Author(s): Rodrigo Vasquez, Ethereum Foundation; Jay Yu, Stanford Blockchain Club

Outline

0 - Quick Links

- Sponsor the Ethereum Protocol Attackathon (ImmuneFi)
- Ethereum Protocol Attackathon in Collaboration with Immunefi
- EthCC - Security Soirée 2024 - Fireside Chat with Immunefi and the Ethereum Foundation (YouTube)

1 - Summary

This proposal seeks funding from the Uniswap DAO to support an Attackathon, a comprehensive security audit event designed to bolster the security of the Ethereum protocol. The Attackathon will consist of three phases: education, active code hunting, and result evaluation. The goal is to enhance the security of the Ethereum network, which in turn benefits the entire DeFi ecosystem, including Uniswap.

2 - Motivation

The Ethereum Foundation and Immunefi are introducing the first-ever “Attackathon” program, which is aimed to be the largest ever crowdsourced security audit contest conducted to augment security for the entirety of the protocol’s code.

An Attackathon is a multifaceted event involving three phases:

1. Before the Attackathon: A comprehensive education program on the protocol’s code delivered via live technical walkthroughs and Attackathon Academy content.
2. During the Attackathon: Security researchers hunt for vulnerabilities in the code based on specific rules to qualify for rewards. Only impactful reports, as specified by the rules of the Attackathon, will be rewarded.
3. After the Attackathon: Immunefi evaluates and compiles the results into an official Attackathon report, spotlighting top researchers with monetary rewards, NFT awards and a leaderboard.

Although the Ethereum Foundation has a permanent bug bounty, it does not get the awareness and eyeballs it should get on the code. While the EF Bug Bounty has existed since 2015, it typically only receives 2-3 low-medium reports per week. Therefore, we hope that through this event we can draw more skilled security professionals to audit Ethereum and blockchain projects more broadly.

Following recent large hard forks such as Dencun and Shapella, the Ethereum network has undergone significant changes, making this the ideal time to conduct an extensive security audit. Ensuring the protocol’s stability and security post-upgrade is crucial for maintaining trust and reliability.

3 - Proposal Details

This Attackathon will be held fully online. Immunefi will host the contest on their platform and triage the bug reports, and the EF Protocol Security Research Team will judge the results together with representatives from client teams.

The scope of this Attackathon program seeks to include:

- Specification Bugs:
- Safety/finality-breaking bugs
- Denial of service (DOS) vectors
- Inconsistencies in assumptions, like situations where honest validators can be slashed
- Calculation or parameter inconsistencies
- Safety/finality-breaking bugs
- Denial of service (DOS) vectors
- Inconsistencies in assumptions, like situations where honest validators can be slashed
- Calculation or parameter inconsistencies
- Client Bugs:
- Spec non-compliance issues
- Unexpected crashes, RCE or denial of service (DOS) vulnerabilities
- Any issues causing irreparable consensus splits from the rest of the network
- Spec non-compliance issues
- Unexpected crashes, RCE or denial of service (DOS) vulnerabilities
- Any issues causing irreparable consensus splits from the rest of the network
- Solidity Compiler Bugs
- Deposit Contract Bugs

The primary ask for the Uniswap community in supporting this project will be in funding, but any contributions to broadcast the program through socials would also be appreciated!

4 - Benefits to the Uniswap Community

Conducting the Attackathon now, following recent major hard forks of the Ethereum network, is crucial. These upgrades have brought significant changes, and a comprehensive security audit will ensure the protocol's stability and security post-upgrade. This increased focus on security will attract significant attention to the Ethereum codebase, enhancing visibility and participation from security researchers.

For the Uniswap community, this initiative has direct benefits. Enhancing Ethereum's security directly improves Uniswap's reliability and trustworthiness, as Uniswap's security is inherently tied to Ethereum's security. A secure Ethereum fosters a confident developer community, which benefits the entire DeFi ecosystem, including Uniswap. Moreover, by including the Solidity compiler in the competition's scope, the Attackathon will specifically address potential vulnerabilities in the primary programming language for Ethereum smart contracts, which includes those used by Uniswap. Ensuring the security of the Solidity compiler will thus directly enhance the security of Uniswap's smart contracts.

Additionally, aligning with Ethereum's security efforts offers cost-effective benefits. Uniswap will gain from top-tier security assessments without bearing the entire cost, ensuring a secure and robust environment for its operations. Furthermore, by upskilling security researchers now, we prepare them for future hard fork contests, enhancing the overall security readiness of the Ethereum and Uniswap ecosystems.

5 - Cost and Timeline

5.1 - Sponsorship Tiers

Unicorn Partners (+75 ETH Commitment, Approx. $250,000) (limited to two sponsors)

- 1x Unique NFT with leaderboard rank
- Participation in Attackathon Kick-off Twitter Space as a partner speaker
- Leaderboard Placement on Sponsor page
- Top-tier logo placement on Sponsor and Program Landing Page
- Top-tier logo placement on the Program Education page and program report
- Call out in Press Releases and EF and Immunefi Program Announcement Blogs
- Digital Logo Placement in the results announcement at Devcon or a dedicated virtual event
- 4x Devcon tickets
- 25% Discount on Crowd Sec offerings [transferable]
- 1x Dedicated Twitter post announcing sponsorship from Immunefi Twitter handle

Panda Partners (+30 ETH Commitment, Approx. $100,000)

- 1x Unique NFT with leaderboard rank
- Leaderboard listing on the sponsor landing page
- Mid-roll logo placement on Sponsor and Program Landing Page
- 2x Devcon tickets
- 10% Discount on Immunefi Crowd Sec offerings [Transferable]
- 1x Dedicated Twitter post announcing sponsorship from Immunefi Twitter handle

5.2 - Timeline and Key Dates

- July 8-11: EthCC program announcement
- August 8: Detailed program announcement and education kickoff.
- September 1st: Attackathon hunting begins.
- October 31st: Attackathon concludes, and results compilation begins.
- November 9-17: Results announced.