# The Impact of GitHub Copilot on the Security of the Code by Novice and Experienced Developers

Ali Zare, Hala Assal
mohammadalizareshahn@cmail.carleton.ca

Carleton University

## Motivation

- Impact of AI assistance on code security has been explored in research efforts.
- It has been shown that LLMs can have an adverse impact on security-related tasks [1], or help in more complex general tasks [2]
- Previous work did not focus on the impact of developers' experience, or were strictly focused on security tasks such as encryption, message signing, etc.
- We want to find out how use of AI with different levels of experience impacts security in regular tasks.

## Research Questions

- **RQ1**: What is the impact of GitHub Copilot on security of the code in relation to experience of the developers?

- **RQ2:** How developers with different levels of experience use and perceive GitHub Copilot?

## Analysis

- **Code:** Automatically with CodeQL, and manually to identify potential vulnerabilities, and cross-checking with screen and audio recordings.

- **Interview and Recordings:** Thematic analysis to gain a deeper insight on developers' use of AI assistance with different level of experience.

## Expected Results

- Previous work has shown that more experienced developers take more time to verify AI-generated code [1]

- We aim to understand whether using an LLM would distract the experienced developers from secure implementation, or whether the suggestions can help the novice developers to write more secure code

- The findings can help future research on LLMs and security, and also can help software development teams on making decision regarding using LLM tools in their workflow and potential impacts on the security of their code by the developers.

**Reference List**
[1] Perry, N. (2023). ACM SIGSAC CCS. 2023
[2] Asare, O. (2024). IEEE/ACM 46th International Conference on Software Engineering

## Study Methodology

- Within subject user study with software developers
- With varying years of experience
- Two programming tasks in Python
- Tasks have potential for common vulnerabilities
- Copilot in one of the tasks
- Semi-structured interview after the study

