Consent Form

INFORMED CONSENT FORM

RESEARCH PROCEDURES

The purpose of this study is to determine your experience related to software engineering and automated security-focused static analysis tools. If you decide to participate, the study will last about 35-50 minutes during which time you will be asked several background questions regarding your familiarity and experience with such tools. Additionally, you will be asked to give your opinion regarding hypothetical scenarios and situations relating to the performance of the tool and your expectations as a software programmer. We may contact you by email to invite you to participate in a follow-up survey.

RISKS

There are no foreseeable risks for participating in this research.

BENEFITS

There are no benefits to you as a participant other than to further research in cybersecurity and software/application testing.

CONFIDENTIALITY

The data in this study will be confidential. Any information obtained in connection with this study and that can be identified with you will remain confidential and disclosed only with your permission. Your responses in this study will be kept confidential. You will be assigned a code number to protect your identity and all data will be kept secured. If you give us your permission by signing this document, we plan to disclose the results of the

questionnaire in any publication resulting from this user study. The disclosed results will not be personally identifiable.
The de-identified data could be used for future research without additional consent from participants.
The Institutional Review Board (IRB) and Protection of Human Subjects (PHSC) committees that monitor research on human subjects may inspect study records during internal auditing procedures and are required to keep all information confidential.

PARTICIPATION
You must be at least 18 years old to participate.

Your participation is voluntary, and you may withdraw from the study at any time and for any reason. If you decide not to participate or if you withdraw from the study, there is no penalty or loss of benefits to which you are otherwise entitled. There are no costs to you or any other party.

[redacted].

If you decide to participate, you will be entered into a drawing for your choice of a $50 USD Amazon.com gift card compensation upon completion of this user study. We will randomly choose one respondent per 30 complete surveys, and hope to give out 9 Amazon.com gift cards in total. Under the U.S. federal tax law, you may have individual responsibilities for disclosing the dollar value of the incentive received on this study.

CONTACT
This research is being conducted by [redacted] at the [redacted] Questions regarding the rights of research subjects may be directed to [redacted] Committee on the Protection of

[redacted]. The Committee on the Protection of Human Subjects at [redacted] has reviewed and approved the present research (Protocol ID: [redacted]

This research is also being conducted by [redacted] He may be reached at [redacted] for questions or to report a research-related problem. You may contact the [redacted] Institutional Review Board office at [redacted] if you have questions or comments regarding your rights as a participant in the research. This research has been reviewed according to [redacted] procedures governing your participation in this research.

CONSENT

You are welcome to print this page to keep a copy of this form.

YOU ARE MAKING A DECISION WHETHER OR NOT TO PARTICIPATE. YOUR SIGNATURE INDICATES THAT YOU HAVE DECIDED TO PARTICIPATE, HAVING READ THE INFORMATION PROVIDED ABOVE.

[redacted]

Do you consent to these terms?

- ◯ Yes
- ◯ No

END-Survey

Since you have not consented to the survey, the survey will conclude here. Thank you.

desc:background

Section 1 of 3

We will ask several questions about your background. Most of the questions are multiple-choice questions. Questions will explicitly state if you can select multiple choices as answers.

ques:background

Which type of developer/programmer are you?

- ◯ Freelancer
- ◯ Work in a team with others, such as developers, testers, project managers
- ◯ Both (i.e., work as freelancer in free time in addition to being a full time employed)

How would you describe your primary role?

- ◯ Programmer
- ◯ Tester
- ◯ Project Manager
- ◯ Non-Specific

How long have you been in this role?

- ◯ More than 5 years
- ◯ 4-5 years
- ◯ 3-4 years
- ◯ 1-2 years
- ◯ Less than a year

About how many people are there in your team? (Numbers only)

Please select all the languages you regularly use for software/applications development:

- [ ] Java
- [ ] C#
- [ ] Python
- [ ] Kotlin
- [ ] Lua
- [ ] C/C++
- [ ] JavaScript
- [ ] PHP

How often did you release or help release a new version of a software/application over the past two years? Please give your best estimate; if you develop more than one software/application, please answer based on the most frequently updated software/application.

- ○ Never
- ○ Annually
- ○ Quarterly
- ○ Monthly
- ○ More Frequently

How important should each of these be for software/applications in your opinion?

	Extremely important	Very important	Moderately important	Slightly important	Not at all important
Runs on multiple platforms/devices	○	○	○	○	○
Secured against malicious attacks	○	○	○	○	○
Protects Privacy	○	○	○	○	○
Easy to use	○	○	○	○	○
Supports many features	○	○	○	○	○
Runs smoothly	○	○	○	○	○

How important is each of these **in your organization** when it comes to developing software/applications?

