IS308
Security Strategies for Web Applications and Social Networking
[Onsite and Online]

Course Description:

This course addresses how the Internet and Web-based applications have transformed the way businesses, organizations, and people communicate. With this transformation came new risks, threats, and vulnerabilities for Web-based applications and the people that use them. This course presents security strategies to mitigate the risk associated with Web applications and social networking.

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

Prerequisites: IT320 WAN Technology and Application or equivalent

Credit hours: 4

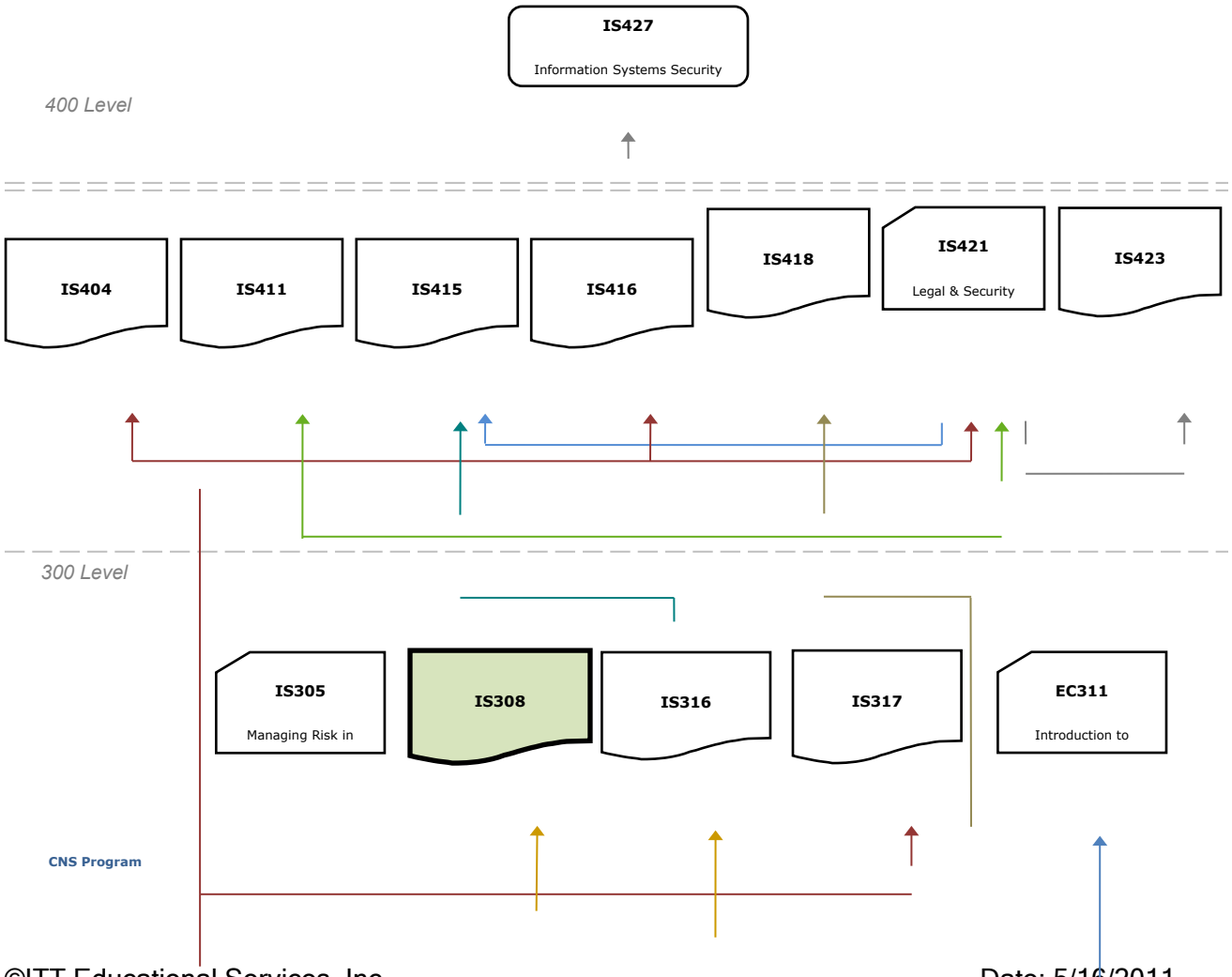
Contact hours: 50 (30 Theory Hours, 20 Lab Hours)

