P8

Interviewer: Ok, first of all, welcome to our interview. The main purpose of our interview is to understand some user habits of auditors during their regular auditing processes.

P8: Okay.

Interviewer: I see that you have three years of experience in the coding and development department and six months of experience in code auditing.

P8: Right.

Interviewer: For you, is the frequency of using ChatGPT a few times per month?

P8: Yes, it is.

Interviewer: Okay, my first question is, could you describe your current practice when doing code auditing? For example, after receiving the code for a project, how do you conduct code auditing? Could you describe the entire process? It would be best if you could illustrate with specific examples. If convenient, you could even find a piece of code and share your screen with us.

P8: Okay, I'll first explain the process to see if it's clear enough.

Interviewer: Okay.

P8: First, when I get a project, I will first look at what contracts the project has, what the scope of our audit is, and then sort out the relationships between the contracts once, because it will involve function calls. The next step is to carefully examine the code logic of the main contracts. In this process, it is equivalent to going through all the code logic within the audit scope, and then marking some points that may have problems or points that seem confusing. After carefully examining all the code, I will re-establish the logic between the contracts. The next step is to carefully examine the previously marked areas to see if there are any problems, whether they are real problems or false positives, and finally write POC tests.

Interviewer: Do you usually use any software or the like to assist you?

P8: The most widely used one is still Vscode, which makes debugging or viewing code more convenient.

Interviewer: You will use some specific plugins and so on.

P8: Yes, that's right.

Interviewer: Can you describe which functions of these tools you mainly rely on to assist you in code auditing?

P8: Actually, it's mainly using the SOLIDITY plugin to view code, so I look at code more often. Then I also use fondary to write some tests, and I'll run the project once first and write tests like this. These are the two main tools I use.

Interviewer: Okay, why don't you explain it with some examples? That way, we can have a better understanding and gain more insights into user behavior.

P8: What kind of example is it? Is it a project? Then show you one of my audited projects?

Interviewer: This approach is also acceptable. Alternatively, you can find a repository on GitHub, for example. Suppose you now have obtained the code from this repository. What would you do after getting the code, and what types of vulnerabilities are you looking for? For example, how to integrate with a tool or some additional tools.

P8: Okay, I'll look for it.

Interviewer: Take your time, think slowly.

P8: I might not be able to demonstrate it, because what I want to show you is public source code. So, okay, should I just take a look at this and share my screen?

Interviewer: Okay.

P8: Can you see it? This is open labeling, and its latest version is 5.0. Then, are you asking me to introduce the whole process?

Interviewer: Right.

P8: During the auditing process, we only look at the content under the ERC20 file. That is to say, I will first focus on ERC20, which is the main contract. Then I will check what content it imports and examine these imported contents. Right, and then I will briefly go through their general logic and so on. For example, after using import, it inherits some functions that might be used in the contract but are not reflected in this contract itself, so the two need to be combined and examined together. In this way, I first simply sort out the relationship between them. After sorting out the relationship, I will start from the beginning and first pay attention to its version, because there were also issues with previous versions, such as various compatibility issues. I will start from the version, and then after that, I will look at what content it inherits, and then check the type of its variables and their visibility. Then I will just follow the logic downwards. For example, at a certain point, there might be an issue, and I will make a note indicating what kind of issue it is, making a mark that I can understand. Then, after finishing looking at this, I will come back and focus on this marked part. That's roughly how it goes.

Interviewer: Right, for some of the tools you just mentioned, how do these tools help you?

P8: In terms of tools, after having the SOLIDITY plugin, it means that jumping is relatively convenient. As long as the input path is set correctly and the files are placed in the corresponding location, this jumping will be relatively convenient. Moreover, regarding function calls, let me see, it means that this part calls an internal function, and then jumping will also be very convenient. For another tool, the fundraiser still needs to download some content by itself, then initialize it, and then write some tests and so on.

Interviewer: Can you describe the process you just described? From my understanding, it should be a process equivalent to you understanding the code.

P8: Right.

Interviewer: For the next step, such as finding vulnerabilities, how do you go about it?

P8: Finding vulnerabilities is actually marked during the process of inspection. For example, there may be some calculations, or if you look at this transfer, there will be authorization and so on. That is, this place will authorize and then transfer, and then this part will specifically jump into this logic to see if there are any suspicious operations. For example, or when encountering some calculation problems, such as division which may have precision loss, and at that time this part will also be marked. Whether to specifically consider precision loss, whether it is a vulnerability, still requires further detailed examination, which needs to be considered in combination with the entire logic, and then incidentally consider the possible risks, and what level it can be marked as, that is, the risk level.

Interviewer: Have you ever, for example, summarized some methods or developed some unique ones to help you find vulnerabilities more quickly?