	Extremely important	Very important	Moderately important	Slightly important	Not at all important
Runs on multiple platforms / devices	○	○	○	○	○
Secure against malicious attacks	○	○	○	○	○
Protects Privacy	○	○	○	○	○
Easy to use	○	○	○	○	○
Supports many features	○	○	○	○	○
Runs smoothly	○	○	○	○	○

In your opinion, how important is software/applications security for sales?

- ○ Extremely important
- ○ Very important
- ○ Moderately important
- ○ Slightly important
- ○ Not at all important

How knowledgeable do you consider yourself about information and software/applications security?

- ○ Extremely knowledgeable
- ○ Very knowledgeable
- ○ Moderately knowledgeable
- ○ Slightly knowledgeable
- ○ Not knowledgeable at all

Which of the software/application security components are you familiar with or use for security? You can select multiple:

- ☐ Private key based Encryption/Decryption (e.g., AES)
- ☐ Public key based Encryption/Decryption (e.g., RSA)
- ☐ HTTPS / SSL
- ☐ Custom Certificate Authority (CA) Verification, Validation
- ☐ Integrity of Data (e.g., SHA-3 checksum)

How often do you use each of the following techniques for finding security issues in software/applications?

	Every Build	Every Release	Once/Occasionally	Decided Not to Use	Have not considered it
Scanning Code with automatic Code Scanners	○	○	○	○	○
Using a tool for scanning libraries with vulnerabilities	○	○	○	○	○
Code review by someone other than the developers	○	○	○	○	○

	Every Build	Every Release	Once/Occasionally	Decided Not to Use	Have not considered it
Penetration Testing	○	○	○	○	○

How would you describe your reliance on automatic code scanners for finding security issues?

- ○ complete reliance on automated techniques / no manual testing is involved
- ○ both manual and automated testing techniques are applied, with emphasis on automated technique
- ○ both manual and automated testing techniques are applied, with emphasis on manual technique
- ○ complete reliance on manual testing / no automated techniques are relied on

Please provide rationale for your answer to the above question.

desc:familiarity

Section 2 of 3

We will ask about your familiarity with using automated code scanning tools for analyzing software/applications you develop for finding security vulnerabilities or issues. You will be shown several tools from both industry and academia. It is possible to select multiple tools from the list. Moreover, you can also enter the names of tools you have used but is not on the list.

Next, we will ask you about your experience regarding the tools.

ques:experience_tools

Which of the following have you used for automatic code scanning of software/applications for finding security related issues?

You can select multiple, or you can select none to indicate that you have not used any of these tools.

We will then ask about your experience of using your selected tools.

- [ ] Coverity
- [ ] CryptoGuard
- [ ] Xanitizer
- [ ] SpotBugs with FindSecBugs
- [ ] CrySL / CogniCrypt
- [ ] ShiftLeft
- [ ] QArk
- [ ] Github Code Scan With CodeQL
- [ ] Semmle-LGTM Code Scan
- [ ] Others - Please enter name(s), separated by comma(,)

Which of the following do you **currently use** for automatic code scanning for analyzing software/applications?

You can select multiple, or you can select none to indicate that you have not used any of these tools.

- [ ] Coverity
- [ ] CryptoGuard
- [ ] Xanitizer
- [ ] SpotBugs with FindSecBugs
- [ ] CrySL / CogniCrypt
- [ ] ShiftLeft

- [ ] QArk
- [ ] Github Code Scan With CodeQL
- [ ] Semmle-LGTM Code Scan
- [ ] Others - Please enter name(s), separated by comma(,)

ques:tools_used

At what stage do you/your organization generally use **${lm://Field/1}?**

- ◯ During development (e.g., as part of your IDE)
- ◯ In addition to compilation/build process after pushing changes
- ◯ Quality Assurance team uses it after any code change is pushed that may be related to security
- ◯ After quality assurance team checks for functionality
- ◯ other

Based on your personal experience of using **${lm://Field/1}**, how would you rate the reliability of the tool as a security oriented code scanner?

- ◯ Extremely adequate
- ◯ Moderately adequate
- ◯ Slightly adequate
- ◯ Neither adequate nor inadequate
- ◯ Slightly inadequate

Consider the scenario where **${lm://Field/1}** is buggy and is not detecting some of the vulnerabilities in the code base of a software/application you are working with. In that case, how much might the security of the software/application be impacted?

- ◯ A great deal

- ◯ A lot
- ◯ A moderate amount
- ◯ A little
- ◯ None at all

Please provide rationale for your answer to the above question.

desc:tools_issues_acceptance

Section 3 of 3

You will be asked to provide your opinion in real-life scenarios where a developer is trying to bypass/evade security checks performed by static analysis tools for security. You will be shown bare-bone, compilable, and executable code samples written in Java.

