Senior Capstone Project Proposal

Project Team ID: Team 11

Project Title: Evaluating Large Language Models for Automated Security Vulnerability Detection and Explanation in Source Code

Team Members

Member	Name	Email
Team leader	Isaiah Reiff	reifim01@pfw.edu
Member 1	Stanley Gevers	gevesm01@pfw.edu
Member 2	Bo Wang	wangb02@pfw.edu
Member 3	Satwinder Singh	singh997@pfw.edu
Member 4	Kanan Badwal	badwkd01@pfw.edu

Faculty Advisor

Name / Title	Dr. Haytham Idriss
Office	ET 125A
Phone	(260)-481-6817
Email	hidriss@pfw.edu

Project Description

Type	Application development Research-focused Information systems
Abstract	In the last five years, the introduction of AI large Language Models (LLMs) has changed the way software development is being done in industry with more code being at least partially generated by LLMs. As LLMs become increasingly involved with software development, it is vital to ensure that these LLMs can accurately and consistently identify and explain security vulnerabilities in source code. The purpose of this research project is to evaluate a representative set of LLMs (e.g., ChatGPT, Claude, Gemini) for their ability to identify and explain common security vulnerabilities from a well-defined dataset of safe and insecure source code. A representative set of LLMs will be given a variety of prompts to evaluate a given safe or insecure piece of code for vulnerabilities. The LLM's will be

	graded on accuracy of the vulnerability identification and explanation using a benchmark of results to compare to. The goal of the project is to produce a formal research paper containing the analysis of the LLMs' ability to correctly identify and explain vulnerabilities in source code along with supporting deliverables (benchmarks, results, and documentation).
Research Requirements	• Produce formal research paper on findings • Produce thorough documentation of prompts, code, and results • Use a minimum of five common software vulnerabilities • Utilize a minimum of two programming languages for source code
Optional Objectives	• Evaluate 1-3 additional vulnerabilities • Evaluate additional programming languages (i.e. JavaScript) • Publish research paper (If possible)
Required resources (HW/SW)	• Code Editor (i.e. VS Code) • Programming languages: C, C++, Python • LLM APIs (i.e. ChatGPT or Gemini) • OneDrive for document sharing • GitHub for code storage and version control
Other notes	

As a member of Project Team, I agree to attend project meetings regularly, participate in developing project actively, and make a full effort to complete this project as proposed.

Isaiah Reiff **9/17/2025**
Team Leader Date

Bo Wang **9/17/2025**
Team Member 1 Date

Satwinder Singh **9/17/2025**
Team Member 2 Date

Stanley Gevers **9/17/2025**
Team Member 3 Date

Kanan Badwal	**9/17/2025**
Team Member 4	Date

As the Faculty Advisor, I agree to meet regularly with the student project team, manage their activities, and participate in the evaluation of project deliverables.

Haytham Idriss	**9/15/2025**
Faculty Advisor	Date

As the Project Sponsor, I agree to communicate with the student project team as needed to provide information related to project scope, requirements, assumptions, constraints or other items that may impact project success, and to participate in the evaluation of project deliverables.

Haytham Idriss	**9/15/2025**
Project Sponsor	Date

Technology and ECCN:
"If your project involves 'technology' that is either (a) not publicly available or (b) includes proprietary source code (not executable files), then it requires an ECCN." 'Technology,' for this purpose, is defined as "information necessary for the development, production, use, operation, installation, maintenance, repair, overhaul or refurbishing of an item. Technology may be in any tangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information revealed through visual inspection."

Interactive tool to determine ECCN:
https://www.bis.doc.gov/index.php/export-control-classification-interactive-tool

NDAs and IP Assignments:
The sponsoring company typically has NDAs and IP assignment forms that it wishes to use. Neither the NDA nor the IP assignment is an agreement with Purdue directly; these agreements are between the students and the sponsoring company. Of course, our office can review the company-provided documents to be certain it aligns with Purdue's standards. Alternatively, our office has draft agreements which we could provide for the sponsor's use. Again, as NDAs are between the student and the sponsor, Purdue cannot be a party to or advise the sponsor or the student on the NDAs, other than to outline some basic expectations as to fairness and suitability of the NDA to a student project.

Sponsor Acknowledgements:
By way of background, Purdue University professors who have senior capstone class projects involving outside sponsor companies notify our office so that we can prepare an acknowledgement form for the sponsoring company's completion. This is not a contract but an acknowledgement form signed by sponsoring companies which lays out Purdue's guidelines regarding class projects and outside company inputs, potential export control issues, and student intellectual property. Some sponsoring companies offer a monetary donation to the project, but that is not a requirement.