ICT80004 Weekly Communication – Week #03

Student Name:

Arun Ragavendhar Arunachalam Palaniyappan

ID: 104837257

Commonwealth Scientific and Industrial Research Organisation (CSIRO)

Organisation:

Industry Supervisor: Dr. Shigang Liu

Date Prepared:

22/08/2025

Internship Week #: 3

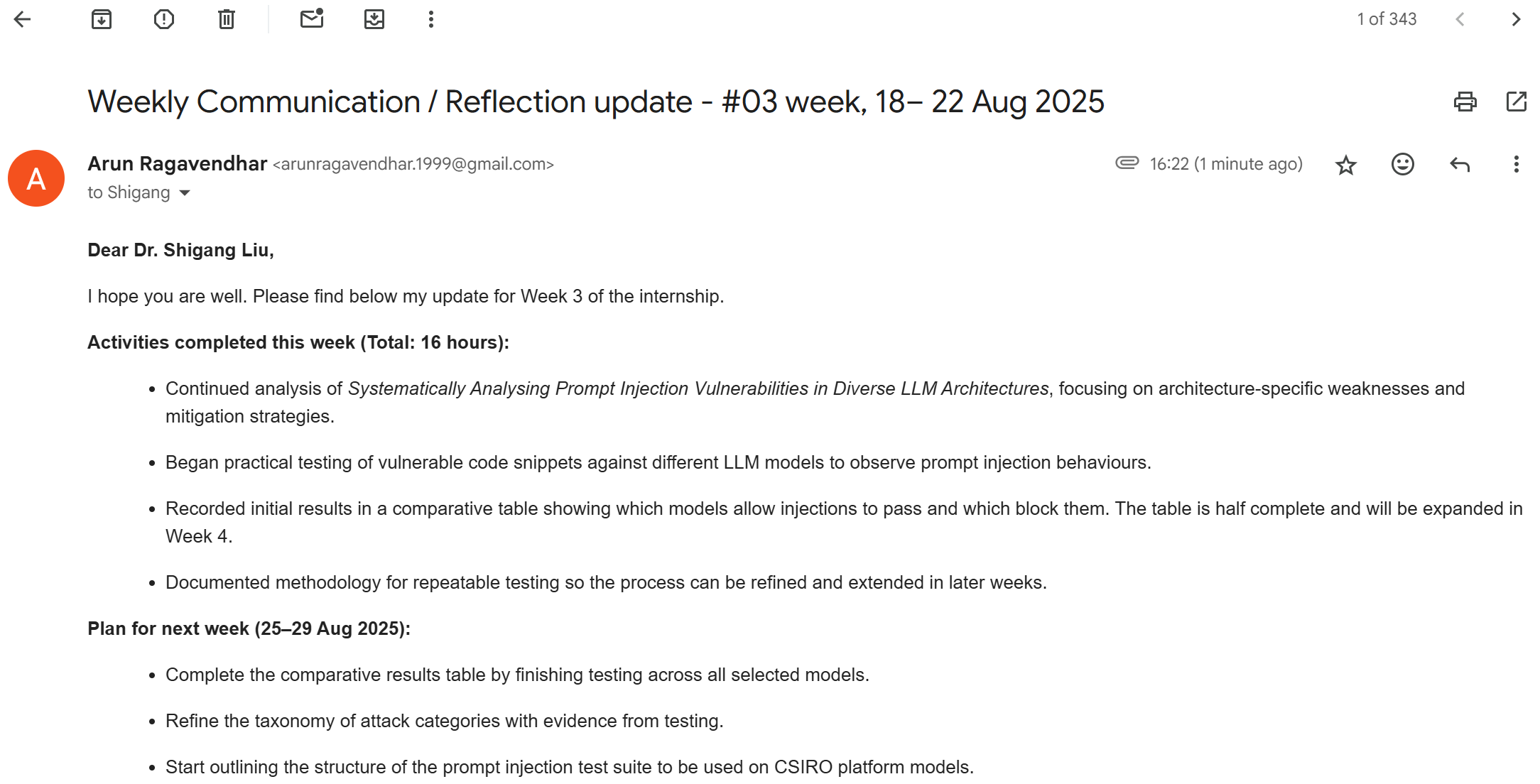
|  |  |  |
| --- | --- | --- |
| Day | Date | Task(s) completed |
| 1 | Monday  18 Aug 2025  8 hours | * Continued reading and analysis of *Systematically Analysing Prompt Injection Vulnerabilities in Diverse LLM Architectures*. * Identified model-specific weaknesses and mitigation strategies. * Prepared notes linking this paper’s findings to our planned test suite design. |
| 2 | Wednesday  20 Aug 2025  8 hours | * Began practical testing of vulnerable code snippets across different LLM models. * Recorded partial results in a comparative table (half complete). * Documented testing methodology for reproducibility. |

