P = Participant

I = Interviewer

I

All right. So quick info before: please be honest. If you think something is bad, just tell me, that's completely fine. I just want to know what you actually think about the things. Also, I'm not sure if you noticed, but there were some errors in the things that I gave you in the documents. It was not -- so the thing is, it was not the tool that we want to investigate here. There was the input data -- the model that the rule checking thing works on had some errors in there. If you didn't notice, it's fine. Just, you know. All right, as a first easy question, could you tell me your job description, please?

P

Yeah, technically I'm a student and interning at [company]. Well, probably the most correct description is full stack developer. So we kind of thought everything related to software development. Yeah, and I'm definitely not so good in AI security. So I'm not a security expert. And also I'm not good familiar with Spring, so it was a difficulty for me.

I

Yeah, I understand. That's completely fine. So can you put it into years? How many years of software engineering experience do you have?

P

Yes, so I work here about half a year ago. And before that, I went to -- currently I'm at the uni. So I have my bachelor's degree, and I have about half a year left from my master's degree.

I

Okay, so like five years?

P

Four or five years, yes.

I

Four or five years, all right. And any security analysis experience, or…?

P

No, this was my first.

I

Very first, okay. Ah, good to know. Okay, so if we go into what you did on Monday, you had two tasks that you did manually first, and then two tasks where you had the tool output directly, right? Can you compare this? How was it for you? Was it easier manually? Was it easier with the output?

P

It was definitely easier for me to do with the output to me. Because of the lack of my knowledge about the topic. But manually, I tried to search for keywords like in the first text for authentication / authorization, and some research on the web after. So I was trying to look for keywords that could suggest if this endpoint is authenticated or not. More or less I could do that. But with the tool, I was more confident with my own results as well. So it was really helpful in that. So without any prior knowledge, I was more confident to… “yes, I was on the right path”. Not so sure if I got the correct conclusion, but I think my path was correct until a certain point, for sure.

I

OK, all right. In terms of time, do you think it was faster when you had the output?

P

Definitely faster, since it has these links with source code. So it was faster with the tool.

I

Okay, all right. What exactly did you do with the output? How exactly did you use it?

P

Well, first I understood the output. So each part means what in the output and how the after parts are connected to the previous block. And after -- basically, I checked that if those nodes or edges that the tool suggested. What did they do, as I could. And technically, I sort of validated in my head, the top two. So I...

I

What do you mean? So you checked if the tool output is correct? Or what did you...

P

Yeah, I tried to do that, so...

I

Oh, okay. Yeah.

P

So it's yeah, so I try to validate it with my knowledge. Yeah.

I

Okay. All right. So just to summarize, you actually went through the steps and tried to understand the process in the output.

P

Yes, yes

I

Okay, all right. Would you say that you trust the output - the document that I gave you?

P

Yeah, I think that in that way I can trust it if that it shows it was correct, I think. But I couldn't check that if it's a full truth. So I couldn't check that if it's missed out something.

I

Yeah, of course. That's hard.

P

Yeah.

I

Did it get -- did you trust it more at the end? So you did four tasks, right?

P

Yeah, definitely. It was. Yeah.

I

Were there specific things in there that looked a bit fishy to you or you thought “something's wrong” or were there specific parts that you trusted, where you thought “okay, this is definitely true”?

P

Maybe that was some kind of fishy for me in the first task... I'm gonna check it...

I

Yeah, sure.

P

Okay, if I can find the documents, but... Okay, yes. Yeah, I think… which was not fishy, more like strange to me in the first task it's the entry points. So it's maybe because of my less knowledge about the topic and about Spring, but I thought there will be more entry points than just the API gateway. But after I digged into a little bit deeper and properly read the README and like this, I could believe that only the API gateway is the only entry point. Yeah, but there I was a little bit confused.