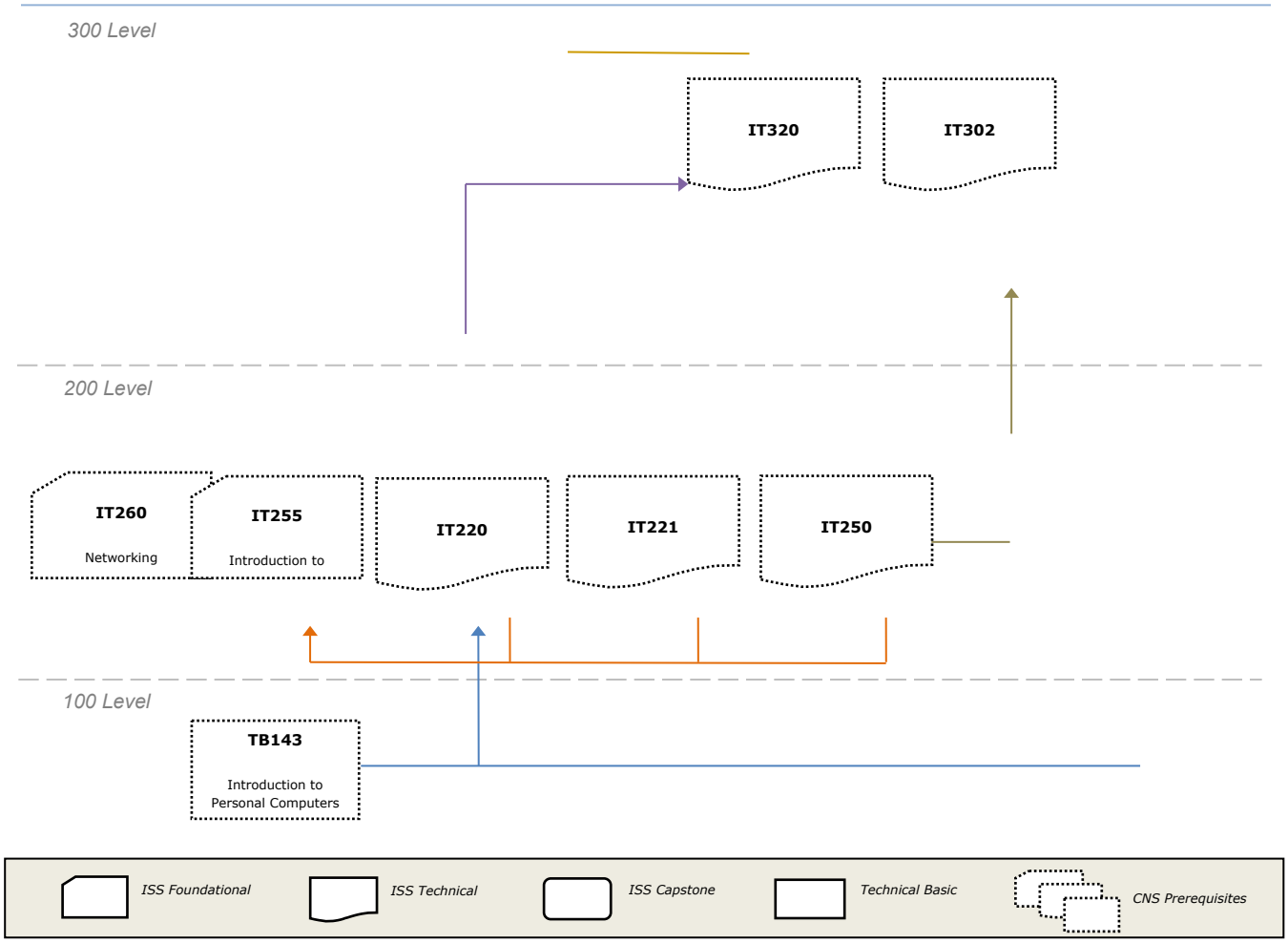
Where Does This Course Belong?

