Developer Confidence in Smart Contract Security Analysis Tools

Thank you for considering participation in our research study. We are exploring how smart contract developers perceive existing security analysis tools, especially in terms of how clearly these tools explain their findings. Your participation will help us identify challenges and opportunities to develop more informative and trustworthy analyzers for smart contract security.

- The survey takes **25–30 minutes** and asks about your experience with smart contract development and your perspective on the clarity of explanations provided by security analyzers.
- Your responses will be **completely anonymous**. We do not collect personally identifiable information, and any quotes that we may use in publications or reports will not be linked to you.
- This study has been approved by the **Institutional Review Board (IRB)** at *** (Study ID: HRPP-***-3).

If you have any questions, you may contact the principal investigator, ***.

* Indicates required question

1. **What is your role in the smart contract development process?** *

Check all that apply.

- [ ] Smart Contract / Blockchain Developer
- [ ] Security Reviewer / Smart Contract Auditor
- [ ] Quality Assurance (QA) / Tester
- [ ] Technical Architect / Project Manager
- [ ] Researcher / Concept Developer / Student
- [ ] Not applicable / No involvement
- [ ] Other: _____

2. **How many years of experience do you have with smart contract development?** *

Mark only one oval.

- ◯ Less than 1 year
- ◯ 1–2 years
- ◯ 3–5 years
- ◯ More than 5 years

3. **Which programming languages do you primarily use for smart contract development?** *
(Select all that apply)

Check all that apply.

- ☐ Solidity
- ☐ Vyper
- ☐ Rust
- ☐ Michelson
- ☐ Move
- ☐ Plutus
- ☐ JavaScript
- ☐ C++
- ☐ Go
- ☐ Other: _____

4. **What type of smart contract projects are you primarily involved in?** * *(Select all that apply)*

Check all that apply.

- [ ] DeFi platforms (e.g., decentralized exchanges, lending protocols)
- [ ] NFT projects (e.g., digital collectibles, marketplaces)
- [ ] Enterprise blockchain solutions (e.g., supply chain, identity management)
- [ ] Decentralized applications (DApps) or Web3 platforms (e.g., backend smart contracts, decentralized infrastructure)
- [ ] Frontend integrations for Web3 (e.g., wallet connections, UI/UX for DApps)
- [ ] Other: _____

5. **How important is security and safety in your smart contract development process?** *

Mark only one oval.

- ◯ Extremely high
- ◯ High
- ◯ Moderate
- ◯ Low
- ◯ Not a priority

6. **Which of the following smart contract security vulnerabilities are you familiar with?** *
(Select all that apply)

Check all that apply.

- [ ] Reentrancy attacks
- [ ] Improper access control (Parity Wallet Hack_1)
- [ ] Suicidal contracts (Parity Wallet Hack_2)
- [ ] Integer overflow/underflow
- [ ] Unchecked external calls
- [ ] Front-running
- [ ] Denial of Service (DoS) attacks
- [ ] Timestamp dependence
- [ ] Flash loan attacks
- [ ] Honeypot
- [ ] Greedy Contract
- [ ] Gas limit vulnerabilities
- [ ] Logic errors
- [ ] Oracle manipulation
- [ ] Other: _____

Usage of Security Analyzers

This section looks at how you use security analyzers during smart contract development — including how often, at what stages, and why.

7. **Which security analyzers have you used during smart contract development?** *
Please list all tools you've used — including any you currently rely on or have used in the past.

_____

8. **How frequently do you use security analyzers when developing smart contracts?** *

Please select the option that best describes the proportion of smart contracts for which you use these tools.

Mark only one oval.

- ◯ Not at all
- ◯ For less than 25% of contracts
- ◯ For 25–50% of contracts
- ◯ For 50–75% of contracts
- ◯ For 75–99% of contracts
- ◯ For all contracts

9. **At which stages of development do you typically use security analyzers?** *

(Select all that apply)

Check all that apply.

- ☐ During initial development / coding
- ☐ During unit or integration testing
- ☐ During the security audit phase
- ☐ After deployment (e.g., production monitoring)
- ☐ Other: _____

10. **What are your main reasons for using security analyzers?** *

(Select all that apply)

Check all that apply.

- ☐ To identify vulnerabilities
- ☐ To ensure code quality
- ☐ To comply with organizational or regulatory policies
- ☐ To learn about potential security issues
- ☐ Other: _____

11. **Which type of interface do you prefer for using a security analyzer?** *

Mark only one oval.

- ◯ Desktop application
- ◯ Web-based tool
- ◯ Command-line interface (CLI)
- ◯ IDE plugin (e.g., VS Code extension)
- ◯ Other: _____

12. **What type of input do you typically analyze with a security analyzer?** *

Mark only one oval.