I

Okay, okay. Yeah, that was actually one of the errors in the model. So you're right. It's I think “Eureka server” and “Zipkin tracing”. These can also be accessed. So it was... your suspicion was correct. All right. So if we assume that everything is correct, would you still have any suggestions how we could improve this? So how you would trust it more or let us see that things are correct or not?

P

So I think it can be seen pretty confident and it can be very trustworthy in a way as it is now. But I think what a good upgrade is to the output could be more human readable. I don't know what's the plans about that. But now it can be read. But as you first look at it, it could be confusing.

I

Okay, so one note on this: of course, this is a prototype. It's a ()?, right? But still, if we think about the structure, this step by step and listing all nodes and so on. This is confusing for you?

P

At first, it was a little bit confusing. So what exactly the included / excluded meant in the decision column and what was brought to the next step. And it's the first look and after about half a -- minute and a half I was getting “Oh, yeah, so that's for that only part statement”. And so it could be read by human. But first, yeah, the first look, it was a little bit confusing for me. I don't know what could be a good step to make it more human readable. Just right now what…? Yeah, maybe… I don't know.

I

Okay. Yeah, that's fine. But yeah, good feedback already. You don't have to come up with a solution. Okay, so this was the evidence that is listed. What about the links to GitHub? Did you use them a lot?

P

I use them and there I was about to... so some of the things were very useful and bring towards certain points in the code, which was “oh yeah, so that's why it is a decision”, but sometimes it was pretty strange for me. So “why here?” Or what does it prove about those exact flag or something?

I

Okay, okay. So what was missing? Was it your knowledge about Spring? Or do you think...?

P

Probably my knowledge about Spring. I think that, who -- I don't know in which task, but something about -- yeah, in where it was about the ribbon package. I think it was Ribbon package -- the link pointed toward the YAML file, I think, or something like that. And first I was sitting there “why here? Why does it relevant for the question?” And after I searched what is Ribbon and what does it do exactly, I could understand it and say “oh, yeah, so probably that's fine because the tool finds it and it uses it. So probably it uses its feature as well”.

I

Okay. I’m trying to think how we can improve this, but yeah. It's good to know.

P

Maybe some explanation could go with -- so... one sentence about.. yeah “it's because Ribbon is a package, which does like that”.

I

Yeah, probably that would help. A short explanation for each of them. Okay, all right. So you didn't write the rules your own, but they're written on the top, right? Of the files always, the statement. Without trying it out, do you think -- do you understand the queries? Is it readable? Do you understand what they check?

P

Yeah, I think the queries, I think it's pretty well readable, even the longer one in the fourth rule, that's a little bit longer to understand, but that was also not ()? the one. I don't know which one was the very one. That was also okay, readable and understandable.

I

Yeah. Just by looking at it, do you think you would be able to write these your own? If I give you a short introduction, of course.

P

Yeah, I think it can be done.

I

Okay, nice. All right. Now you don't really do security analysis, so this question might be strange for you, but still: do you think you could, you would use such a tool in your job, assuming that you do security analysis?

P

Yes, I would use tools like this, even for security analysis, if I had to solve for a little task, I need to test or check if my product is correctly defended. I could use something like this, and I could trust the output “if I go there, you should do some modifications”. Yeah, so I think I could use it, and I would use tools like this. And maybe -- I don't know how big of a work would it be -- to not just to specify for security, but other territories I think it could be very helpful.

I

Do you have an example? So what could you use it for?

P

I think maybe to map out a database, I think this could have, I'm not exactly like this, but the map out also to map out the joins and like this.

I

Okay, I see. All right. Now that's good, good suggestion. All right, I'm already through with my questions. Do you have anything to add? Anything we didn't talk about? Conclusive statement about everything?

P

[SHAKING HEAD]

I

All right. In that case, thanks a lot for your time. That was really helpful. I appreciate it.

P

Yeah.

I

I'll tell [name] if there are any news about this. Maybe you can use it.

P

Yes.

I

All right. Thanks a lot. And have a nice day.

P

Have a nice day, bye.

I

Bye.