Bounty Based Smart Contract Auditing Service

Introduction:

My private smart contract security auditing offers a unique approach to projects that differs from traditional methods. Price is charged based on the number of bugs found in the codebase, rather than an hourly or fixed rate. This means that the clients only pay for the results they receive and not for the time it takes me to find them. In this document, I will outline my process for determining pricing, and payment policies.

Pricing:

My pricing is based on the complexity of the protocol and the number of lines of code in the system being audited. I will discuss and agree on the cost for each low, medium, and high severity bug found during the audit. then determine a fair and reasonable price based on their budget and the level of risk associated with their smart contract.

Transparency and fairness are important, which is why I provide a clear breakdown of the cost associated with each type of bug found during the audit. This approach ensures that my clients only pay for the value they receive and have a clear understanding of the cost associated with my services.

My payment policies are designed to reflect my commitment to delivering results. Clients will only pay for the bugs found and nothing more. There is no lower limit, and my upper limit payment ensures that clients are not charged exorbitant fees, even if a large number of bugs are found.

About me:

I provide a unique and effective approach to auditing services. By charging based on the number of bugs found, my clients only pay for the results they receive, and my bug classification system ensures that issues are addressed in order of severity. My payment policies are fair and transparent, ensuring that clients receive the best value for their investment. I have audited some of the big protocol in the space, such as the graph protocol and optimism. My mission to secure the smart contract and eliminates bugs before it hits the production.

Contact me today to learn more about my services and to schedule an audit of your system.

Book a private auditing and reach out to ladboy233 on twitter

Or ladboy233#0859 from discord, my DM are open!

Public Audit Contests in my portfolio

Contest	Date	Platform	Rank	Report

Contest	Date	Platform	Rank	Report
Optimism	February 2023	Sherlock	12rd	Link
OpenQ	February 2023	Sherlock	5th	Link
Ajna	January 2023	Sherlock	5rd	Link
UXD Protocol	January 2023	Sherlock	3th	Link
Numoen	January 2023	Code4rena	3th	Link
Lyra finance	December 2022	Sherlock	4th	Link
GoGo Pool	December 2022	Code4rena	3th	Link
Dodo finance	November 2022	Sherlock	1th	Link
Sense finance	November 2022	Sherlock	2th	Link
Holograph	October 2022	Code4rena	5th	Link
Mycelium	October 2022	Sherlock	1th	Link
Notional Finance	October 2022	Code4rena	4th	Link
Graph Protocol L2 Bridge	October 2022	Code4rena	2th	Link
Confidential	September 2022	Immunefi	N/A	Link

Security review process guide

Questions to project

1. What is the clear scope (`.sol` files) of the security review?

2. Does the project have well written specifications & code documentation?

3. What is the code coverage percentage?

4. Are there any protocols that are similar to yours, which are they?

5. Have you had any audits so far, are you planning to do other audits/security programs as well?

6. Threat Model interview

Based on the answers we can discuss the effort needed, the payment amount and the timeline.

Security review result & fixes review

After the time agreed upon has passed, the project will receive the security review report. The project has 7 days to apply fixes on issues found. Each issues should be fixed in a separate commit that has a message pointing to the issue being fixed. Then, a single iteration of a "fixes review" will be executed by me, free of additional charges, to verify your fixes are correct and secure.

Important notes for the fixes review

- for any questions or clarifications on the vulnerabilities/recommendations in the report, you can reach out to me on the intended channel of communication
- changes to be reviewed should not include anything else other than fixes for the reported issues, so no big refactorings, new features or architectural changes
- in the case that fixes are too difficult to implement or more than one iteration of reviews is needed then this is a special case that can be discussed independently of this review

Disclaimer

A smart contract security review can never verify the complete absence of vulnerabilities. This is a time, resource and expertise bound effort where I try to find as many vulnerabilities as possible. I can not guarantee 100% security after the review or if even the review will find any problems with your smart contracts.