Institute of Data Capstone Feedback

For : Laurent Gatefait
Capstone Title : Automated LLM prompt testing tool

Course Code : 2025-06-10-CS-FT-AU-NZ
Feedback By : Luke Elin
Presentation Date : 29th August 2025

Aspect	Notes	Score
Relevance and Importance of Business Problem/Need	Laurent has chosen a business problem that could not be more timely or impactful: the rise of prompt injection attacks against LLMs. His report draws a clear parallel between today's rapid AI adoption and the early days of the internet, where innovation outpaced security, leaving behind systemic vulnerabilities. The problem is well defined, backed by industry context, and positioned as a genuine risk to businesses, particularly SMBs with limited security resources. This framing underscores the project's relevance and urgency, making it highly significant for the industry.	**9/10**

Effectiveness of Solution in Addressing Business Problem/Need	The solution—Prompt Jester—is both innovative and practical. Laurent developed a fully automated prompt injection testing pipeline that integrates AI agents, n8n orchestration, and flexible deployment options. The tool demonstrated measurable results, generating and evaluating 525 prompts with a 95.2% refusal/evasion rate, while also candidly documenting limitations such as false positives. The inclusion of recommendations for refinement (QA review, RAG workflows, CVE integrations, dashboarding) shows foresight and scalability. This balance of real-world testing and forward-looking improvements makes the solution highly effective.	**9/10**
Mastery of Handling Tools and Configuration	Laurent demonstrated advanced technical mastery. He successfully deployed n8n workflows, integrated local LLMs and orchestrated external services (Slack, Gmail, Google Sheets). The technical section showcases not just functional execution but sophisticated handling of OAuth, API credentials, JS nodes, and Cloudflare tunneling. This work reflects both breadth and depth in tool configuration, with careful attention to integration, scalability, and resilience.	**9/10**
Quality of Presentation and Audience Engagement	Laurent's presentation was polished, engaging, and logically structured. Complex ideas such as prompt injection risks were communicated in an accessible way, with strong visual aids including workflow diagrams, UI screenshots, and attack map outputs. The delivery was confident, and audience questions were addressed with clarity and authority. Overall, this was a highly professional presentation.	**9/10**

Written Report	The written report is exemplary. It is meticulously organized (executive summary, background, methodology, technical solution, results, recommendations, integrations, learnings, appendix), free of errors, and supported with authoritative references (OWASP, Palo Alto Networks, industry statistics). The inclusion of technical appendices (workflow JSON, UI screenshots, Slack notification examples) elevates the report into a professional-grade document. **It could easily serve as a reference model for future students.**	**10/10**

Overall Feedback:

Laurent Gatefait has delivered an outstanding capstone project—arguably the best in the cohort. It is relevant, rigorous, and forward-looking, marking him out as someone capable of making significant contributions to the field of AI and cybersecurity.

Frankly Laurent your project is an extremely high standard and easily in the top 5 I have seen during my time at IOD.

Simply WOW and you have an incredibly bright future in cyber and I am not just saying I have no filters 🫡