

Workshop 1: Automated Security Weakness Identification

Mary Mitchell (mem025)

Due Date: September 05, 2022

Most frequent security weaknesses:

Issue: [B101:assert_used] Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.

Severity: Low Confidence: High

CWE: CWE-703

(<https://cwe.mitre.org/data/definitions/703.html>)

Issue: [B311:blacklist] Standard pseudo-random generators are not suitable for security/cryptographic purposes.

Severity: Low Confidence: High

CWE: CWE-330

(<https://cwe.mitre.org/data/definitions/330.html>)

Issue: [B603:subprocess_without_shell_equals_true] subprocess call – check for execution of untrusted input.

Severity: Low Confidence: High

CWE: CWE-78

(<https://cwe.mitre.org/data/definitions/78.html>)