P3

Interviewer: OK, that's fine. Then I'll start by asking roughly. During the process of code auditing, do you use ChatGPT? If so, how do you use ChatGPT to assist you?

P3: Actually, I do use it, but perhaps not very much. Well, when I use it, it's mainly for some relatively more difficult grammar issues. I might just throw the code directly into ChatGPT and let it analyze what the code is roughly doing. Well, like how it processes the data. That's mainly it, but I generally don't put very long code in there, just a few lines, definitely no more than 10 lines of code.

Interviewer: Oh, definitely no more than 10 lines. So, if you encounter very complex code, like a very complex project with, say, a dozen or twenty files, how do you use ChatGPT to assist you?

P3: Generally, I don't put many files into ChatGPT. Well, actually, I haven't tried it either, because I always feel that it might be more accurate for it to analyze a small piece of code. Analyzing a large piece might, I think, be better done manually, like analyzing the logic of the code and such. It might be clearer to analyze manually.

Interviewer: Oh, the process of code auditing generally consists of three stages: first planning, then reasoning, and then validating. I wonder if this is how you operate in your practice? For planning, it's probably something like first looking at these codes as a whole, then getting to know these codes, then trying to understand what they do. Then, for bug reasoning, it's about looking for logical loopholes in them. And thirdly, it's about writing a report to see if the loophole I've found is indeed there. Do you think your usual operating habits are like this?

P3: It's probably like this. Because first, you definitely have to look at these codes. For example, when I look at a large block of code, I first need to know what its function is, what it's generally doing. Well, what kind of business is it handling? Well, first, you need to know this in general. Then, if you're analyzing the logic, you definitely have to trace the data flow. What kind of data is it processing? How is it processed step by step? Well, only in this process can you find out if there are any processing loopholes, right? Well, and thirdly, for example, if I find this loophole, then I definitely need to, for example, write a POC script or EXP to see if this loophole actually exists. It mainly revolves around these three points.

Then, in this process, I think I use ChatGPT relatively more. Specifically, if a piece of code is relatively complex, I might put some complex statements into ChatGPT for interpretation. Well, and in the last stage, for example, when writing some utilization methods or scripts, I might tell ChatGPT a function and ask it to implement a certain function. So, it's mainly in these two stages that I use it. Well, and for myself, when doing logical analysis, I think it's more about manual analysis, just analyzing it myself.

Interviewer: Well, when you use ChatGPT, do you think you've encountered any difficulties or challenging aspects?

Participant: Uh. I think when asking it to implement a certain function, it may not achieve the ideal result. You really need to modify a lot of things yourself. And for example, the first time you use it, the function it writes may have problems and not work, and may not achieve the desired effect. You still need to modify it yourself. This is what I think ChatGPT may still have a little problem with for now.

Interviewer: Then, as you just mentioned, ChatGPT can only understand partial information. So, in the planning stage, if you were to interact with GPT, which specific aspects of information would you mainly ask it to help you understand? In this business process, how do you interact with GPT step by step to understand the specific business process?

Participant: To be honest, I haven't tried to have ChatGPT understand the entire business. Since I haven't actually asked it to analyze the whole business, I think it might be rather inaccurate and could mislead me. Another thing is that I think it would affect my thinking. Also, for some code and tasks that have information security requirements, you can't put certain business processes into ChatGPT, as I think it would be relatively insecure.

Then I found that some of its code gave a feeling of over-interpretation, because there was a function inside it. I saw a function, and when it was called in the original codebase, it was just calling this function, but the implementation of this function was not written in this script. And when interpreting it, it would also interpret the function's functionality. Right, there is a function call, calling this function, and there are also the parameters for this call, but there is no implementation of this function.

Actually, when auditing real code, it depends on what is being audited. If some code is not open source, it may involve information security issues. Directly uploading this code to ChatGPT, could there be a risk of leakage? If it is open source, I might, but if it is not open source, I won't.

Interviewer: When using ChatGPT, do you think there are other challenging aspects?
P3: With ChatGPT, I may still need to describe to it what to analyze, right? Yes, I need to interact with it.
Interviewer: Okay. Thank you very much.