

# MCAST

## Computer Security Laboratory Project

### Project #4—Web Exploit and Vulnerability Assessment

The objective of this project is to understand the methods of web exploitation and vulnerability assessment of web servers. These methods are used by both legitimate and illegitimate (hackers) users of the system to test for web site vulnerability. You are required to perform a simulated attack on an existing web server that is used by an e-commerce application.

**Goal 1. Produce a plan to perform system reconnaissance on the web server. Execute the plan of action.**

**Task 1: Develop a plan to perform system reconnaissance on the web server.**

**Task 2: Implement the reconnaissance procedure to identify the operating system and services offered using the scanning process capability of nmap and UMIT.**

**Assessment and Grading Criteria:**

**Task 1: (20%)**

- **What is the most appropriate type of scanning option that can be used to minimize disruption of service on the victim's web server? Justify your selection.**

**Task 2: (80%)**

- Completion of the following subtasks:
  - 1) Identify and describe all the available services offered by the systems.
  - 2) What type of web server is the system running? What type of database server is it running? What type of operating system is it on?

**Goal 2. Perform web exploitation and vulnerability assessment on the web server.**

**Task 1: Describe and perform a cross site scripting (XSS) attack.**

**Task 2: Describe and perform an SQL injection attack.**

**Task 3: Describe and perform a session hijacking attack.**

**Task 4: Describe and perform a cookie/information stealing attack.**

## **Assessment and Grading Criteria:**

### **Task 1: (25%)**

- **What is an XSS attack?**
- **Describe in detail how the attack was carried out.**
- **Describe the greatest impact of this attack.**

### **Task 2: (25%)**

- **What is an SQL injection attack?**
- **Describe in detail how the attack was carried out.**
- **Describe the greatest impact of this attack.**

### **Task 3: (25%)**

- **What is a session hijacking attack?**
- **Describe in detail how the attack was carried out.**
- **Describe the greatest impact of this attack.**

### **Task 4: (25%)**

- **What is a cookie/information stealing attack?**
- **Describe in detail how the attack was carried out.**
- **Describe the greatest impact of this attack.**