P = Participant

I = Interviewer

I

So, first a short explanation before: there were some issues in the model that you worked on. Maybe you noticed, I don't remember what exactly you wrote. The tool output that I gave you wasn't exactly correct. The problem is that this was not an issue with the tool, it was with the input data, the model that the tool works on. It's a bit annoying. I don't know, maybe you can keep this in mind when you answer, but we'll see, that's fine. Also, just one note: please be honest. If you didn't like anything, just tell me, I want to have correct feedback. Okay. As a start, could you tell me your job description first?

P

Okay, I work as a security researcher and I work at [company] for 15 years.

I

Okay.

P

So I have evaluations mainly for embedded devices, such as mobile phones, laptop boxes, computers and so on. But in the recent years, we have some evaluations of websites and applications also. And I have a little developer background also.

I

Okay. Could you put that in years?

P

…not in Java.

I

Okay.

P

Mainly in C++

I

All right. Can you tell it in years? How many years of software analysis experience do you have? And how many years software development?

P

Okay, so software development is about five years. And evaluation 15.

I

Okay, good to know, thanks. So let's have a look at the analysis on Monday. So you performed two tasks manually first and then you had the tool output and two tasks with the output directly. Was it easier for you to do it in either of these settings?

P

Yes, maybe with tool output it was easier because I can find quicker the relevant parts but in this case, I have also have to look at the major context of the first code and the config files. So I have to do all of the same task which I prepare from during the manual analysis. It was fine that I see all of the entrypoints which I have to look at.

I

Okay. So was it a bit quicker when you had the tool output, time-wise, do you think you were faster?

P

I don't know. It is not... the tasks very different, so...

I

Yeah, that's true. So then how exactly did you use the tool output that I gave you? What exactly did you do with it?

P

Mainly I checked the evidence (classes)?. So, I think it was the main part -- most important part for me. And it was a little bit annoying that some of the evidences were missing. There are some where "authorization" contains evidence (papers)? and a lot of which didn't contain. Besides, you don't know why it was marked as “authorized”, because there wasn't any evidence for it.

I

Okay, I see. Yeah, I've heard that from the others as well. It's funny, you all think the same thing basically. So, would you say that you trusted the tool output that I gave you?

P

Yes, I can trust it. But maybe the DFD model wasn't -- it was different from what I think. For example, there was the “external entities should check…” and there was two entities which I think that it's an external entity, but it wasn't marked as external entity in the DFD model.

I

Yeah, okay. I see. So, did you trust in the tool change over the four tasks that you did? Did it decrease because you found the errors, or did it increase because you got more familiar with it?

P

It's increased, I think. Because I saw that the model is good behind it, then the tool output is correct.

I

Okay, okay, good. Is there anything… do you have any idea how we could improve the trust. So you already said that some of the annotations did not have the link to GitHub?

P

Yeah.

I

Okay.

P

I think it would be better if I see the model.

I

Okay.

P

...with the initial...

[…]

I

OK. So now we're talking about the linking to GitHub. But if you think about just the document that I gave you -so this listing of the step-by-step evidence- was this clear to you? Did you understand everything?

P

It was clear.

I

OK.

P

I like this structure.

I

OK, that's good. Nice to hear.

P

I wouldn't use this... terminal-like... --

I

Yeah. It's a prototype.

[LAUGHTER]

I

Yeah, of course we would like to have a nice UI with it, but… maybe later. But, like I said, the structure was clear to you, that's already good. Was there anything missing? So you said the traceability for all the links, but any content missing?

P

Actually, I'm not a Java Spring expert, so I'm not sure about it, but maybe in some cases, not just one line can be an evidence, but more lines.

I

Yeah, I see. Yeah, that's true of course, for some cases that's true. So you didn't write the queries on the model, of course, I gave them to you, but you saw them in the beginning, right? The statement where I wrote the -- do you have it in mind?

P

[NODDING]

I

The language behind it, do you think you would understand it easily? Did you understand the components? Is it --

P

Yes.

I

Okay. Do you think it would be easy for you to write such queries on your own?

P

I think yes, but it requires a little bit of practice.

I

Of course, I would have to explain it to you...

P

Yeah, it doesn't seem to be too difficult.

I

Okay, good. So when you read the query, do you understand in natural language what the rule behind it is? What is checked with the query?

P

[NODDING]

I

All right. Now, a bit away from last Monday, do you think you would use such a tool -if we have a nice UI and so on- do you think you would use such a tool in your job?

P

I think yes. But I think in case if I have to analyze a lot of DFDs. So for one DFD I don't think that I would want to learn syntax and every single... to use it, but to analyze more of them, then it would work.

I

Okay. But if you, let's say you always have a DFD for the applications that -or the website- whatever you're analyzing. So if we have an automatic DFD extraction, then you always have a DFD. Would you use it in that case? So if it's always possible to use it, would you use it?

P

Yes. Because it can improve the speed of finding every annotation and every entrypoint and so on, It should ()? to our work

I

Okay.

P

None of our evaluation projects contain DFD.

I

Yeah, that's true. So how would you use it? You say that… to look around. Yes, so do you have in mind how exactly you would use it?

P

Yes, I will use it to get a... for example, entry points, connections and so on. And I have to check one by one manually - with which the evidences can help… is that they point… move me to the right place where I can check it.

I

Okay. Are there specific tasks that you think it is more useful for? So, let's say more for simple analysis, just finding specific things, or more for complex things like the-- if we talk about the connections between the nodes and properties of these connections. So do you think it's better for just simple things, finding something, or also for more complex things working together? Any difference in your mind?

P

No, I don't know any other components. But, maybe it's useful for it, just I don't see.

I

OK, all right. OK, I'm actually already through my questions. One last question. Basically, is there anything else you would like to add, anything that I didn't ask?

P

No, I don't think.

I

All right. OK, in that case, thanks a lot for your time. That was good insight. And yeah, via [name], I will let you know if something happens with this.

P

Thank you.

I

Yeah, thanks a lot for participating. All right. Have a nice day. Bye bye.