P7

Interviewer: Could you briefly describe the entire process of your current code auditing, and preferably share your screen and then explain it in combination with some projects?

P7: Actually, the processes are generally quite similar. Because when we get a project, it may not necessarily compile successfully directly. It may require me to download some dependencies myself, or configure some environment variables, and then make it compile successfully. Usually, we will put it into a Foundry framework, which is to make it compile successfully first and also convenient for writing some script tests later. If we talk about the auditing process, first we need to understand the structure of the project and its code logic. If ChatGPT is used in this process, it is generally used in this stage, mainly for understanding the functional logic of the project. In terms of auditing, personally, I think ChatGPT is not very useful for now. Maybe it's also because I haven't provided some data to ChatGPT, so its false negatives and false positives are actually quite serious. We will use tools like Slither to scan, which can only detect very simple vulnerabilities, such as variable naming and variable const.

Only some very simple things can be detected by Slither. In fact, although Slither can be used for scanning, the useful information it detects is mostly quite simple. For example, most of the high-risk and medium-risk issues it reports are actually false positives. And for real audits, most of the detected vulnerabilities still need to be manually reviewed. That's about it.

Interviewer: So you mainly still use traditional software to assist you with this. The reason you don't use ChatGPT is that the false positives and false negatives in the results it audits are relatively high. So when you use tools to assist you, you value their accuracy and reducing false negatives.

P7: Actually, false negatives are not a big deal. The main issue is that the information it provides is not correct, mainly false positives. I have to read the information it gives me again to check if it is accurate. But if it is incorrect information, it is actually a waste of time, because the main reason for using ChatGPT is to save time and effort. That's it.

Interviewer: You just mentioned two, no, actually three processes. One is understanding, then finding loopholes, and then verifying what you've found using tools, which amounts to three processes. Then you just mentioned that it's equivalent to the understanding process where you use it the most. Currently, apart from ChatGPT, are there other methods to help you better understand? How did you do it before?

P7: In Slither, if there are many contracts in a project, it actually provides a way to show the dependencies between projects, and these diagrams can be output to help understand.

Interviewer: Do you have any specific examples? You can share your screen to explain and show what you're talking about.

P7: Check to see if there are any archives.

Interviewer: Or you can just open the software interface, then directly let it scan, and let it generate.

P7: Let me show you a relatively simple graph. Can you see it? This is the CG graph output by a contract, but in fact, this kind of graph is generally viewed less often because most of the time, it is still manually inspected.

Interviewer: This diagram was generated by Slither, right?

P7: Yes, it can also generate quite a few graphs, but in most cases, people still manually examine such relationships.

Interviewer: Actually, it's equivalent to the fact that during the process of understanding this code, you will form such a thing in your mind.

P7: Yes, I will take note of the relationships between contracts and their most important functions.

Interviewer: Can ChatGPT help you form such a [missing word], or is ChatGPT not very good at this?

P7: I feel so, because especially when I want to understand the relationships between multiple files or multiple contracts, it probably won't be able to help me in this regard. Especially when ChatGPT has more input data, the feedback it provides is rather broad. For example, if I want it to tell me about the functions of a contract, if I directly feed the entire contract to it, what it gives me are all very broad things, or even wrong things. If I want it to give me precise feedback, I usually give it a single function instead of stuffing the entire contract into it at once, because if I do so, it won't be very accurate.

Interviewer: That's equivalent to having two types. One is a more high-level type, and the other is a very specific type of code snippet. For this very specific type of code snippet, when looking for vulnerabilities, which vulnerabilities do you think ChatGPT is better at finding?

P7: The identified segment is not meant to find vulnerabilities; it's meant to tell me the functional logic of this function, because it really isn't very good at finding vulnerabilities. If we want it to find vulnerabilities, we may need to adjust it. I feel like there are many companies working on this, but I don't really understand the specific operations.

Interviewer: When you're doing this relatively manual process of finding vulnerabilities on your own, do you think you have something like a Knowledge Base, a knowledge system, or a checklist, and then you go through it item by item according to your criteria? Or do you rely more on tacit knowledge or your intuitive sense?

P7: It's probably based on experience, and there's no specific summary, but it's indeed related to different project types. For example, for token-type projects or projects of other types that need to be checked, there's indeed roughly a list, just not specifically summarized. For instance, it's necessary to check if there are any centralization risks, or simply put, if there are any fixed areas for cost savings, or if there are mild [unclear] issues during calculations. If it's a project with deflation and closure [unclear] for specific situations, there will be some vulnerabilities that are likely to occur in deflation and closure [unclear], and then a specific check will be conducted in this regard. That's roughly how it is.