- ◯ A single contract or transaction
- ◯ Multiple contracts or transactions
- ◯ Large datasets of contracts or transactions
- ◯ Other: _____

13. **What is your preferred pricing model for a security analyzer?** *

Mark only one oval.

- ◯ Free
- ◯ Freemium (free with paid features)
- ◯ Paid subscription
- ◯ One-time purchase

14. **What is the longest amount of time you would typically allow a security analyzer to run before expecting results?** *
(i.e., if you could set a timeout, what would it be?)

Mark only one oval.

- Less than 1 minute
- 1–5 minutes
- 5–10 minutes
- 10–30 minutes
- 30–60 minutes
- More than 60 minutes

15. **On average, how much time do you spend verifying whether a reported vulnerability is a true positive?** *
(i.e., confirming that it reflects a real issue)

Mark only one oval.

- Less than 5 minutes
- 5–15 minutes
- 15–30 minutes
- 30–60 minutes
- More than 60 minutes
- I do not verify

Confidence in Security Analyzer Outputs

This section explores what influences your trust in the results provided by security analyzers — especially when it comes to reported vulnerabilities.

16. **How confident are you in the accuracy of vulnerabilities reported by security analyzers?** *

Mark only one oval.

- ◯ Fully confident — I trust the results without additional verification
- ◯ Confident — but I verify critical findings manually
- ◯ Somewhat confident — I perform significant manual review
- ◯ Not confident at all

17. **Which of the following factors increase your confidence in a security analyzer's results?** *
(Select all that apply)

Check all that apply.

- ☐ The analyzer is well-known and reputable
- ☐ The analyzer provides detailed explanations for each reported vulnerability
- ☐ The analyzer has a low false positive rate
- ☐ The analyzer is regularly updated
- ☐ The analyzer is open-source
- ☐ I've had positive past experiences with the analyzer
- ☐ I've received recommendations from peers
- ☐ Other: _____

18. **Which of the following factors reduce your confidence in a security analyzer's results?** *

(Select all that apply)

Check all that apply.

- [ ] The analyzer has a high false positive rate
- [ ] The analyzer lacks explanations for flagged vulnerabilities
- [ ] The analyzer is outdated or not regularly maintained
- [ ] The analyzer is unable to detect recent or emerging vulnerability types
- [ ] The analyzer has a complex installation process
- [ ] The analyzer has a poor user interface
- [ ] The analyzer doesn't have sufficient support or documentation
- [ ] I've had negative past experiences with the analyzer
- [ ] Other: _____

19. **Have you ever ignored a vulnerability reported by a security analyzer?** *

If yes, what was the reason?

Mark only one oval.

- ◯ Yes, due to a high false positive rate
- ◯ Yes, due to unclear or insufficient explanations
- ◯ Yes, due to time or resource constraints
- ◯ No, I always review or address flagged vulnerabilities
- ◯ Other: _____

20. **Can you briefly explain a situation where you chose to ignore a reported vulnerability?**

(Your answer will remain anonymous)

_____

_____

_____

_____

_____

Impact of Explanation on Confidence

This section explores how the clarity and completeness of explanations affect developers' trust in vulnerabilities reported by security analyzers.

21. **What kinds of explanation do you find most helpful from a security analyzer when it reports a vulnerability?** *
(Select all that apply)

Check all that apply.

- [ ] A brief description of the vulnerability
- [ ] The exact location in the code where it occurs
- [ ] A demonstration example of how the vulnerability could be exploited
- [ ] A simulation of the vulnerability's effect (e.g., before vs. after contract state)
- [ ] Suggestions on how to fix or mitigate the issue
- [ ] References to related security standards or best practices
- [ ] Links to further reading or documentation
- [ ] Other: _____

22. **To what extent does the quality of the explanation affect your confidence in the analyzer's results?** *

Mark only one oval.

- ◯ Greatly affects
- ◯ Somewhat affects
- ◯ Neutral / unsure
- ◯ Slightly affects
- ◯ Does not affect at all

23. **If a security analyzer reports a vulnerability and provides a detailed explanation with a code snippet or suggested fix, how confident are you that the vulnerability is a true positive?** *

Mark only one oval.

- ◯ Very confident
- ◯ Somewhat confident
- ◯ Neutral
- ◯ Somewhat not confident
- ◯ Not confident at all

24. **If a security analyzer reports a vulnerability but does *not* include an explanation, how confident are you that it is a true positive?** *

Mark only one oval.

- ◯ Very confident
- ◯ Somewhat confident
- ◯ Neutral
- ◯ Somewhat not confident
- ◯ Not confident at all

25. **Do you have any suggestions for improving the explanation formats used by security analyzers?** *
(How could they better support your understanding, trust, or workflow?)