CS253A Assignment 4

Submitted on 22/3/2021 23:11

Instructions

- You are given an extra 10 minutes after due time to submit your assignment.
- However, please note that any submissions made after the due time are marked as late submissions.

CS253A Assignment 4

Question:

Statement:

In this assignment, we will be working on common software bugs and methods to exploit them.

You can refer to https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html and https://samate.nist.gov/SRD/index.php for reference to common software weaknesses (CWEs).

Select any CWE (except those pertaining to buffer overflow). You will have to understand the weakness and develo one program/system where you design an exploit on that CWE.

You will have to write a report that covers:

> Details of the weakness as YOU understand it?
> The attack model under which you have built your exploit. Is there any specific requirement for the bug to be exploited (specific operating system, hardware, libraries, etc.)?
> How to run your vulnerable system to expose the exploit.
> Explain how your exploit works (in the accompanying program/system).
> Explain how to mitigate this weakness, i.e. exactly pin-point what was wrong in the program/system and wha is the way the program should have been written.

You are allowed to use any language/system to implement your vulnerable system/program.

Deliverables:

You have to submit only one zip folder as final submission in the format **cs253_assign_4_<your_roll_number>.zip**

This zip folder should contain the following files:

Report
A report file must be in PDF format and CANNOT be longer than 4 pages in 10 font.
Vulnerable and mitigated program/system
Working software/program, test case/suite, automated script to run the test, the output of the exploitation when r on your machine.

Uploaded Files:

cs253_assign_4_190200.zip