CS 547: FOUNDATION OF COMPUTER SECURITY

PROJECT PROPOSAL

Team Members:

Ravi Kishan   1701CS39   ravi.cs17@iitp.ac.in
Vivek Kumar Shaw   1701CS55   vivek.cs17@iitp.ac.in
Shrish Chandra Sharma   1701CS58   shrish.cs17@iitp.ac.in

Topic:

Tools for vulnerability detection

Motivation:

We all know that a lot of malware is constantly trying to break into systems and compromise the security services. Hence there is a need to write code that has as few vulnerabilities as possible. But we should assume that developers are humans and will make mistakes while developing software. Hence we need to develop a system of efficient code review that will expose the vulnerabilities in code before deployment. This becomes particularly a must for security-critical source code. Now to make the review process efficient and fast there is a need to develop some tools which can perform vulnerability tests on various source codes. Hence we analyze different techniques that can be employed to make tools for vulnerability detection.

Goals:

- To detect classes of common vulnerabilities through:
  - **Static analysis**: We will focus on aspects of
    - White box testing,
    - Analyse code smells,
    - Compare language-independent static analysis vs language specific static analysis

- **Dynamic Analysis/Runtime testing**: We will focus on
  - Grey box testing
  - Black box testing ,
  - Analyze common types of malicious inputs
- **Model-checking/Formal validation**: We will focus on
  - Design faults
  - Program slicing of vulnerable part
- To do a case study of Web Vulnerability Scanners(WVS)
- To try to implement a vulnerability detection tool through the knowledge gained.