Code samples will be described as either **base case** or **variation**. **A base case** means the related code sample is written in the most possible basic way. **A variation** of a base case means that the variation is written using a different syntax, but **performs identically** to the base case.

*All the code samples provided/shown are considered misuse and are considered security vulnerabilities***.**

There will be 7 questions in total in this section.

ques:tools_issues_acceptance

Consider yourself as someone using an automated code scanner for detecting software/application security issues in source code.
Consider the following vulnerable code example as a **base case**:

```
Cipher.getInstance("DES");
```

This statement creates a Cipher object that uses the "DES" algorithm, a vulnerable security algorithm that compromises the confidentiality of data.

5 variations of the same, bad code are shown below. Each of the variations functions identically.

In case the vulnerability detection tool reports the base case, but does not report each variation below, how would you rank the tool in terms of competency?

There are **5 choices** available for each of the variations. Please select the best option that matches your opinion about the competency of a static analysis tool. You may need to scroll across the screen to view all 5 options.

	Extremely competent	Somewhat competent	Neither competent nor incompetent	Sor inco
Cipher.getInstance("des");	○	○	○	
Cipher.getInstance("AES".replace("A","D");	○	○	○	
Cipher.getInstance("DE$S".replace("$","");	○	○	○	
String s = "DES"; Cipher.getInstance(s);	○	○	○	
Cipher.getInstance("des".toUpperCase());	○	○	○	

Consider the following vulnerable implementation of HostnameVerifier instance as **base case**:

```
new HostnameVerifier(){
    @Override
    public boolean verify(String hostname, SSLSession session) {
        return true;
    }
};
```

The above will create a vulnerable instance of the HostnameVerifier interface from the Java SDK. Because it always returns true, it will accept any HTTPS connection certificate presented by any server without verifying the identity of the server. Software/Applications using this approach for verifying hostname will be automatically rejected from marketplaces such as Google App Store since this is insecure.

Consider yourself using an automated code scanner for detecting issues in code.

What would be your opinion regarding the competency of a vulnerability code scanning tool if the tool is **unable to detect** the following **variation** of vulnerable code, even though it successfully reports the above base case?

```
public abstract class ABadHostNameVerifier
    implements HostnameVerifier {}

new ABadHostNameVerifier(){
    @Override
    public boolean verify(String hostname, SSLSession session) {
        return true;
    }
};
```

- ◯ Extremely competent
- ◯ Somewhat competent
- ◯ Neither competent nor incompetent
- ◯ Somewhat incompetent
- ◯ Extremely incompetent

Consider that a vulnerability code scanning tool does not detect the above variation of the base case. How severely do you think it might impact the software/application security?

- ◯ A great deal
- ◯ A lot
- ◯ A moderate amount
- ◯ A little
- ◯ None at all

Please provide rationale for the choice you selected for above question.

```
new HostnameVerifier(){
    @Override
    public boolean verify(String hostname, SSLSession session) {
        return true;
    }
};
```

Similarly, what would be your opinion if a tool is **unable to detect** the following **variation**, even though it successfully reports the **above base case**?

```
public interface ABadHostNameVerifier
    extends HostnameVerifier {}

new ABadHostNameVerifier(){
    public boolean verify(String hostname, SSLSession session) {
        return true;
    }
};
```

- ◯ Extremely competent
- ◯ Somewhat competent
- ◯ Neither competent nor incompetent
- ◯ Somewhat incompetent
- ◯ Extremely incompetent

Consider that a tool does not detect one or more of the above variations of the base case. How severe do you think it might be in terms of security of the software/application?

- ◯ A great deal
- ◯ A lot
- ◯ A moderate amount
- ◯ A little
- ◯ None at all

Please provide rationale for the choice you selected for above question.

desc:residence

In the following sections, we will ask about your country of residence for the purpose of sending an Amazon.com gift card. We will also ask you about your contact information for a chance at winning a lottery and/or participating in a follow-up survey.

Providing contact information for both is completely optional.

Country

In which country do you currently reside/work at?

desc:lottery

To be considered for the Amazon.com Gift Card Lottery, please include your name and email address. At most 9 lucky winners will be chosen based on completed survey responses.

In the case that you win the lottery, we will contact you using the email address you have provided.

Rest assured that your name and email address will not be shared or published anywhere else.

Your Name

Your Email Address

desc:survey_followup

We may contact some participants for a follow-up survey later based on complete responses. Furthermore, the participants of the follow-up survey will be compensated separately.

Would you be interested in participating in such a survey? Your interest in participating in such a survey will in no way affect your chance of winning the lottery.

If you are interested to be considered for such a survey, please provide your email address so that we may contact you.

Your email address

Powered by Qualtrics