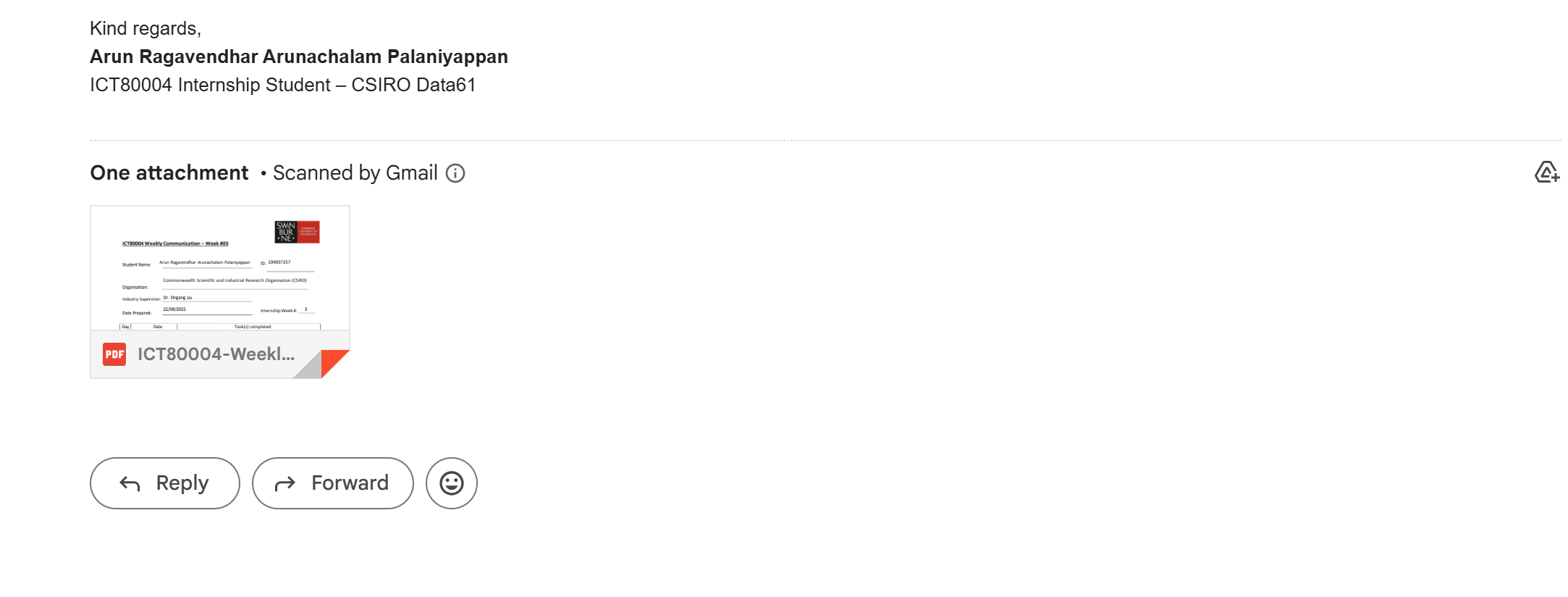
Total hours completed for the week: 16

**Plans for next week: #02 week (18– 22 Aug 2025)**

* Complete the comparative table of model test results.
* Use results to refine taxonomy of attack categories and defence methods.
* Draft initial structure for a prompt injection test suite to evaluate CSIRO platform models.

**Screenshot of Timely EMAIL communication update to the Supervisor at the end of week #02 sent on 22 August 2025 Friday at 4:22 PM (16:22).**

****

****