ITSC 302 - Web Application Security

Course Description:
This course provides students an introduction to web technologies with an emphasis on web application hardening and exploitation. Topics include: application auditing, proxies, web attacks, web server hardening, man in the middle attacks, secure application protocols and data exfiltration.

3 Credits

Time Guidelines:
The standard instructional time for this course is 60 hours.

Prerequisite(s):

- ITSC 203

Course Assessment:

Labs	25%
Lab Quizzes	15%
Assignments	10%
Midterm Exam	25%
Final Exam	25%
Total	100%

Other Course Information:
Learner Engagement:

In order to be successful, the learner is expected to be engaged in learning activities for a total of 9 to 12 learning hours per course per week, which includes both in-class and out-of-class time.

ICT Policies:

The School of Information and Communications Technologies (ICT) expects students to act professionally during their studies. These expectations are described in the school’s Student Guidelines document page. Students should review the guideline regularly, as the content may change.

SAIT Policies and Procedures:
For information on the SAIT Grading Scale, please visit policy AC 3.1.1 Grading Progression Procedure: http://www.sait.ca /Documents/About SAIT/Administration/Policies and Procedures/AC.3.1.1 Grading and Progression Procedure.pdf

For information on SAIT Academic Policies, please visit: www.sait.ca/about-sait/administration/policies-and-procedures/academic-student

Course Learning Outcome(s):

1. Explain web application security and the technologies involved.

    Objectives:

    1.1 Discuss types of web applications and their functionality.

    1.2 Explain current technologies used by web applications.

    1.3 Summarize core defense mechanisms used by web applications.

    1.4 Examine methods to map web applications.

2. Evaluate client-side vulnerabilities and security measures.

    Objectives:

    2.1 Analyze data transmission to and from the client.

    2.2 Collect user data from HTML forms.

    2.3 Collect user data from browser extensions.

    2.4 Compare methods to handle client data securely.

3. Evaluate authentication technologies and counter-measures.

    Objectives:

    3.1 Describe authentication technologies.

    3.2 Analyze authentication designs.

    3.3 Analyze authentication implementations.

    3.4 Compare methods to secure authentication.

4. Evaluate session management technologies and counter-measures.

    Objectives:

    4.1 Describe session management technologies.

    4.2 Discuss vulnerabilities to man-in-the-middle attacks.

    4.3 Analyze token generation.

    4.4 Analyze session token handling.

    4.5 Compare methods to secure session management.

5. Evaluate access control technologies and counter-measures.

    Objectives

    5.1 Describe access control technologies.

    5.2 Analyze common vulnerabilities.

    5.3 Analyze methods to attack access controls.

5.4 Compare methods to secure access controls.

6. Evaluate back-end components, data stores and application attacks.

Objectives

6.1 Explain SQL.

6.2 Analyze SQL injection.

6.3 Analyze advanced data stores injection.

6.4 Analyze back-end attacks.

6.5 Examine logic flaws.

6.6 Compare methods to secure back-end components and data stores.

7. Evaluate attacks on users and counter-measures.

Objectives

7.1 Describe the role of users and the vulnerabilities.

7.2 Explain the varieties of XSS.

7.3 Compare methods of finding and exploiting XSS vulnerabilities.

7.4 Analyze XSS prevention techniques.

7.5 Identify other techniques used to attack the user.

8. Evaluate web application server technologies and their vulnerabilities.

Objectives:

8.1 Describe server technologies used for web applications.

8.2 Analyze information disclosure exploits.

8.3 Analyze natively compiled applications.

8.4 Analyze attacks on web application architectures.

8.5 Analyze attacks on the web application server.