American Public University System

American Military University | American Public University

ISSC297

Course Summary

Course : ISSC297 **Title :** Security Applications **Length of Course :** 8
Prerequisites : N/A **Credit Hours :** 3

Description

Course Description:

This course is an introduction to the study of the principles, practices, procedures, and methodologies to ensure security of data within web-based applications. It examines secure coding practices and processes, web application security configuration management techniques, and web application security standards. It appraises the convergence between web application security and associated threat vectors/attack methods. It appraises secure development processes, web application secure configuration techniques, and legal issues related to securing vital digital assets. Course topics include: Secure Configuration & Development, Vulnerability & Risk Mitigation, Vulnerability Assessments & QA Testing, and PCI DSS Compliance. Requires CITRIX CLIENT SOFTWARE INSTALLATION FOR ONLINE VIRTUAL LABS accessibility.

Course Scope:

This course is a study within the Information Assurance discipline of Web Application Security as it relates to security assessments and secure deployment.

Objectives

The successful student will fulfill the following learning objectives:

- CO1: Describe web-based applications and associated threats
- CO2: Compare and contrast mainframes, client-server, and applications
- CO3: Describe the role of web-based applications in E-commerce transactions
- CO4: Describe social networking and evaluate associated risks
- CO5: Evaluate web application security vulnerabilities against published standards
- CO6: Identify web application security controls and risk mitigation techniques
- CO7: Develop a security strategy and solution for securing web-based applications
- CO8: Assess web application security compliance requirements and objectives
- CO9: Design a web – application Vulnerability and Security Assessment Test Plan

Outline

Week 1:

Topic(s)

Types of Applications:

- Web-Based Applications
- Mainframe
- Client-Server
- Thick Client
- Thin Client

Learning Objective(s)

CO1

CO2

Reading(s)

Chapter 1: From Mainframe to Client-Server to World Wide Web

Assignment(s)

Week 1 Discussion

Assignment 1 (Wk1)

Week 2:

Topic(s)

E-Commerce Transactions Web-Application Functionality

Learning Objective(s)

CO3

Reading(s)

Chapter 2: From Brick-and-Mortar to E-commerce to E-business Transformation

E-Commerce and E-Business/E-Commerce Applications: Issues and Prospects

Assignment(s)

Week 2 Discussion

Assignment 2 (Wk2)

Week 2 Lab: Lab#1

Term Paper Topic (Wk2)

Week 3:

Topic(s)

Social Networking and Associated Risks

Learning Objective(s)

CO1

CO4

Reading(s)

Chapter 3: Evolution of People-to-People Communications

Chapter 4: From Personal Communication to Social Networking

Attack Timing Papers:

Remote Timing Attacks are Practical & Timing Attacks of Diffie-Hellman, RSA, DSS, and Other Systems

Assignment(s)

Week 3 Discussion

Assignment 3 (Wk3)

Term Paper Outline (Wk3)

Week 4:

Topic(s)

Web Application Security Vulnerabilities

Learning Objective(s)

CO5

Reading(s)

Chapter 5: Mitigating Risk When Connecting to the Internet

OWASP Top 10 – 2010: The Ten Most Critical Web Application Security Risks. **(PDF)**

2011 CWE/SANS Top 25 Most Dangerous Software Errors

Attack Trees article by Bruce Schneier

Assignment(s)

Week 4 Discussion

Assignment 4 (Wk4)

Week 4 Lab: Lab#3

Week 5:

Topic(s)

Web Application Security Controls

Learning Objective(s)

CO5

CO6

Reading(s)

Chapter 6: Mitigating Web Site Risks, Threats, and Vulnerabilities

OWASP Top 10 – 2010: The Ten Most Critical Web Application Security Risks. **(PDF)**

2011 CWE/SANS Top 25 Most Dangerous Software Errors

Assignment(s)

Week 5 Discussion

Assignment 5 (Wk5)

Week 5 Lab: Lab#4

Week 6:

Topic(s)

Web-Based Application Security Solutions

Learning Objective(s)

CO6

CO7

Reading(s)

Chapter 8: Securing Web Applications

Chapter 9: Mitigating Web Application Vulnerabilities

OWASP Secure Coding Practices and Quick Reference Guide

OWASP Code Review Guide, V1.1. **(PDF)**

OWASP Embed within SDLC

Assignment(s)

Week 6 Discussion

Assignment 6 (Wk6)

Term Paper Presentation (Wk6)

Week 7:

Topic(s)

Web Application Security Compliance

Learning Objective(s)

CO8

Reading(s)

Chapter 10: Maintaining PCI DSS Compliance for E-commerce Web Sites

PCI DSS Requirements and Security Assessment Procedures, Version 2.0 – Requirement 6 (PDF pages 38-43)

Assignment(s)

Week 7 Discussion

Assignment 7 (Wk7)

Week 7 Lab: Lab#7

Week 8:

Topic(s)

Web Application Vulnerability Assessments

Learning Objective(s)

CO6

CO9

Reading(s)

Chapter 12: Performing a Web Site Vulnerability and Security Assessment

OWASP Top 10 Tools and Tactics

OWASP Testing Guide v3

Assignment(s)

Week 8 Discussion

Assignment 8 (Wk8)

Term Paper Final Product (Wk8)

Week 8 Case Study

Evaluation

Evaluation Procedures

The grading will be based on assignments, discussion postings, case study, term paper, and labs.

