Demographics

Hello!

Welcome to our study on "Assessing the interpretability of vulnerability reports". This survey is part of a research study (STUDY2024_00000346) conducted by X and Y (email_address) at Z University.

Thank you for taking the time to participate in our survey. Your responses are important to our research.
While some questions are open-ended to allow you to express your thoughts freely, **please refrain from providing any personal or personally identifiable information about yourself or others, unless specifically requested.**

Contacts: If you have any questions, please contact X.

How old are you?

- ○ 18-24
- ○ 25-34
- ○ 35-44
- ○ 45-54
- ○ > 55
- ○ I prefer not to say

For data management purposes, where are you located?

- ○ Europe
- ○ United States of America
- ○ Other

Past experience

How many years of experience do you have running and analyzing vulnerability scans/reports?

- ○ Less than 1 year of experience
- ○ 1-5 years of experience
- ○ 5-10 years of experience
- ○ More than 10 years of experience
- ○ I have never run or analyzed a vulnerability scan or report.

How many hours per week do you spend running and analyzing vulnerability scans/reports?

- ○ Less than 5 hours per week
- ○ Between 5 to 10 hours per week
- ○ More than 10 hours per week

How confident are you in your ability to identify software vulnerabilities (either using auxiliary tools or doing it manually)?

- ○ Not confident
- ○ Neutral
- ○ Confident

In which context(s) have you found security vulnerabilities?

- ☐ Bug bounty programs (e.g. sell specific vulnerabilities to a vendor)
- ☐ General software testing (e.g. static or dynamic analysis)
- ☐ Penetration testing
- ☐ Vulnerability discover exercises (e.g. Capture the Flag, school courses)

☐ Other

☐ Never found a vulnerability before

Which tools have you used in the past?

	I have used it	I have never used it
Infer	○	○
CodeQL	○	○
joern	○	○
AmazonQ	○	○

List any additional vulnerability detection tools you use. If you don't remember any or have not used any, leave the field blank.

Would you use AI assistants (e.g. ChatGPT) to discover security vulnerabilities? Why or why not?

Study introduction

In the upcoming exercises, you will work with **three types of security reports.**

The **complexity of the code samples and vulnerability types are similar across tasks** but the reports will be

different.

You will use our Github credentials and use GitHub Codespaces for this study, which includes all the necessary data and provides a consistent environment for interacting with the reports and modifying code.

Please keep this questionnaire open to answer questions as you go.
[**Make sure you have access to Codespaces before moving forward!**]

Task 1

Welcome to Task 1!
Please, read the README file in the Github Codespace and then proceed to answer the questions below.

Note that:
1. Reports may not be 100% correct.
2. There is always a vulnerability in code.

Based on the report, what is the vulnerability in the code?

Do you agree or do not agree with the vulnerability described in the report?

- ○ Yes, I agree.

- ○ No, I do not agree because...
- ○ I am not sure.

Based on the report, what is the severity level of the vulnerability?

Do you agree or do not agree with the level of severity described in the report?

- ○ No, I do not agree because...
- ○ Yes, I agree.
- ○ I am not sure.

Based on the report, where is the vulnerability located?

Do you agree or do not agree with the location of the vulnerability described in the report?

- ○ No, I do not agree because...

- ○ Yes, I agree.
- ○ I am not sure.

Please, assume the report is completely correct.

From Strongly Disagree to Strongly Agree, answer the following questions regarding perceived interpretability of the report results.

	Strongly Disagree	Disagree	Agree	Strongly Agree
The report helps me identifying the vulnerabilities in the code.	○	○	○	○
The report helps me understanding why the code is vulnerable.	○	○	○	○
The report helps me locating the vulnerability in the code.	○	○	○	○
The report provides the necessary information to effectively address the vulnerability.	○	○	○	○
Navigating the report to find relevant information is straightforward and intuitive.	○	○	○	○
The report provides context-specific information helpful to understand the cause of the vulnerability.	○	○	○	○
The report provides context-specific information helpful for addressing and fixing the vulnerability.	○	○	○	○
The report provides context-specific information helpful for understanding code flow.	○	○	○	○

Using the information provided in the report and your knowledge, please **generate an appropriate code patch/code fix that removes the vulnerability** from the codebase. You can compile and test the code at your convenience. Please, try to preserve method signature (i.e. method name, arguments and return types) as much as possible.

Please, make the necessary changes in Github Codespaces. Then, copy and paste the FULL code here (not just the patch).

Task 2

Welcome to Task 2!

Note that:
1. Reports may not be 100% correct.
2. There is always a vulnerability in code.

Based on the report, what is the vulnerability in the code?

Do you agree or do not agree with the vulnerability described in the report?

- ○ Yes, I agree.

- ○ No, I do not agree because...
- ○ I am not sure.

Based on the report, what is the severity level of the vulnerability?

Do you agree or do not agree with the level of severity described in the report?

