Course Title: Web Application Penetration Testing

Duration: Five (5) Days

Class Schedule: 9:00am to 5:00pm

Total Hours: 35 Hours


Course Pre-requisite: The course requires basic knowledge in Linux OS, Website Application, HTTP, and different Programming Languages.

Course Description: The course covers principles of computer systems and website application security. We will discuss various attack techniques and how to defend against them. Topics include hacking attacks and defenses, operating system holes, web security, social engineering attacks, data privacy act of 2012, and cybercrime act of 2012. Course projects will focus on breaking website applications, computer system, and understanding attacks.

Course Goals: By the completion of this course, the students will learn the important concepts and principles applied to Cyber Security.

Teaching Methods & Strategies:

- Lecture-Demonstration
- Group Work
- Online Discussion
- Lab Activities

Required Materials:

- Laptop with Kali Linux Operating System

Course Contents:

- Introduction and Information Gathering
- Different hacking attacks using different tools
- Writing a Vulnerability Assessment and Pentesting Report
- Introduction to Bug Bounty Hunting
- Introduction to Capture the Flag and CTF Competition
- Discussion about Data Privacy and Cybercrime Prevention Act of 2012

Reading Materials:

"Penetration Testing: A Hands-On Introduction to Hacking" by Georgia Weidman
"The Basics of Hacking and Penetration Testing" by Patrick Engebretson