1. **Assignments:** There will be eight assignments. The assignments and exercise will count as 28% of the final grade. The assignments will follow each of the major portions of the course. These assignments should include at least 3 references and be submitted in APA formatting. Assignments should be prepared in Microsoft Word or an equivalent word processor program and uploaded into the student folder by the due date.

2. **Discussion Postings:** There will be eight Discussion postings you will need to respond to. Answers should be a paragraph with a **topic sentence** that **restates the question** and **supporting sentences** using the terms, concepts, and theories from the required readings. You may respond to other students' answers using the terms, concepts and theories from the required readings. All responses should be a **courteous paragraph** that contains a **topic sentence** with good **supporting sentences**. You may respond multiple times with a continuous discussion with points and counter points. The key requirement is to express your idea and then **support your position** using the terms, concepts and theories from the required readings to demonstrate to me that you understand the material. The Discussion postings will count as 24% of the final grade.

3. **Case Study:** There will be a case study in this course. Details will be provided during the term in the course management system. This will count as 10% of your total course grade.

4. **Term Paper:** There will be a comprehensive and research based Term Paper for this course. The items that count towards the term paper are worth a total of 18% of your total course grade. The deliverable for this assignment MUST NOT be less than 10-pages. Borrowed materials must be properly cited per APA documentation format. Any clear evidence of plagiarism will result to automatic zero. (Please see the section below for the details of the 4 parts towards the term paper).

5. **Labs:** There will be 4 lab assignments for this course. More details will be provided during the term in the course management system. This will count as 20% of your total course grade.

Term Paper Topic (Due at end of Week 2)

Instructions: Only the topic is due at the end of Week 2

Submission Instructions: You are required to write a 10-page research paper on a topic of your choosing, related to the course concepts. Your topic must be submitted for approval by the end of Week 2. Please submit the topic via in the assignment section and not email.

Term Paper Outline (Due at end of Week 3)

Instructions: You must submit an outline for approval by the end of Week 3. It must include a detailed outline of topics and subtopics, as well as an annotated bibliography.

Submission Instructions: You are required to write a 10-page research paper on a topic of your choosing, related to the course concepts. The annotated bibliography must include at least three of the references you will use in your paper, written in APA style, with each one followed by a brief description of the reference.

Term Paper PowerPoint Presentation (Due at end of Week 6)

Instructions: A PowerPoint presentation with a minimum of 10 slides outlining the following:

At a minimum include the following:

- Detailed description of the area researched
- Technology involved in the area
- Future trends in the area
- Example companies involved in the area
- Regulatory issues surrounding the area
- Global implications for the area
- References (minimum of 4)

Submission Instructions: You are required to write a 10-page research paper on a topic of your choosing, related to the course concepts. The presentation highlights major areas of the paper. Typically the presentation would be a presentation of what you plan to include in the paper project to 'sell' the idea to the executive team or the funding team that would make a final decision whether or not to continue with the project.

Term Paper (Due at end of Week 8)

Instructions: You are required to write a 10-page research paper on a topic of your choosing, related to the course concepts. Your final draft is due at the end of Week 8.

Submission Instructions: Be sure your paper meets the following requirements:

You will be required to write one research paper this semester. The specifications are as follows:

1. 10 pages (double-spaced), excluding the title page, the abstract page (if included), and the references pages.
2. Choose any topic related to the course and write about the latest developments and issues.
3. Use at least five references outside of your textbook (you may use your textbook too, but are not required to).
4. In addition to the required number of pages for the assignment, you must also Include a reference page (bibliography), written in APA style, and a title page. Be sure to give all of your papers a descriptive title.
5. You must get your topic approved by the end of Week 2.
6. You must provide a 1-page outline of your paper by the end of Week 3. Your outline must include citations to three references (other than your textbook) and a brief summary of at least three references that you will use in your paper.
7. At Week 6 you will be working on a PowerPoint presentation highlighting the key points of the paper you are working on.
8. Use APA Style formatting in Arial 11 or 12-point font or Times New Roman styles.
9. Page margins Top, Bottom, Left Side and Right Side = 1 inch, with reasonable accommodation being made for special situations
10. Your paper must be in your own words, representing original work. Paraphrases of others' work must include attributions to the authors. **Limit quotations to an average of no more than 15% of the paper, and use quotations sparingly!**

This assignment has the embedded TurnItIn feature turned on. When you submit the paper, an originality report will be generated. The report must comply with the acceptable originality criteria displayed in the announcements on Academic Honesty in Week 1 of the course.