Interviewer: When you use ChatGPT to help you understand things, do you have some specific prompts of your own? How do you design these prompts to make it better assist you?

P7: I will tell it what content I want. For example, at the beginning, I want it to tell me the specific content of the entire contract on a large scale. For example, I will specifically tell it to tell me what variables are inside, that is, some important state variables, and help me summarize the important functions of those public functions. I will probably specify for it to summarize certain content. If its feedback is inappropriate, I will further tell it. Then, after using the conversation for a long time, indeed, when I directly send something to it, it will also give me some answers that meet the requirements I previously gave it.

Interviewer: Are there any tricks when you use ChatGPT? For example, how to improve your prompt so that its returned results will be better, and how to design the prompt when its returned results are not satisfactory.

P7: There's nothing like that after this. I haven't specifically done anything about it. I've set requirements for it. If its response to me is not accurate enough, I'll provide feedback to it, telling it which part of the response doesn't meet my requirements and what I expect from it.

Interviewer: Okay. Then the next question is, when using your traditional method or the method assisted by ChatGPT, what challenges do you think you encounter respectively?

P7: Traditionally speaking, when reading code, especially when there are many projects, it is indeed rather troublesome to read. So in this regard, using ChatGPT allows me to quickly get a general idea of what the contract does. However, ChatGPT does sometimes mislead and give an incorrect understanding. But if such a situation occurs, when I later look at the code, there will be an incorrect impression in my mind, which I consider a bad impression.

Interviewer: Does it mean you've formed a negative impression of ChatGPT, or is it something like this?

P7: If it gives me incorrect feedback, it will leave a bad impression when I read the code later.

Interviewer: In this way, when you see a potentially wrong direction, it leads you to take a detour in that wrong direction. But in terms of understanding, it should be okay.

P7: It's quite good in terms of understanding.

Interviewer: There is relatively little misinformation.

P7: Right, mainly in terms of auditing and finding loopholes, what it provided was basically wrong.

Interviewer: We are currently planning to develop a tool using ChatGPT to assist in different stages of your code auditing, such as the understanding stage, the vulnerability discovery stage, and the verification stage after discovery. In these different stages, what features do you think you would most like to have from ChatGPT?

P7: If it's in the identification phase, I do hope there will be a function that provides the relationships between contracts, because the existing functions are not very useful and can only be manually checked. In the vulnerability search phase, actually some simple vulnerabilities, such as the calculation precision or unused variables mentioned just now, which are very simple areas that can be optimized, can also be detected by tools like Slither. Actually, I'm not quite sure to what extent ChatGPT can find vulnerabilities. It may need quite a lot of data to support it in identifying what vulnerabilities are likely to occur in a certain type of project, for example, what vulnerabilities are likely to occur in token-type projects. I hope it can work in this direction.

Interviewer: In terms of verification.

P7: In terms of verification, it's like we all use Foundry to write scripts, but actually ChatGPT is not very good at using Foundry in this regard. It can write Python and other languages quite well, but it may still be relatively lacking in writing contracts using Foundry. So we do this part manually. Of course, it should also be able to implement this function, that is, to verify vulnerabilities. If it can implement this function, that would be great and acceptable.

Interviewer: It's like you find a loophole, and it verifies it for you in a relatively good and reliable way.

P7: Implement an attack process for it to see if an attack can indeed succeed.

Interviewer: After the code auditing is completed, you still need to write a report. I'm not sure if a report is required in all scenarios, but there is such a task. So, do you think you will use ChatGPT during this stage?

P7: I will. I've already used it, and in this regard, what it writes is actually quite good. I'll give it the audit reports I've written before, then let it learn which structures and headings need to be written, tell it about the structure and requirements, and generally what it outputs is quite good, mostly meeting the requirements. Just make some revisions, and it'll work. It's great.

Interviewer: Then it might be about the understanding of the initial stage of this project audit.

P7: When it comes to using ChatGPT, I think it's not just about giving it requirements, because sometimes it does understand things differently. However, if you do give it some examples, the information it returns will basically meet expectations. For example, as I just mentioned, when asking it to help me write an audit report, if I simply give it requirements and say I want it to be like this, the language it uses or the level of conciseness, and perhaps these detailed aspects, it's difficult to accurately describe them, and it's also difficult for it to produce something accurate. But if I give it a few reports I've written myself, and then it returns something, it will be much more accurate.

Interviewer: Is it equivalent to helping you improve this stage, and it's done quite well?

P7: Right, in terms of its feedback text information, it's quite good. I describe to it what this vulnerability is like, then roughly how it can be resolved, and then include it in the report, asking it to supplement information according to this format, and generally it can understand.

Interviewer: This is also a good use. Thank you.