This course is required for the Bachelor of Science in Information Systems Security program. This program covers the following core areas:

- Foundational Courses
- Technical Courses
- BSISS Project

The following diagram demonstrates how this course fits in the program:




300 Level
IT320
IT302
200 Level
IT260
Networking
IT255
Introduction to
IT220
IT221
IT250
100 Level
TB143
Introduction to
Personal Computers
ISS Foundational
ISS Technical
ISS Capstone
Technical Basic
CNS Prerequisites

Course Summary

Major Instructional Areas

1. Internet, Web applications, social media, and social networking in business
2. Web-based risks
3. Secure coding practices
4. Auditing, compliance, and quality assurance for Web applications
5. Web application security

Course Objectives

1. Analyze the impact of the Internet and Web applications on the business world.
2. Analyze the evolution of social media and social networking.
3. Compare and contrast Web-based risks.
4. Analyze common Web site attacks, weaknesses, and security best practices.
5. Describe the attributes and qualities of secure coding practices.
6. Analyze the role and importance of audit and compliance to Web application security.
7. Analyze the role and importance of quality assurance testing for Web applications.
8. Explain the value and importance of vulnerability and security assessments for Web applications.
9. Evaluate next-generation challenges in securing Web applications and data.
10. Construct a comprehensive lifecycle approach to Web application security.

SCANS Objectives

SCANS is an acronym for Secretary's Commission on Achieving Necessary Skills. The committee, appointed by the National Secretary of Labor in 1990, created a list of skills and competencies that

continue to be a valuable resource for individuals developing their careers in a high-tech job market. For more information on the SCANS objectives, visit The U.S. Department of Labor Employment and Training Administration: www.doleta.gov.

Learning Materials and References

Required Resources

Textbook Package	New to this Course	Carried over from Previous Course(s)	Required for Subsequent Course(s)
Harwood, Mike. *Security Strategies in Web Applications and Social Networking.* 1st ed. Sudbury, MA: Jones & Bartlett, 2011.	▪		
Printed IS308 Student Lab Manual	▪		
ISS Mock IT Infrastructure (1) – Cisco Core Backbone Network consisting of Cisco 2811 routers, 2950/2960 catalyst switches, ASA 5505s for classroom hands-on labs that require a live, IP network. (For onsite only)	▪	▪	▪
ISS Mock IT Infrastructure (2) – VM Server Farm (2 Microsoft Windows Servers and 2 Ubuntu Linux Servers) for classroom hands-on VM labs. (For both onsite and online)	▪	▪	▪
ISS Mock IT Infrastructure (2) – VM Workstation (Microsoft Windows XP Professional Workstation with Core ISS Apps and Tools) for classroom hands-on VM labs. (For both onsite and online)	▪	▪	▪

(1) The following presents the core ISS Cisco core backbone network components needed for some of the hands-on labs for onsite delivery only. (Note: video labs will be used for online delivery):

- Cisco 2811 Routers
- Cisco 2950/2960 Catalyst Switches
- Cisco ASA 5505 Security Appliances
- Simulated WAN Infrastructure
- EGP using BGP4 or IGP using EIGRP
- Layer 2 Switching with VLAN Configurations
- Telnet and SSH version 2 for Remote Access
- Inside and Outside VLANs
- DMZ VLAN

