

Top 10 Most Common Bugs Found in Audit Contests

Jack Sanford
CEO and Co-founder, Sherlock



How popular are Audit Contests?

◆ Audit contests completed all-time: 625

◆ Vulnerabilities rewarded all-time: 36,783

◆ Contest prizes all-time: \$36,206,526

OPTIMISM

 **MAKER**

 **GMX**

 **aave**



Uniswap



What is an Audit Contest?

- Goal is to find bugs in code
- Pot of money (\$100k for example) open to anyone
- Participants earn based on:
 - severity
 - uniqueness
 - number of findings



1. First depositor inflation attack in ERC-4626 vaults

- ◆ First depositor can inflate share value to steal funds from later depositors
- ◆ **Example:** Flat Money Issue #190
- ◆ **Detailed Explanation:** Overview of the Inflation Attack



2. Using `transfer()` instead of `safeTransfer()`

- ◆ `transfer()` does not check success/failure of transfer and can allow reentrancy with non-standard tokens like USDT

- ◆ **Example:** [Amphor Issue #79](#)

- ◆ **Detailed Explanation:** [Why You Should Always Use SafeERC20](#)



3. Missing validation / admin checks

◆ Functions that are meant to be restricted or whitelisted are not

◆ **Example:** Winnables Issue #30

◆ **Detailed Explanation:** Access Control



4. Missing check for active L2 sequencer

- ◆ Malicious actors can take advantage of stale prices in the protocol
- ◆ **Example:** Notional Issue #44
- ◆ **Detailed Explanation:** How to Consume Chainlink Price Feeds Safely



5. Reentrancy

- ◆ Various exploits become possible when a function can be called again before its previous execution completes
- ◆ **Example:** [Zap Protocol Issue #5](#)
- ◆ **Detailed Explanation:** [Reentrancy Attacks and the DAO Hack Explained](#)



6. Fee-on-transfer/rebasing tokens

- ◆ Non-standard tokens are often not compatible with protocol functionality
- ◆ **Example:** MagicSea Issue #78
- ◆ **Detailed Explanation:** ERC-20 and Rebase Tokens: ERC-20 Security Bug You Need to Know



7. Rounding / Precision Loss Issues

- ◆ EVM returns inaccurate values due to the lack of floating point arithmetic
- ◆ **Example:** Gamma Rewarder Issue #39
- ◆ **Detailed Explanation:** Precision Loss Vulnerability in Solidity: A Deep Technical Dive



8. Using spot price instead of TWAP in Uniswap

- ◆ Uniswap's spot price (slot0) is easy for an attacker to change
- ◆ **Example:** [Teller Finance Issue #235](#)
- ◆ **Detailed Explanation:** [Price Oracle Manipulation Attacks - The Full Guide](#)



9. Incorrect implementation of UUPS upgradability

- ◆ Various implementation errors mean contracts cannot be upgraded
- ◆ **Example:** Cork Protocol Issue #47
- ◆ **Detailed Explanation:** Proxies



10. No slippage check in custom vaults/pools

- ◆ Non-ERC-4626 vaults can be highly volatile, exposing users to high slippage
- ◆ **Example:** Perpetual Issue #29
- ◆ **Detailed Explanation:** What Are Slippage Attacks in DEXs?

Q&A

[Links](#)