizzes: 9.1 • Course Project Part 8: Submit • Labs: 9.1 • Assignments: 9.1
10— Buffer Overflows	• Read from *Application Security*: ○ Chapter 22, “Buffer Overflows” • Quizzes: 10.1 • Course Project Part 9: Submit • Labs: 10.1 • Assignments: 10.1
11— Course Review and	• Course Review

Unit	Activities
Final Exam	• Final Exam

Instructional Methods

This course takes a “good guy/bad guy” approach to understanding software security. In other words, to secure software, you must understand both the potential risks and the attack patterns used to exploit software.

This course begins by exploring software security principals and technologies, followed by examining how to analyze software during the design and development phase–just as attackers analyze the software after deployment. The remainder of the course focuses on recognizing specific attack patterns and exploits and mitigating the risk of your software falling victim to those attacks.

The success of the class hinges on active participation through discussion, hands-on labs, and research. You will be given the opportunity to discuss various security issues and to interact with your peers to recognize and define steps to mitigate risk. Homework assignments will consist of paper-based exercises to help you understand software vulnerabilities and the coding practices that can help to avoid those vulnerabilities.

Starting with the first unit, you will also perform targeted hands-on labs. These labs provide practice in using specific technologies and in identifying and correcting security problems in code.

Finally, you will conduct a research project with incremental submissions throughout the course. The final submission will be due in Unit 10. You will be given topics by your Instructor to research the various technologies and to analyze an application’s design to identify potential risks.

Instructional Materials and References

Student Textbook Package

- Viega, J., McGraw, G., Andrews, M., Whittaker, J. A., Hoglund, G., & McGraw, G. (2009). *Application security* w/CD (Custom ed.). Boston, MA: Pearson Custom..

Required Reading Resources

- *Application Security Learning Packet (Provided by your instructor)*
- *How to Break Web Software PDF: Chapter 9, "Privacy," pp. 135-147*

(Download from the ITT Tech Virtual Library> School of Study> School of Information Technology> Recommended Links> CS420 Course Materials> How to Break Web Software CH 9*)*

- Vieira, Robert. *Microsoft SQL Server 2008 for Dummies. Hoboken, NJ; Wiley, 2008.*

(ITT Tech Virtual Library> Ebrary> Chapter 16, "Protecting Your Data from Prying Eyes")

References

Log on to the ITT Tech Virtual Library at http://www.library.itt-tech.edu/ to access online books, journals, and other reference resources selected to support ITT Tech curricula.

Books

You may click "Books" from the Main Menu or use the "Library Catalog" function on the home page to find the following books.

ITT Tech Virtual Library> Main Menu> Books> Ebrary>

- Dorrans, Barry. *Beginning ASP.NET Security*. Hoboken, NJ: Wrox, 2010.
- Howard, Michael, David LeBlanc, and John Viega. *24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them*. Emeryville, CA: McGraw-Hill/Osborne, 2009.
- Manzuik, Steve. Network Security Assessment: From Vulnerability to Patch. Rockland, MA: Syngrass, 2006
- Scambray, Joel. Hacking Exposed Web Applications: Web Application Security Secrets and Solutions. 3rd ed. New York, NY: McGraw-Hill, 2010
- Sethi, Harpreet. *Java Security*. Cincinnati, OH: Premier Press, 2002.

Other References

The following resources can be found **outside** of the ITT Tech Virtual Library.

Websites

- Microsoft Developer Network http://msdn2.microsoft.com
- Oracle Technology Network: Java http://www.oracle.com/technetwork/java/index.html
- US-CERT: United States Computer Emergency Readiness Team

http://www.us-cert.gov

All links to web references are always subject to change without prior notice.

Course Evaluation and Grading

Evaluation Criteria

The final grades will be based on the following categories:

CATEGORY	WEIGHT
Assignments	15%
Labs	25%
Quizzes	20%
Course Project	20%
Final Exam	20%
Total	**100%**

Grade Conversion Table

The final grades will be calculated from the percentages earned in the course, as follows:

A	90–100%	4.0
B+	85–89%	3.5
B	80–84%	3.0
C+	75–79%	2.5
C	70–74%	2.0
D+	65–69%	1.5
D	60–64%	1.0
F	<60%	0.0

(End of Syllabus)