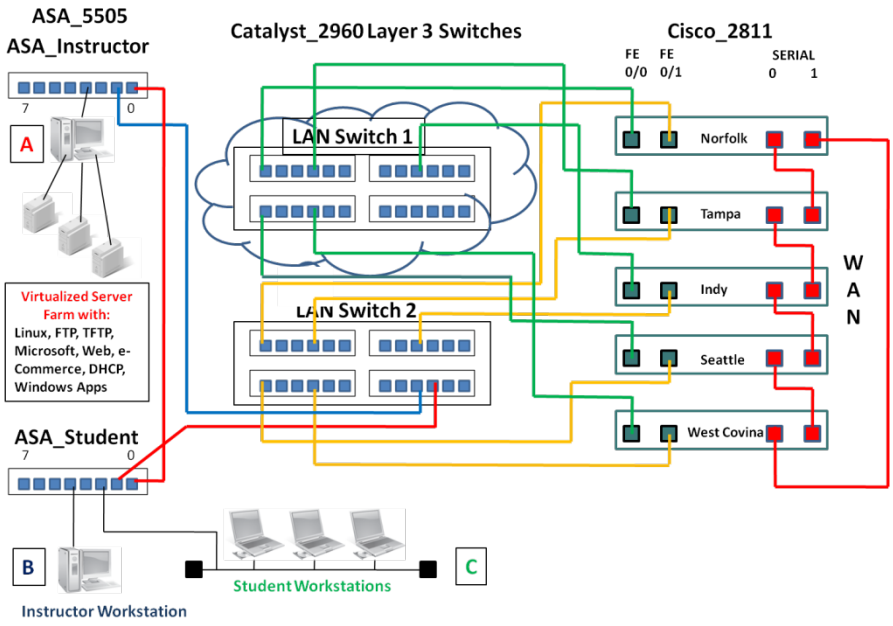


Figure 1 – ISS Cisco Core Backbone Network

(2) The following lists the core ISS VM server farm and VM workstation OS, applications, and tools required for this course for both onsite and online course deliveries:

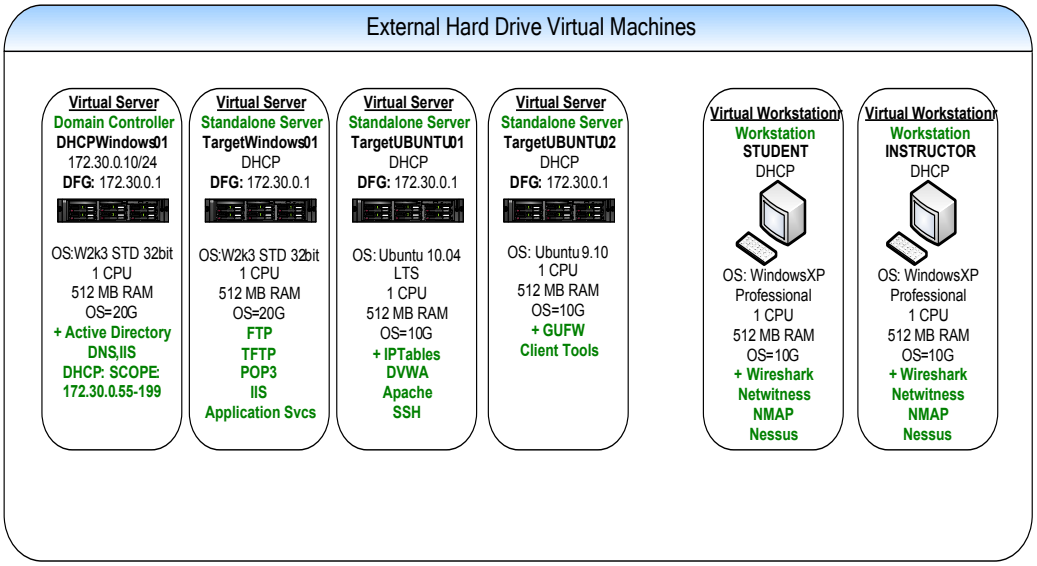


Figure 2 – ISS Core VM Server Farm & VM Workstations

Note #1: ISS onsite students can obtain their removable hard drive directly from their ITT campus. ISS online students will be required to download the core ISS VM server farm and VM workstations directly to their personal computer for installation. The ITT Onsite or Online Instructor will provide students with the specific instructions and procedures for how to obtain the core ISS VM server farm and workstation image files during the first week of class.

(3) The following lists the new VMs, applications, and tools required to perform the hands-on labs for this course for both onsite and online deliveries:

1. New VM for server farm: “VulnerableXP01”. This VM is a vulnerable Microsoft Windows Server 2003 Standard Edition server used for performing attacks.

2. New VM for server farm: “Backtrack01”. A Backtrack 4 Ubuntu Server pre-loaded with the following applications and tools:

a. Metasploit with required plug-ins
b. Kismet
c. Aircrack-ng
d. Airsnort
e. Snort
f. MySQL
g. BASE

3. New VM that Replaces the Old “TargetUbuntu01” VM on the VM server farm. An Ubuntu Server 10.4 VM pre-loaded with the following applications and tools:

a. Damn Vulnerable Web App (DVWA)
b. ClamAV Installed
c. Rootkit Hunter: http://www.rootkit.nl/projects/rootkit_hunter.html
d. Chrootkit: http://www.chkrootkit.org/
e. Appropriate rootkit tools can be found at:

   http://www.packetstormsecurity.org/UNIX/penetration/rootkits/indexdate.html

f. Infected with EICAR
g. tcpdump
h. Common Linux tools such as strings, sed and grep

