CityUniversity of Seattle

Syllabus

SCHOOL OF TECHNOLOGY AND COMPUTING

ISEC 612: Breaking and Securing the Web

3 Credits
Effective: Summer 2014

Access to the Internet is required.
All written assignments must be in Microsoft-Word-compatible formats.
See the library's APA Style Guide tutorial for a list of resources that can help you use APA style.

FACULTY

Faculty Name: FACULTY NAME

Contact Information: CONTACT INFORMATION

[INSTRUCTOR MAY INSERT PERSONAL MESSAGE IF DESIRED]

COURSE DESCRIPTION

In this course, students look at the tools and techniques used to break and secure web applications. During the course students examine common web architectures and identify the points in those architectures with potential security vulnerabilities. Students learn and apply fundamental tools, processes and techniques for exploiting and securing vulnerabilities. Following this course, students are prepared to dive deeper into the breaking and securing code.

COURSE RESOURCES

Required and recommended resources to complete coursework and assignments are available from the Course Document Lookup.

CITYU LEARNING GOALS

This course supports the following City University learning goals:

- Professional competency and professional identity
- Critical thinking and information literacy

COURSE OUTCOMES

In this course, learners:

- Examine a proposed web design and determine its potential vulnerabilities.
- Describe web architecture and identify potential security points of weakness.
- Explain fundamental concepts of web security.
- Enumerate common web security problems and the corresponding best practices for defense.
- Identify and evaluate tools that can assist in securing an implementation.

CORE CONCEPTS, KNOWLEDGE, AND SKILLS

- Assess the relative merits of whitelisting and blacklisting.
- Demonstrate use of black-box web application scanners.
- Describe the common elements of web architectures.
- Differentiate between types of Cross-Site Scripting (XSS).
- Discuss authentication and session management.
- Discuss defenses against XSS.
- Discuss proper use of cryptography.
- Discuss relaxation of SOP through Cross-Origin Resource Sharing (CORS)
- Discuss session attacks and best-practice defenses.

- Discuss the various forms of injections.
- Enumerate security risks of ActiveX controls.
- Enumerate the most prevalent web security problems per OWASP.
- Examine Cross Site Request Forgery (CSRF) attacks.
- Examine direct object references as a security weakness.
- Examine poor usability as a security issue.
- Explain security risks of various error handling strategies.
- Explain the concept of Separation of Duties
- Explicate browser Same-Origin Policy (SOP)
- Explore attack surface reduction through Principle of Least Privilege.
- Illustrate parameter manipulation and hidden parameter guessing attacks.
- Illustrate validation techniques.
- Outline how to classify and prioritize threats.
- Study non-atomic check and use (TOCTOU) vulnerabilities
- Study proper security configuration.
- Study the attack vector chain and where viruses/worms can develop.

OVERVIEW OF COURSE GRADING

The grades earned for the course will be derived using City University of Seattle's decimal grading system, based on the following:

Overview of Required Assignments	***% of Final Grade***
Case Study of Website Attack	20%
Finding Website Vulnerabilities	20%
Web Scanning Tool	20%
Ecommerce design	20%
Discussions and Instructor Determined Assignments.	20%
TOTAL	**100%**

SPECIFICS OF COURSE ASSIGNMENTS

The instructor will provide grading rubrics that will provide more detail as to how this assignment will be graded.

Case Study of Website Attack

Students will perform a 5-7 page case study of a professional website that was attacked. This website can be one that the student knew about within their school or nonprofit or commercial organization, or can based on their technical book/web readings. Students will describe the vulnerabilities that allowed the attack and what lessons to take away.

Components	*% of Grade*
APA Style (citations, references, formatting)	20%
Finding and selecting information resources	20%
Web security probs & defenses	20%
Web architecture weaknesses	20%
Vulnerabilities of a design	20%
TOTAL	**100%**

Finding Website Vulnerabilities

A website sponsored by Google Code University (http://google-gruyere.appspot.com) purposely contains multiple common vulnerabilities. Students will follow the instructions and hints on that site to uncover five (5) vulnerabilities. Students will exploit each of those vulnerabilities found to prove their existence. The students will then explain how they would fix the site to remove those vulnerabilities. Students will write up their results, including source listings and screen snips to illustrate their findings.

Components	*% of Grade*
APA Style (citations, references, formatting)	20%
Finding and selecting information resources	20%
Vulnerabilities of a design	20%
Web security probs & defenses	20%
Web security tools	20%
TOTAL	**100%**

Web Scanning Tool

Students will choose a demo version of a web scanning tool that is paired with a purposely vulnerable website provided by that same vendor. Students will configure and run the tool. Students will document their steps and findings and provide a review of the tool.

Components	*% of Grade*
Web security tools	40%
APA Style (citations, references, formatting)	20%
Evaluating information	40%
TOTAL	**100%**

Ecommerce design

The students will assume they are assigned as the architect of new tiered ecommerce website. The students will describe the major components of their system and the security principles they will employ.

The web site must include at least these concepts: web server, load balancing, app server, database, DMZ, SSL, firewalls, session management, authentication.

The instructor may provide additional instructions.

Components	*% of Grade*
Vulnerabilities of a design	40%
Finding and selecting information resources	10%
Web architecture weaknesses	20%
Style and Mechanics	20%
APA Style (citations/references)	10%
TOTAL	**100%**

Discussions and Instructor Determined Assignments.

Students will be required to participate in a meaningful manner in discussions related to the content of the course. The instructor may also direct the completion of other assignments to enhance learning the course material.

Components	*% of Grade*
Quality of Responses	50%
Quantity of Responses	30%
Timeliness	20%
TOTAL	**100%**

COURSE POLICIES

Late Assignments

LATE ASSIGNMENT

Participation

PARTICIPATION

Professional Writing

Assignments require error-free writing that uses standard English conventions and logical flow of organization to address topics clearly, completely, and concisely. CityU requires the use of APA style.

UNIVERSITY POLICIES

You are responsible for understanding and adhering to all of City University of Seattle's academic policies. The most current versions of these policies can be found in the University Catalog that is linked from the CityU Web site.

Scholastic Honesty

Scholastic honesty in students requires the pursuit of scholarly activity that is free from fraud, deception and unauthorized collaboration with other individuals. You are responsible for understanding CityU's policy on scholastic honesty and adhering to its standards in meeting all course requirements. A complete copy of this policy can be found in the University Catalog in the section titled *Scholastic Honesty* under *Student Rights & Responsibilities*.

Attendance

Students taking courses in any format at the University are expected to be diligent in their studies and to attend class regularly.

Regular class attendance is important in achieving learning outcomes in the course and may be a valid consideration in determining the final grade. For classes where a physical presence is required, a student has attended if s/he is present at any time during the class session. For online classes, a student has attended if s/he has posted or submitted an assignment. A complete copy of this policy can be found in the University Catalog in the section titled *Attendance Policy for Mixed Mode, Online and Correspondence Courses*.

SUPPORT SERVICES

Disability Resources

If you are a student with a disability and you require an accommodation, please contact the Disability Resource Office as soon as possible. For additional information, please see the section in the University Catalog titled *Students with Special Needs* under *Student Rights & Responsibilities*.

Library Services

CityU librarians are available to help you find the resources and information you need to succeed in this course. Contact a CityU librarian through the *Ask a Librarian* service, or access library resources and services online, 24 hours a day, seven days a week.

Smarthinking

As a CityU student, you have access to 10 free hours of online tutoring offered through Smarthinking, including writing support, from certified tutors 24 hours a day, seven days a week. Contact CityU's Student Support Center at help@cityu.edu to request your user name and password.