# Thesis Defense

Computer Science Master's Program

## "A Study on API Security Pentesting"

By **Hadi Asemi**

**Abstract:**

Application Programming Interfaces (APIs) are essential in the digital realm as the bridge enabling seamless communication and collaboration between diverse software applications. Their significance lies in simplifying the integration of different systems, allowing them to work together effortlessly and share data. APIs are used in various applications, for example, healthcare, banks, authentication, etc. Ensuring the security of APIs is critical to ensure data security, privacy, and more. The security of APIs is vital because if breaches occur within these applications, attackers have the potential to pull users' data and use it maliciously. Therefore, the security of APIs is not only urgent but mandatory for pentesting APIs at every stage of development and to catch vulnerabilities early. The primary purpose of this research is to provide guidelines to help apply existing tools for reconnaissance and authentication pentesting. To achieve this goal, we first introduce the basics of API and OWASP's Top 10 API security vulnerabilities. Secondly, we propose deployable scripts developed for Ubuntu Debian Systems to install pentesting tools automatically. These scripts allow future students to participate in API security courses and conduct API security pentesting. API security pentesting, regarding reconnaissance and authentication, is discussed based on the configured system. For reconnaissance, passive and active approaches are introduced with different tools for authentication, including password-based authentication brute-forcing, one-time password (OTP) brute-forcing, and JSON web token brute force.

**Date: Monday, October 30th, 2023**
**Time: 5:00 PM – 7:00 PM**
**Location: 14-232a**
**Zoom: https://calpoly.zoom.us/j/84701501809**
**Committee: Dr. Fang, Dr. DeBruhl, Dr. Sisodia**