4. Tools Directory: A directory called "tools" which contains the binary installation files for each tool covered in the course, including:

a. Infected with EICAR
b. ClamAV Installed
c. Rootkit Hunter: http://www.rootkit.nl/projects/rootkit_hunter.html
d. Chrootkit: http://www.chkrootkit.org/

e. Appropriate rootkit tools can be found at: http://www.packetstormsecurity.org/UNIX/penetration/rootkits/indexdate.html

f. Wireshark

g. Netwitness Investigator

h. FileZilla FTP client/Server

i. Putty SSH client

j. Nessus®[1]

[1] Nessus® is a Registered Trademark of Tenable Network Security, Inc.

k. Zenmap

l. MD5sum

m. SHA1sum

n. GnuPG (Gnu Privacy Guard)

o. OpenSSL

p. VMware Player

Note #2: Installation instructions for installing these new VMs, applications and tools will be provided by the ISS onsite or online Instructor during day 1/ week 1 of the course.

Recommended Resources

Books, Professional Journals

Please use the following author's names, book/article titles and/or keywords to search in the ITT Tech Virtual Library for supplementary information to augment your learning in this subject:

Books

Books24X7

Ebrary

Periodicals

ProQuest Computing

- Michael Cross

  Developer's Guide to Web Application Security

- Steven Splaine

  Testing Web Security: Assessing the Security of Web Sites and Applications

Professional Associations

- WASC

  Web site of the Web Application Security Consortium, which is an international, non-profit group that produces open source and best-practice standards for the Web.
  http://www.webappsec.org/

- ISACA

  This Web site provides access to original research, practical education, career-enhancing certifications, industry-leading standards, and best practices. It also provides a network of like-minded colleagues and contains professional resources and technical/managerial publications.

  http://www.isaca.org/

- The RMA Journal

  The official publication of the Risk Management Association

  http://www.rmahq.org/RMA/RMAUniverse/ProductsandServices/RMABookstore/RMAJournal/

Other References

- OWASP

The Website of the Open Web Application Security Project with techniques to build, design, and test the security of Web applications and Web services.
http://www.owasp.org/

NOTE: All links are subject to change without prior notice.

Keywords:

Internet Applications

Web Applications

Brick-and-Mortar

E-Business

E-Commerce

Internet Risks

Web Risks

Web Application Risks

Social Media

Social Networking

Web 2.0

Web Privacy

Business Communications

Internet Marketing

Secure Coding

WASC

Web Audit

PCI DSS

Quality Assurance Testing

Security Assessment

Web Application Security

Course Plan

Instructional Methods

This course is designed to promote learner-centered activities and support the development of cognitive strategies and competencies necessary for effective task performance and critical problem solving. The course utilizes individual and group learning activities, performance-driven assignments, problem-based cases, projects, and discussions. These methods focus on building engaging learning experiences conducive to development of critical knowledge and skills that can be effectively applied in professional contexts.

Suggested Learning Approach

In this course, you will be studying individually and within a group of your peers. As you work on the course deliverables, you are encouraged to share ideas with your peers and instructor, work collaboratively on projects and team assignments, raise critical questions, and provide constructive feedback.

Use the following advice to receive maximum learning benefits from your participation in this course:

DO	DON'T

- Do take a proactive learning approach
- Do share your thoughts on critical issues and potential problem solutions
- Do plan your course work in advance
- Do explore a variety of learning resources in addition to the textbook
- Do offer relevant examples from your experience
- Do make an effort to understand different points of view
- Do connect concepts explored in this course to real-life professional situations and your own experiences

- Don't assume there is only one correct answer to a question
- Don't be afraid to share your perspective on the issues analyzed in the course
- Don't be negative towards the points of view that are different from yours
- Don't underestimate the impact of collaboration on your learning
- Don't limit your course experience to reading the textbook
- Don't postpone your work on the course deliverables – work on small assignment components every day