- ○ No, I do not agree because...
- ○ Yes, I agree.
- ○ I am not sure.

Based on the report, where is the vulnerability located?

Do you agree or do not agree with the location of the vulnerability described in the report?

- ○ No, I do not agree because...

- ○ Yes, I agree.
- ○ I am not sure.

Please, assume the report is completely correct.

From Strongly Disagree to Strongly Agree, answer the following questions regarding perceived interpretability of the report results.

	Strongly Disagree	Disagree	Agree	Strongly Agree
The report helps me identifying the vulnerabilities in the code.	○	○	○	○
The report helps me understanding why the code is vulnerable.	○	○	○	○
The report helps me locating the vulnerability in the code.	○	○	○	○
The report provides the necessary information to effectively address the vulnerability.	○	○	○	○
Navigating the report to find relevant information is straightforward and intuitive.	○	○	○	○
The report provides context-specific information helpful to understand the cause of the vulnerability.	○	○	○	○
The report provides context-specific information helpful for addressing and fixing the vulnerability.	○	○	○	○
The report provides context-specific information helpful for understanding code flow.	○	○	○	○

Using the information provided in the report and your knowledge, please **generate an appropriate code patch/code fix that removes the vulnerability** from the codebase. You can compile and test the code at your convenience. Please, try to preserve method signature (i.e. method name, arguments and return types) as much as possible.

Please, make the necessary changes in Github Codespaces. Then, copy and paste the FULL code here (not just the patch).

Task 3

Welcome to Task 3!

Note that:
1. Reports may not be 100% correct.
2. There is always a vulnerability in code.

Based on the report, what is the vulnerability in the code?

Do you agree or do not agree with the vulnerability described in the report?

- ○ Yes, I agree.

- ○ No, I do not agree because...
- ○ I am not sure.

Based on the report, what is the severity level of the vulnerability?

Do you agree or do not agree with the level of severity described in the report?

- ○ No, I do not agree because...
- ○ Yes, I agree.
- ○ I am not sure.

Based on the report, where is the vulnerability located?

Do you agree or do not agree with the location of the vulnerability described in the report?

- ○ No, I do not agree because...

- ○ Yes, I agree.
- ○ I am not sure.

Please, assume the report is completely correct.

From Strongly Disagree to Strongly Agree, answer the following questions regarding perceived interpretability of the report results.

	Strongly Disagree	Disagree	Agree	Strongly Agree
The report helps me identifying the vulnerabilities in the code.	○	○	○	○
The report helps me understanding why the code is vulnerable.	○	○	○	○
The report helps me locating the vulnerability in the code.	○	○	○	○
The report provides the necessary information to effectively address the vulnerability.	○	○	○	○
Navigating the report to find relevant information is straightforward and intuitive.	○	○	○	○
The report provides context-specific information helpful to understand the cause of the vulnerability.	○	○	○	○
The report provides context-specific information helpful for addressing and fixing the vulnerability.	○	○	○	○
The report provides context-specific information helpful for understanding code flow.	○	○	○	○

Using the information provided in the report and your knowledge, please **generate an appropriate code patch/code fix that removes the vulnerability from the codebase.** You can compile and test the code at your convenience. Please, try to preserve method signature (i.e. method name, arguments and return types) as much as possible.

Please, make the necessary changes in Github Codespaces. Then, copy and paste the FULL code here (not just the patch).

Interpretability

This next question is very important to understanding the concept of interpretability in security. Please take your time answering it.
In your own words, what makes a vulnerability detection report interpretable?

Regarding **report interpretability**, order the following reports from Most Interpretable (1) to Least Interpretable (3).

Report from Task 1

Report from Task 2

Report from Task 3

Recall the tasks you have just completed. In your opinion, which of the following attributes facilitates a better understanding of a vulnerability detection report?

	Does not help/facilitate comprehension.	Facilitates/helps comprehension.
Identification of vulnerability type (e.g. "CWE-787")	○	○
Description of the vulnerability type (e.g., "CWE-787 is a software security vulnerability that occurs when the data is written beyond the boundaries.")	○	○
Location of the vulnerability at FILE-level (e.g. "CWE-787 is located in file.c"	○	○
Location of the vulnerability at FUNCTION-level (e.g. "CWE-787 is located in function X")	○	○
Location of the vulnerability at LINE-level (e.g. "CWE-787 is located in line Y")	○	○
Transparency in the process/methodology used for the detection (e.g., "The vulnerability was detected using tool T and the rule Z")	○	○
Severity (e.g. Low/Medium/High)	○	○
Identification of code sources and code sinks.	○	○
Code fix/patch suggestion.	○	○
Textual explanation for the code fix/patch.	○	○
Code example explaining the vulnerability.	○	○

If you have any additional feedback regarding the tasks and/or reports, please let us know!

Block 7

If you would like to receive a 20$ gift card, please provide the email to where you would like to send the gift card information.