

CWE Detection Analysis

Mahavir

Common Weakness Enumeration

- ▶ List of common software weaknesses
- ▶ Unified terminology provides common ground for discussions regarding software security
- ▶ Allows software vendors to quantify the security characteristics of their software in a uniform manner

Problem Statement

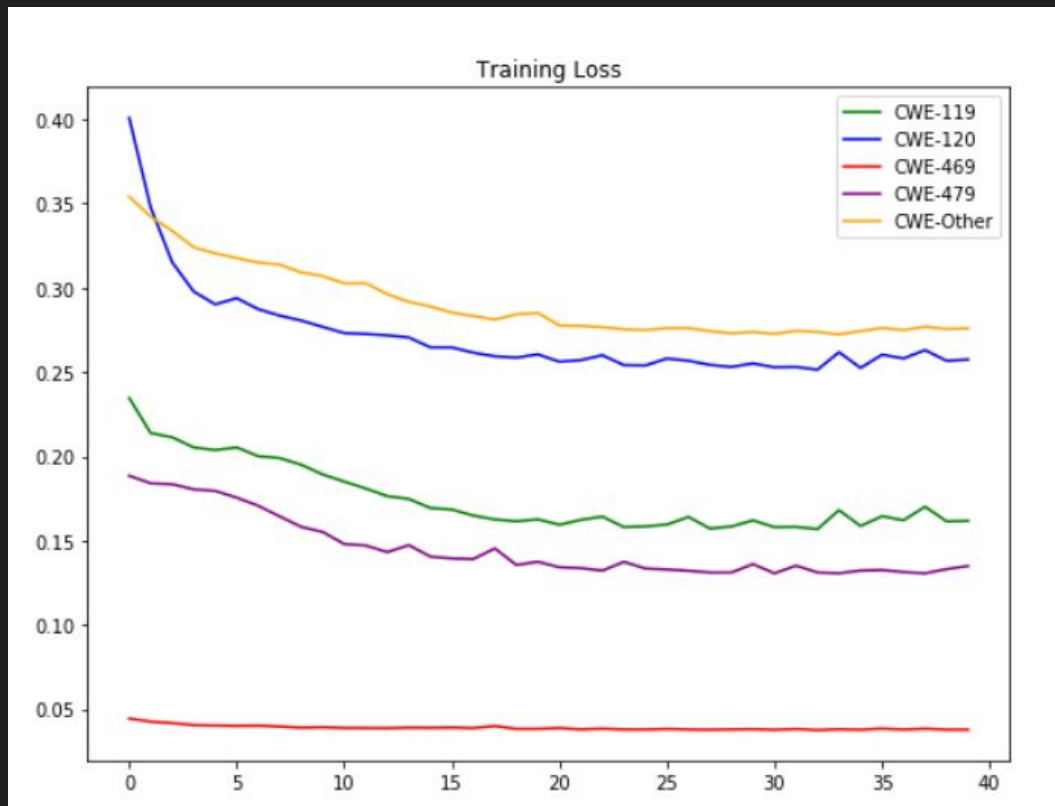
- Software vulnerabilities exist both in public and proprietary code
- Vulnerabilities can lead to system compromise, risk of exploit, result in system compromise
- Existing program analysis tools detect limited subset of possible errors based on predefined rules
- Automated Vulnerability Detection

Manual CWE analysis:

For manual extraction of CWE vulnerabilities we used:

1. CppCheck
2. Flawfinder

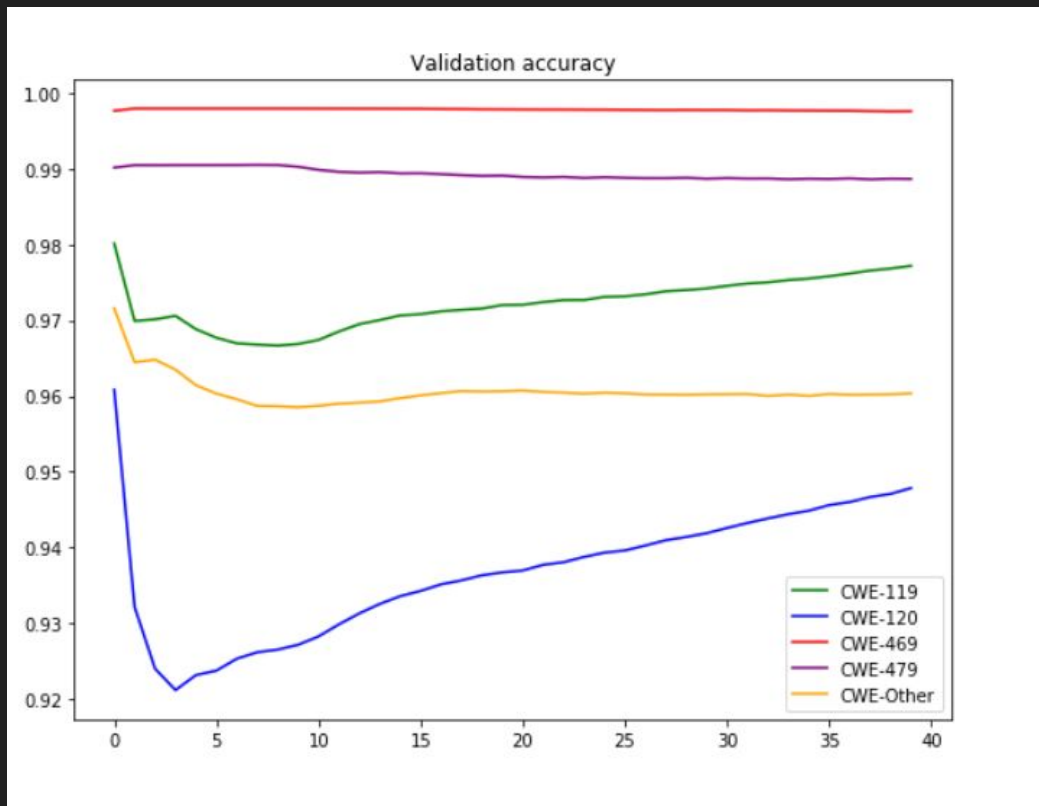
Loss on Training on Dataset



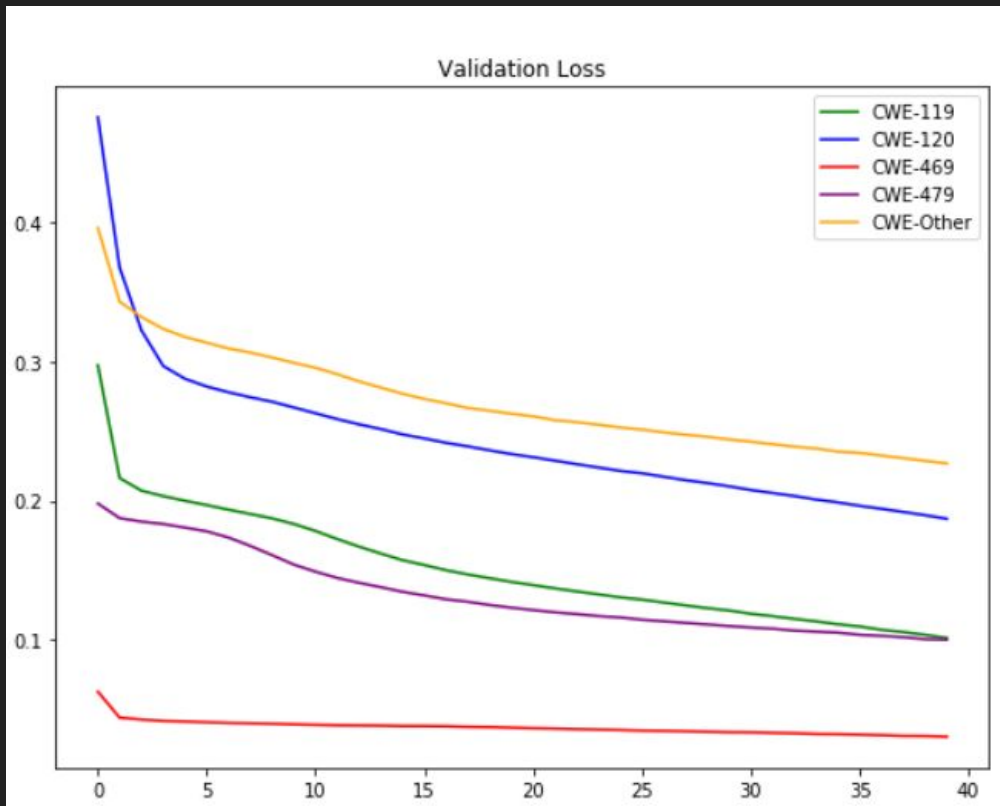
Accuracy on Training Dataset



Accuracy on Validation Dataset



Validation Accuracy



Binary Classification