Course Outline

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
1	Business Evolution and the Internet	*Security Strategies in Web Applications and Social Networking:* ▪ Chapter 1 ▪ Chapter 2	Quiz	1.1	Quiz 1	1
			Lab	1.2	Evaluate Business World Transformation – Impact of the Internet and WWW	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
2	Social Networking and the Evolution of Personal Communication	*Security Strategies in Web Applications and Social Networking:* ▪ Chapter 3 ▪ Chapter 4	Quiz	2.1	Quiz 2	1
			Lab	2.2	Engage in Internet Research to Obtain Useful Personal Information	2
			Project	2.3	Project Part 1: Identify E-Business and E-Commerce Web Apps for Planned Transformation	2
3	Understanding and Managing Risk in Web Applications	*Security Strategies in Web Applications and Social Networking:* ▪ Chapter 5 ▪ Chapter 6	Quiz	3.1	Quiz 3	1
			Lab	3.2	Perform a Post-Mortem Review of a Data Breach Incident	2
			Project	3.3	Project Part 2: Identify Social Networking Apps for Planned Transformation	2
4	Identifying and Classifying Weaknesses in Web Applications	*Security Strategies in Web Applications and Social Networking:* ▪ Chapter 7	Discussion	4.1	Social Network Groups for All—"A Stupendous Idea or Security Incident Waiting to Happen?"	6
			Lab	4.2	Exploit Known Web Vulnerabilities on a Live Web Server	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
			Project	4.3	Project Part 3: Identify Risks, Threats, and Vulnerabilities	2
5	Strategies for Developing Secure Web Applications	*Security Strategies in Web Applications and Social Networking:* ▪ Chapter 8 ▪ Chapter 9	Quiz	5.1	Quiz 4	1
			Lab	5.2	Apply OWASP to a Web Security Assessment	2
			Project	5.3	Project Part 4: Web Application Vulnerabilities and Motivations for Attack	2
6	Auditing Web Applications	*Security Strategies in Web Applications and Social Networking:* ▪ Chapter 10	Quiz	6.1	Quiz 5	1
			Lab	6.2	Align Compliance Requirements to FISMA, SOX, HIPAA, GLBA, PCI DSS and AICPA	2
			Project	6.3	Project Part 5: Analyze the Software Development Life Cycle (SDLC)	2
7	The Role of Quality Assurance Testing for Web	*Security Strategies in Web Applications and Social*	Discussion	7.1	"Web site analysis—Know your visitors"	6

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
	Applications	*Networking:* ▪ Chapter 11	Lab	7.2	Perform Dynamic and Static Quality Control Testing	2
			Project	7.3	Project Part 6: Plan for Compliance	2
8	Vulnerability and Security Assessments of Web Applications	*Security Strategies in Web Applications and Social Networking:* ▪ Chapter 12	Quiz	8.1	Quiz 6	1
			Lab	8.2	Perform an IT & Web Application Security Assessment	2
			Project	8.3	Project Part 7: Configuration Management, Change Management, and Test Plans	2
9	Emerging Trends in Web Application Security	*Security Strategies in Web Applications and Social Networking:* ▪ Chapter 13	Discussion	9.1	"Business Anywhere—Security and the Mobile User"	6
			Lab	9.2	Recognize Risks & Threats Associated with Social Networking & Mobile Communications	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
			Project	9.3	Project Part 8: Vulnerability and Security Assessment	2
10	Modeling Web Application Security Strategies	*Security Strategies in Web Applications and Social Networking:* ▪ Chapter 14	Quiz	10.1	Quiz 7	1
			Lab	10.2	Build a Web Application & Security Lifecycle Plan	2
			Project	10.3	Project Part 9: End-Point Device Security	2
11	Course Review and Final Examination	N/A	Project	11.1	Project Part 10: Web Security Life Cycle	12
			Exam	11.2	Final Exam	25

Evaluation and Grading

Evaluation Criteria

The graded assignments will be evaluated using the following weighted categories:

Category	Weight
Lab	20
Project	30
Quiz	7
Discussion	18
Exam	25
TOTAL	**100%**

Grade Conversion

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

Grade	Percentage	Credit
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

Academic Integrity

All students must comply with the policies that regulate all forms of academic dishonesty, or academic misconduct, including plagiarism, self-plagiarism, fabrication, deception, cheating, and sabotage. For more information on the academic honesty policies, refer to the Student Handbook.

(End of Syllabus)

