Birla Institute of Technology & Science, Pilani

Work Integrated Learning Programmes Division

First / Second Semester 2024-2025

Assignment: Assessing Open-Source Project Security using OpenSSF Scorecard

Course: Open-Source Software Engineering
Marks: 10
Due Date: *17-August-2025*
Submission Mode: PDF report upload on LMS

🎯 Objective:

To understand and evaluate the security health of open-source projects using **OpenSSF Scorecard** by uploading and analyzing a project on https://scorecard.dev.

🔍 Task Overview:

1. **Choose an Open-Source Project:**
   - Select any open-source GitHub repository (either your own project or a public one).
   - The project **must have a public GitHub URL**.
2. **Upload and Analyze:**
   - Go to https://scorecard.dev.
   - Enter the repository URL in the **search bar**.
   - Wait for the analysis to complete and review the security scores and checks.
3. **Create a Report:**
   - Prepare a report (2–3 pages) covering the following:

📄 Report Guidelines:

Your report must include the following sections:

1. Project Details (1 mark)

- Name of the project
- GitHub URL
- Brief description (2–3 lines)

2. Scorecard Summary (2 marks)

- Overall Scorecard Score (out of 10)
- List the individual checks and their results
- Highlight which checks passed and which failed

3. Security Analysis (3 marks)

- Discuss **at least 3 important checks** (e.g., Dependency Update Tool, Signed Releases, Branch Protection, etc.)
- Explain their relevance to project security
- Mention how your project performed on each

4. Improvement Suggestions (2 marks)

- Based on failed or low-score checks, suggest **2–3 ways to improve** the project's security posture

5. Reflection (1 mark)

- In 3–4 sentences, explain what you learned from using Scorecard and how it can help in real-world open-source development