Course Syllabus Part I
CYBR 350 Web, Commerce and Application Security

3 Credit Hours

Course Description

This course explores securing core technologies that support Internet applications and commerce. Processes for creating and administering Internet web sites to ensure proper protections are introduced. The course also addresses security applications on Internet websites and mobile platforms, and introduces basic methods for secure development.

Course Prerequisites

None

Course Objectives

Students who successfully complete this course should be able to:

1. Identify plans to design and implement strong security in e-commerce (electronic commerce) that is also user-friendly.
2. Discuss the principles of defense in depth, least privilege, trust, and communication security.
3. Compare and contrast e-commerce and m-commerce (mobile commerce) secure environmental solutions.
4. Identify techniques to implement adaptive, risk-driven and scalable security infrastructures.
5. Develop e-commerce and m-commerce architectures for high-availability and large transactional capacity
6. Identify weak security in a large-scale, transactional system.

Grading Scale

93 – 100% = A	87 – 89% = B+	77 – 79% = C+	67 – 69% = D+
90 – 92% = A-	83 – 86% = B	73 – 76% = C	63 – 66% = D
	80 – 82% = B-	70 – 72% = C-	60 – 62% = D-
			0 – 59% = F

Topic Outline

I. Internet Era: E-commerce
   a. Basics of commerce online
   b. Digital goods
   c. Payment methods
   d. M-commerce

© 2016 Bellevue University. Unless otherwise noted, the contents of this course, including the text and images and how they are arranged and presented, are owned by Bellevue University and protected by U.S. Copyright law. You may use this course content for your own personal, educational, informational and non-commercial use.

II. Mobile Commerce
a. Hardware
b. Operating systems
c. Stacks
d. Clients
e. Warehousing

III. Important “Ilities” in Web Commerce Security
a. Availability
b. Interoperability
c. Reliability
d. Scalability

IV. E-Commerce Basics
a. Security
b. Risk Management
c. Scalability
d. Security Transactions

V. Building Blocks of Protection
a. Cryptography
b. Access control
c. System Hardening
d. Host and network level security

VI. System Components
a. Authentication
b. Authorization
c. Privacy

VII. Security Troubleshooting
a. Vulnerability assessment
b. Intrusion detection and prevention
c. Scanning tools
d. Penetration testing

VIII. Threats and Attacks
a. Attack trees
b. Spamming
c. Phishing
d. Data harvesting
e. Cross-site scripting

© 2016 Bellevue University. Unless otherwise noted, the contents of this course, including the text and images and how they are arranged and presented, are owned by Bellevue University and protected by U.S. Copyright law. You may use this course content for your own personal, educational, informational and non-commercial use.