P = Participant

I = Interviewer

I

So quickly before: first of all, please be honest. So if you didn't like anything, just tell me. That's better than just hearing everything that's good.

P

Yeah, okay.

I

And also, unfortunately there were some errors in the output I gave you. It was the input data. The model that this tool works on, there were errors in it, which is quite annoying, but it's the way it is. Maybe when you answer your tasks, maybe keep this in mind, we'll see, answer your, what else()?

All right. So as a little background, could you tell me your job description?

P

Yes, I work here as an intern. So I'm not that experienced. I've been working as a software engineer for about half a year.

I

Okay. So all in all, how many years of software development experience do you have?

P

In working field, a bit more than half a year, I'm finishing my bachelor's degree.

I

Okay. So then like three years or something together with the studies?

P

Yes.

I

All right. Okay. And do you have any security analysis experience?

P

Not really.

I

Okay.

P

So yeah, I'm quite new for this Spring and microservices environment.

I

Yeah, that's good to know.

P

Yes.

I

Good to have someone like you as well, someone that is not this experienced. It's good insights. So let's have a look at what you did. So you did two tasks manually first and then two tasks directly with the tool output. If you compare this, was it easier when you did it manually or when you had the output directly? Do you think it was faster one of the ways?

P

Like when I did manually, I mainly looked for the annotations and I had to Google them what they exactly do because I don't really know about these security annotations. So that's really helpful that --yeah after the query, it points exactly to that exact line of code that it does something. So doing it by myself, it will have taken much longer. Like, the exposure is not really clear for me. What did the exposure in the first task?

I

Yeah. The entry point, you mean?

P

Yes, yeah.

I

Yeah, I've heard this from the others as well that some things were just… didn't know what it means. That's good to know. So-

P

Yeah, I don't have that much experience. So, finding them wasn't easy for me.

I

Okay. Yeah, it's not just your experience. It's also that we could explain some things better. So, it's not only you who had the problem. But okay, that's good to know. So how exactly did you use the file that I gave you? What exactly did you do with it?

P

I checked all the links that I found... a couple. And it showed that snippet. And for example, with the annotations, I checked what they do. And basically that's what I did. But I noticed there are, there are these tags which do not have a code snippets.

I

That's true. Okay, so would you say that you trusted what I gave you... the evidence?

P

Yep, to me it seems pretty convincing. So for example, everywhere where I clicked on the authorization, it always showed me that exact code of line. So yeah, the... maybe what's harder to know it, that it misses something. But that's even more difficult to spot as a person.

I

Yeah, I understand. And when the tool pointed you to -for example- these annotations that you look at now, did you double check? So did you Google that annotation, for example, like you did when you did it manually? Or did you just see “okay, this is the annotation” and then you believed it? Did you double check?

P

I think I just... I only checked one, but after then I believed it.

I

Okay, all right. Okay, good. So over the course of the session, of the four tasks, did you trust it more? So did you trust the tool output more at the end than in the beginning?

P

Yes.

I

All right. That's good. Do you think there's anything missing or would anything help you further that we can put in there?

P

I can't think of it right now.

I

Okay, that's fine. So now we're talking about this linking back to code, but if you just look at just the document that I gave you, this step-by-step listing of the single steps and listing all the nodes included, excluded, and so on - so just the structure of the document. What do you think of that? Does it help? Do you understand it directly?

P

The only thing which took me a bit of time is what's the reason something is being included or excluded. The steps are pretty understandable.

I

Okay.

P

I think sometimes it wasn't visible initially that why something was included or excluded.

I

Yeah, okay. So just very practically, do you have an idea how we could do this? Would you put like colour behind - I don't know -- if you don't know why it was included, it's hard to answer for you. Okay, that doesn't matter. We'll have to think of something.

P

Yes.

I

All right. So just real quick: as an intern, what do you do? Do you do software development?

P

Yes.

I

So your daily work is development basically?

P

Yes.

I

Yeah, okay. So I don't know if this question applies, but I still ask you: do you think you would use such a tool in your job or is it just not your field of working?

P

Maybe it's not my field yet, but one day.

I

Okay.

P

If I would be more knowledgeable, then sure.

I

All right. So of course then we have to expect -- we have to assume that we have a proper UI and everything, not this crappy HTML. What do you think, what you could use it for? How would you integrate it into your job?

P

Maybe if a bigger team was working on a bigger project, it would be pretty useful even for security measures or even to just get an overview on the application.

I

Yeah, okay. So for this overview, for getting to know an application that you haven't looked at before, do you think it's good for this? Do you think this helps you starting to analyze an application?

P

Yeah, I think getting the edges and the entry points are very useful.

I

Okay. All right.

P

Because it shows the code exactly.

I

Okay. Now, you didn't write the queries on your own, of course. I gave them to you, but they're written on the top, right? Do you understand them? Do you think they're self-explanatory?

P

Yes, they're pretty self-explanatory.

I

All right. Hypothetical question, but do you think you could write them your own? If I tell you what the language looks like, do you think it's easy to write them?

P

If I see an example, then yes.

I

All right. That's good to know. Okay, that was all I wanted to ask already. Do you have anything to add? Anything conclusive, feedback...

P

[SHAKING HEAD]

I

All right. Okay, in that case, thanks a lot for your time. I'm happy that we don't only have security experts in here, but also someone that's not so familiar. That's pretty good. Thanks a lot for that.

P

Thank you very much.

I

Yeah. Have a nice day.

P

All right. See you.