In the name of God

Sharif University of Technology
Department of Computer Engineering

CE 874: Secure Software Systems

Mehdi Kharrazi *Azar 25th, 1398*

Homework 3

1 CVE

CVE numbers are a popular identifier used to track a vulnerability and its related updates/patches for a software. Without CVEs, it is almost impossible to address software security issues. A CVE numbers is composed of a prefix, the year the CVE was registered, and a unique sequence number. The sequence number could be as large as 10 million-1, although before January 1, 2014, the maximum number was ten thousand-1.

In this homework, you will get familiar with CVEs and learn how to gather information (severity, attack vector, and type) related to each CVE. Additionally you will be employing a CVE to develop a fully working exploit. To that end, you need to choose a CVE from 2018 or 2019 and submit it for approval to the class TA. Afterwards, you should develop an exploit based on the chosen CVE and submit a report which states why the program is vulnerable and explain how the attack works. More specifically:

- Your CVE type should be related to the C programming language vulnerabilities.
- You should complete the attack and exploit the vulnerability to bypass system security. For instance, if a CVE requires a remote user, then the developed exploit should work remotely.
- You should submit the source of the code you have developed to implement the exploit, plus instructions on how the code should be executed.