Grading:

Name	Grade %
Assignments	28.00 %
Assignment 1 (Wk1)	3.50 %
Assignment 2 (Wk2)	3.50 %
Assignment 3 (Wk3)	3.50 %
Assignment 4 (Wk4)	3.50 %
Assignment 5 (Wk5)	3.50 %
Assignment 6 (Wk6)	3.50 %
Assignment 7 (Wk7)	3.50 %
Assignment 8 (Wk8)	3.50 %
Discussions	24.00 %
Discussion 1	3.00 %
Discussion 2	3.00 %
Discussion 3	3.00 %
Discussion 4	3.00 %
Discussion 5	3.00 %
Discussion 6	3.00 %
Discussion 7	3.00 %
Discussion 8	3.00 %
Labs	20.00 %

Week 2 Lab: Lab#1	5.00 %
Week 4 Lab: Lab#3	5.00 %
Week 5 Lab: Lab#4	5.00 %
Week 7 Lab: Lab#7	5.00 %
Case Study	10.00 %
Week 8 Case Study	10.00 %
Term Paper Topic	1.00 %
Term Paper Topic (Wk2)	1.00 %
Term Paper Outline	2.00 %
Term Paper Outline (Wk3)	2.00 %
Term Paper Presentation	5.00 %
Term Paper Presentation (Wk6)	5.00 %
Term Paper Product	10.00 %
Term Paper Final Product (Wk8)	10.00 %

Materials

Book Title: Requires CITRIX CLIENT SOFTWARE INSTALLATION FOR ONLINE VIRTUAL LABS accessibility - instructions provided inside the classroom.

Author: No Author Specified

Publication Info:

ISBN: N/A

Book Title: Internet Security: How to Defend Against Attackers on the Web, 2nd Ed - the VitalSource e-book is provided inside the classroom

Author: Harwood, Mike

Publication Info: VS-Jones & Bartlett

ISBN: 9781284090550

Book Title: ISSC297 virtual lab manual provided inside the classroom

Author:

Publication Info: CLASS-Jones & Bartlett

ISBN: NTMO-ISSC297

Web-Based Readings

WEEK 1:

Ousterhout, J. (2012). *Why Web?* Web Applications. Standford University. Retrieved from
http://openclassroom.stanford.edu/MainFolder/CoursePage.php?course=WebApplications

WEEK 2:

Wikibooks (2011). *E-Commerce and E-Business/E-Commerce Applications: Issues and Prospects.*

WEEK 3:

US-CERT (2011) [Cyber Security Tip ST06-003](#).

Brumley, David & Boneh, Dan (nd.) [*Remote Timing Attacks are Practical*](#).

Kocher, Paul (nd.) [*Timing Attacks of Diffie-Hellman, RSA, DSS, and Other Systems.*](#)

WEEK 4:

The OWASP Foundation (2010. *OWASP Top 10 – 2010: The Ten Most Critical Web Application Security Risks.* Retrieved from http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf

MITRE Corporation ([2011.) 2011 CWE/SANS 25 Most Dangerous Software Errors](#).

Top **WEEK 5:**

The OWASP Foundation (2010. *OWASP Top 10 – 2010: The Ten Most Critical Web Application Security Risks.* Retrieved from http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf

MITRE Corporation ([2011.) 2011 CWE/SANS Top 25 Most Dangerous Software Errors](#).

WEEK 6:

The OWASP Foundation (2010) [*OWASP Secure Coding Practices Quick Reference Guide*](#).

The OWASP Foundation (2008) [*OWASP Code Review Guide, V1.1.*](#)

The OWASP Foundation (2007. Embed within SDLC. Retrieved from http://www.owasp.org/images/f/f2/Education_Module_Embed_within_SDLC.ppt

WEEK 7:

PCI Security Standards Council (2010) [*PCI DSS Requirements and Security Assessment Procedures, Version 2.0.*](#)

WEEK 8:

InfoSec Institute (2011) [*OWASP Top Ten Tools and Tactics*](#).

The OWASP Foundation (2008) [*OWASP Testing Guide v3.*](#)

<u>Software Requirements</u>

- Microsoft Office (MS Word, MS Excel, MS PowerPoint)

Selected Bibliography

Brumley, David & Boneh, Dan (nd). *Remote Timing Attacks are Practical.*

InfoSec Institute (2011). *OWASP Top Ten Tools and Tactics*.

