CMT 447: WEB APPLICATION SECURITY   **3 CREDIT HOURS**
LIS 402: ADVANCED WEB AUTHORING

Pre-requisite: CMT 209: WEB DEVELOPMENT
                        LIS 304: WEB AUTHORING AND MANAGEMENT

Purpose:
To equip the learner with principles, practices, procedures, and methodologies to ensure security of data within web-based applications.

Objective:
At the end of the course students should be able to:
a) Evaluate web application security vulnerabilities
b) Identify web application security controls and risk mitigation techniques
c) Develop a security strategy and solution for securing web-based applications
d) Design a web–application Vulnerability and Security Assessment Test Plan

Course Description:
Secure coding practices, techniques and processes, web application security configuration management techniques, web application security standards. Web applications vulnerabilities and analysis, Parameterized queries. Threat vectors/attack methods. Secure configuration & development, vulnerability & risk mitigation, vulnerability assessments, and PCI DSS Compliance. Web application secure configuration techniques, legal issues related to securing vital digital assets. Secure development processes. Web privacy. RFI, CSRF, SQL Injection, XSS attacks, Cross-Site Request Forgeries, Invalidated redirects, Invalidated forwards, session hijacking. Function level access control, Hashing, Authentication, encryption, tokenization. Browser security. Penetration testing.

Teaching Methodologies:
Lectures, demonstrations, group/class discussions and practical exercises.

Instructional materials / Equipment:
Computers, writing boards, writing materials, projectors, etc.

Course Assessment:
Student performance
Assignments, tutorials, tests, practical exercises, practical projects and end of semester final examination.

Staff performance

To be based on student evaluations, evaluation by head of department and self evaluation.

Textbooks for the Course:
1) Andrew Hoffman (2020). *Web Application Security: Exploitation and Countermeasures for Modern Web Applications*. 1st Edition. O'Reilly Media Publishers.
2) Chris Dotson (2019). *Practical Cloud Security: A Guide for Secure Design and Deployment*. 1st Edition. O'Reilly Media Publishers.
3) Heather A., Betsy B., Paul B., Piotr L., Ana O. & Adam S. (2020). *Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems* 1st Edition. O'Reilly Media Publishers.
4) Tanya Janca (2020). *Alice and Bob Learn Application Security*. 1st Edition. Wiley Publishers.