P8: Actually, there are also cases. After each audit, I would write a report to summarize the findings. Then I have a template, or I would refer to previous ones, which is equivalent to having gained experience. For example, for this kind of large-arm contract, it mainly focuses on what kind of authorization or quantity calculation during transfer, and then corresponding to different types of projects, there will be different points to note. Based on some experience, these used experiences will emphasize paying attention to certain aspects.

Interviewer: Have you ever tried using ChatGPT to assist this process?

P8: Yes.

Interviewer: Can you describe how you use ChatGPT to assist you?

P8: Actually, when I use ChatGPT, it mainly helps me understand. If the project code is relatively large, the logic will also be very complex, and when its logical model is very complex, I will ask ChatGPT to explain what the function of that piece of code is. First, I'll ask it to explain so that I can understand. Then, if I'm unsure about something I think might be a problem, I'll put it on ChatGPT to help me see how it assesses the risk and whether there is a risk or not.

Interviewer: Do you think it can improve your understanding efficiency?

P8: Yes.

Interviewer: How much do you think it can increase approximately?

P8: If it's used very frequently, I think it's probably around 70 to 80.

Interviewer: There are quite a few of them. Why don't you use them frequently?

P8: If it's not used frequently, on the one hand, it's because some projects are relatively simple and don't require it; on the other hand, it's still preferred to use it as an auxiliary tool, that is, not to rely on it completely, because I'm currently in the process of learning, and if I rely too much on tools, I think my ability might improve more slowly.

Interviewer: Have you ever tried using it as a learning tool while using it, and learning from it yourself?

P8: There will be some concepts that are really hard to understand. This part involves some financial knowledge, which is difficult to comprehend. Then I will combine it with code

to help me explain what this part specifically means. If it can help me understand through code, it will also be very clear, like this.

Interviewer: So it actually still helps you learn, but why hasn't its usage changed from monthly to daily?

P8: Isn't daily use a bit too frequent? There might not be that much work every day, and it depends on one's own work tasks and workload. Sometimes it is also used very frequently.

Interviewer: So your current main job task is not to conduct audits, right?

P8: No, it's also an audit.

Interviewer: So it's like in the past six months you've just transitioned from, say, a developer to an auditor, right?

P8: Yeah, more or less.

Interviewer: During this process, for example, from your first exposure to code auditing until now, in your learning process, what difficulties and challenges do you think you have encountered? What are the similarities and differences between it and development?

P8: Let me start by talking about the differences. That is to say, at the beginning of an audit, one has to look. Not only do you need to look at the code, but also if you have a bit of experience, you'll know. For example, with contracts, I can tell which parts need to be focused on. At the beginning, there will be a lack of such experience, not knowing where to find these vulnerabilities and what areas to focus on. After a long period of time, say half a year, there will be some gains and some experience will be accumulated. That is to say, for specific projects, one will know what to focus on, and there will be a little progress. As for the commonalities, it means that one has to test on their own. Some of the logic in the tests and POCs still has to be thought out by oneself, and then implemented after that.

Interviewer: So the amount of code audited is actually smaller than that developed, right?

P8: Right, auditing still tends to focus more on observation.

Interviewer: What was one of the starting points for your transfer to auditing?

P8: In terms of auditing, I actually mainly want to get in touch with the field of security because my major is in this area, and then I want to get in touch with blockchain security.

Interviewer: Regarding the question just now, what do you think are the challenges you've encountered during the learning process?

P8: The challenge is the lack of experience, and in some areas, I actually think less. Maybe I find that this is a vulnerability, but I can't precisely locate whether it is a high-risk or medium-risk one. I haven't been able to accurately assess its risk for the time being. I think this is a challenge. The more experience I accumulate, the more I will know what attack methods might be used in this area and what the potential harm of the attacks might be. I think this is a challenge.

Interviewer: So auditing is an industry that relies more on some domain knowledge than development, right?

P8: I think it is relatively dependent on experience.

Interviewer: Understood. Are there any other challenges that are difficult? Or any inconveniences?

P8: If there are any inconvenient aspects, another one is that it is a bit more difficult to understand the economic models they use in the model, because although they will provide a white paper during the audit, there are still some differences between the white paper and the actual implementation of the code, which makes it a bit hard to understand, just like that.

Interviewer: Can ChatGPT be of any help here?

P8: Yes.

Interviewer: Can you describe how you interact with ChatGPT to, for example, understand code or find bugs?

P8: Let me think. Roughly speaking, if it uses or copies too much code, its explanations won't be very accurate. Then I usually locate a function and copy it in. For example, if it's a token function, I'll ask it to explain what its purpose is and what its variables mean. This is the explanation stage. Or, if there are some economic models involved, I'll also clarify in advance that this function belongs to a certain model, is a certain function, etc., and ask it to explain, which means I'll put forward some requirements.