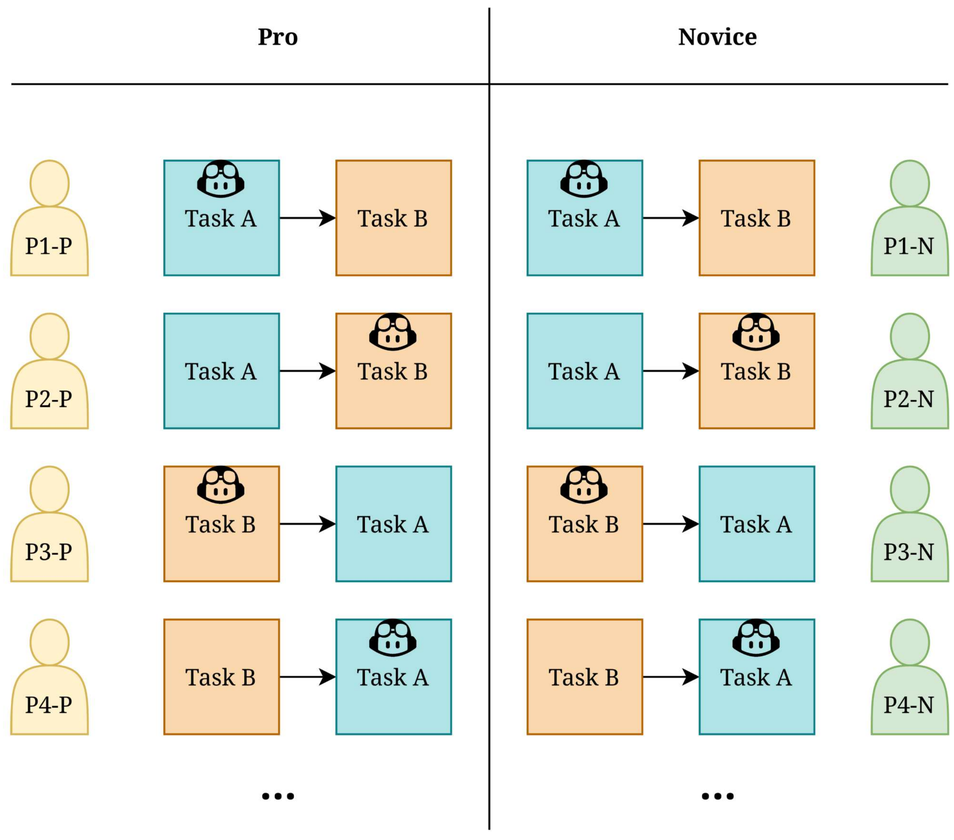


**Figure 1.** Task assignments are designed in a way to eliminate order effect. P represents professional developers and N reperesents novice developers.

## Study Setup

- In a Virtual Machine with remote desktop (RDP)
- Synchornous (in-person or over Zoom)
- Using think-aloud technique
- Screen and audio is recorded

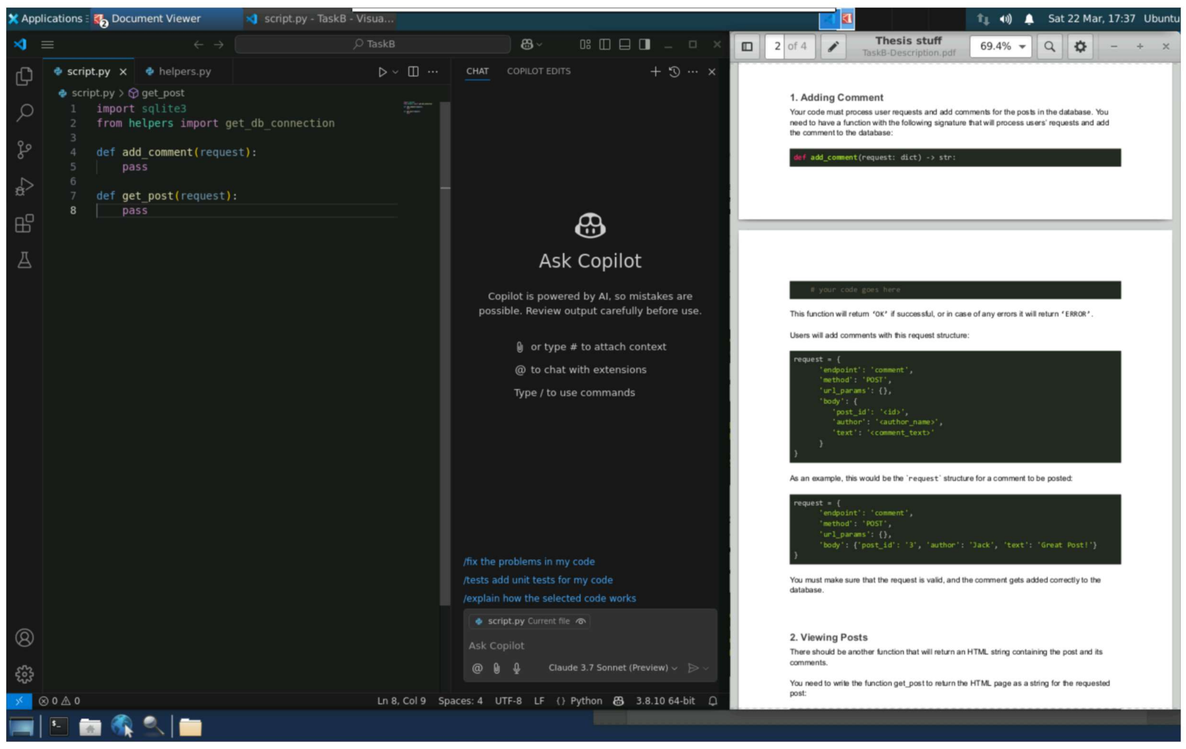


**Figure 2.** Screenshot of the VM with VSCode and task description open