Kocher, Paul (nd). *Timing Attacks of Diffie-Hellman, RSA, DSS, and Other Systems.*

MITRE Corporation (2011). 2011 CWE/SANS Top 25 Most Dangerous Software Errors.

Ousterhout, J. (2012). *Why Web?* Web Applications*. Standford University. Retrieved from http://openclassroom.stanford.edu/MainFolder/CoursePage.php?course=WebApplications

PCI Security Standards Council (2010). *PCI DSS Requirements and Security Assessment Procedures, Version 2.0.*

The OWASP Foundation (2008). *OWASP Code Review Guide, V1.1.*

The OWASP Foundation (2007). Embed within SDLC. Retrieved from http://www.owasp.org/images/f/f2/Education_Module_Embed_within_SDLC.ppt

The OWASP Foundation (2010). *OWASP Secure Coding Practices Quick Reference Guide*.

The OWASP Foundation (2008). *OWASP Testing Guide v3.*

The OWASP Foundation (2010). *OWASP Top 10 – 2010: The Ten Most Critical Web Application Security Risks.* Retrieved from http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf

US-CERT (2011). Cyber Security Tip ST06-003.

WikiBooks (2011). *E-Commerce and E-Business/E-Commerce Applications: Issues and Prospects.*

Course Guidelines

Citation and Reference Style

- Attention Please: Students will follow the APA Format as the sole citation and reference style used in written work submitted as part of coursework to the University. Assignments completed in a narrative essay or composition format must follow the citation style cited in the APA Format.

Tutoring

- Tutor.com offers online homework help and learning resources by connecting students to certified tutors for one-on-one help. AMU and APU students are eligible for 10 free hours* of tutoring provided by APUS. Tutors are available 24/7 unless otherwise noted. Tutor.com also has a SkillCenter Resource Library offering educational resources, worksheets, videos, websites and career help. Accessing these resources does not count against tutoring hours and is also available 24/7. Please visit the APUS Library and search for 'Tutor' to create an account.

Late Assignments

- Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. The due date for each assignment is listed under each Assignment.
- Generally speaking, late work may result in a deduction up to 15% of the grade for each day late, not to exceed 5 days.
- As a working adult I know your time is limited and often out of your control. Faculty may be more flexible if they know ahead of time of any potential late assignments.

Turn It In

- Faculty may require assignments be submitted to Turnitin.com. Turnitin.com will analyze a paper and report instances of potential plagiarism for the student to edit before submitting it for a grade. In some cases professors may require students to use Turnitin.com. This is automatically processed through the Assignments area of the course.

Academic Dishonesty

- Academic Dishonesty incorporates more than plagiarism, which is using the work of others without citation. Academic dishonesty includes any use of content purchased or retrieved from web services such as CourseHero.com. Additionally, allowing your work to be placed on such web services is academic dishonesty, as it is enabling the dishonesty of others. The copy and pasting of content from any web page, without citation as a direct quote, is academic dishonesty. When in doubt, do not copy/paste, and always cite.

Submission Guidelines

- Some assignments may have very specific requirements for formatting (such as font, margins, etc) and submission file type (such as .docx, .pdf, etc) See the assignment instructions for details. In general, standard file types such as those associated with Microsoft Office are preferred, unless otherwise specified.

Disclaimer Statement

- Course content may vary from the outline to meet the needs of this particular group.

Communicating on the Discussion

- Discussions are the heart of the interaction in this course. The more engaged and lively the exchanges, the more interesting and fun the course will be. Only substantive comments will receive credit. Although there is a final posting time after which the instructor will grade comments, it is not sufficient to wait until the last day to contribute your comments/questions on the discussion. The purpose of the discussions is to actively participate in an on-going discussion about the assigned content.
- "Substantive" means comments that contribute something new and hopefully important to the discussion. Thus a message that simply says "I agree" is not substantive. A substantive comment contributes a new idea or perspective, a good follow-up question to a point made, offers a response to a question, provides an example or illustration of a key point, points out an inconsistency in an argument, etc.
- As a class, if we run into conflicting view points, we must respect each individual's own opinion. Hateful and hurtful comments towards other individuals, students, groups, peoples, and/or societies will not be tolerated.

Identity Verification & Live Proctoring

- Faculty may require students to provide proof of identity when submitting assignments or completing assessments in this course. Verification may be in the form of a photograph and/or video of the student's face together with a valid photo ID, depending on the assignment format.
- Faculty may require live proctoring when completing assessments in this course. Proctoring may include identity verification and continuous monitoring of the student by webcam and microphone during testing.

University Policies

Student Handbook

- Drop/Withdrawal policy

- Extension Requests

- Academic Probation

- Appeals

- Disability Accommodations

The mission of American Public University System is to provide high quality higher education with emphasis on educating the nation's military and public service communities by offering respected, relevant, accessible, affordable, and student-focused online programs that prepare students for service and leadership in a diverse, global society.