Interviewer: During the process of interacting with it, do you have any specific methods for prompting it, that is, specific ways of asking questions? Do you have any methods that can, for example, enable it to provide you with results faster and better?

P8: That means clarifying the requirement more clearly. For example, if I want it to explain what's inside this function, then I'll say what kind of contract this function belongs to and what it does. Sometimes I also need it to explain what this function is for, then help me explain its purpose, and also explain the variables and their meanings. Such requirements will be put forward in more detail when raised.

Interviewer: Will you use it when you write your report?

P8: Yes, it will.

Interviewer: How do you generally use it?

P8: When I write a report, I can only describe what comes to mind in words, then ask it to help polish it up a bit, and then help with the translation. It will describe things more clearly.

Interviewer: During the learning process, how did you interact with it to assist your learning?

P8: For example, when trying to understand an economic model, since its database may have been updated some time ago, but some economic models have been around for a long time, then some known economic models will be used, and then questions will be asked, such as about a loan or a token, and it will be queried from its known database. If there is really no updated version available, then other methods will be considered.

Interviewer: Do you think the current ChatGPT has been helpful to you, and are you satisfied with its assistance? Or, how many points would you give it for its capabilities, specifically its capabilities in code auditing?

P8: Score 8 or 9 points.

Interviewer: The full score is 10 points?

P8: Right.

Interviewer: Where do you think the eight or nine out of ten mainly come from?

P8: Mainly from two aspects. One is in terms of explanation, that is, it can explain functions very clearly, and also explain what they are used for very clearly. This will be very helpful. Also, for example, if I think there is a problem with it, I can give feedback, and it will adjust its subsequent output based on my feedback, which is also very convenient. Another aspect is that in terms of text description, it can also play a significant role when writing reports.

Interviewer: Where do you think the dissatisfaction lies? Where are the remaining 1-2 points?

P8: Actually, I think there will still be some special situations during the audit, and that's exactly why manual work exists. That is to say, in some cases, when making a judgment, it may seem that there is a problem, but in fact it may not be a problem; it just points out a suspicious point and is not that precise, like this.

Interviewer: Anyway, it's error-prone, right? You'll also verify it.

P8: It's not exactly wrong; the range it provides is relatively larger. In this case, while on one hand it helps us rule out many things, on the other hand it requires us to verify more things.

Interviewer: Do you have any way, have you adopted any methods to reduce it, for example, narrow down the scope?

P8: If I narrow it down, I'll ask questions and also tell it that I think this is because of something, so I don't think this is a bug. I'll give it feedback like this, and maybe it will get better, much better, later on.

Interviewer: Do you often ask it questions like this and then let it give you better results as much as possible?

P8: Yes.

Interviewer: Besides this, do you think there are any other areas where it could do better?

P8: If we want to do better, considering the context, I think it has actually taken the context into account quite clearly. However, after all, some things can be very complex, such as the dependencies between contracts, which may be a bit more difficult. But I still hope that we can take the context into account and consider it again.

Interviewer: Based on the context, does providing it with more code enable it to better integrate the context and then...

P8: I haven't tried it yet, because providing more code would mean providing more contracts, which might be a bit messy. I haven't tried this.

Interviewer: Are there any other areas you think could be improved?

P8: There are no other items for now.

Interviewer: Currently, we plan to propose a new platform or tool based on ChatGPT that can assist in code auditing. So, what features do you most hope it to have?

P8: That's the context just mentioned. For example, Solidity has many versions, and different versions may actually have vulnerabilities or bugs. We hope to understand the situation and state of each version, and take this into account in the contract. That is to say, because there are some issues in this version, the contract may have such vulnerabilities, and we hope to be more precise in terms of the version.

Interviewer: So it means that different versions can cause some vulnerabilities, right? If the version is incorrect, then vulnerabilities will appear here.

P8: Actually, it's not that the version is incorrect. Let me give an example. If the version is below 8.0, it does not have overflow protection for calculations. Then, we hope that based on this version, we can determine whether overflow protection needs to be checked. If it is above 0.8.0, then we don't need to consider the overflow vulnerability. If it is below 0.8.0, we hope to point out this, that is, for the corresponding version, whether there are any issues, and then consider them accordingly, rather than considering all versions.

Interviewer: Are there any other customized features? For example, can it help you learn?

P8: If learning, it's okay to learn. It will summarize what its functions are based on the current contract, then stop looking at some existing projects, and directly summarize what this project does, what functions it has, and what model it uses.

Interviewer: You just said not to look at what already exists. What does that mean?

P8: Just analyze this project and see what type of project it is. Now it's basically the same.

Interviewer: That's all my questions. Thank you.