Testing Auction Smart Contracts for Ethereum Virtual Machine

Prepared By: Team 9
Venkata Ashok sairam Dasari – 1002029845
Mithun Ekanandan – 1001843906
Vankireddy Karthik reddy - 1002038114
Teja Sankara - 1002033648

Introduction

- Auction smart contract allows bidding and closes the auction in a specific time.
- Allows multiple users to place bids and the highest bidder is the winner.
- Fuzz testing tool is used to test for this Auction Smart Contract.

Fuzzing tools vs Symbolic execution tools

- Random Input data vs Order Execution.
- Fast vs slow.
- Fuzzing is scalable, ineffective while selecting right inputs.
- Symbolic execution is ineffective to cover complex path conditions.

Competitors

- Echidna – Fast Smart contract fuzzer
- Oyente - Analysis tool for smart contracts
- Driller – Fuzzer + Auditor

Features

- Report generation
- Easily usable CLI tool
- Auto notification triggering for failed testcases

Risks

- Can be Hacked.
- Without thorough testing, vulnerabilities may be exploited.
- New features pose new vulnerability risks.

Customers and users

- Team 9 – We are the first to use
- Smart Contract Developers
- Organizations

Use cases for Audit smart contract

- Online Advertisement auctions
- Ecommerce Auctions
- Mobile network bandwidth utilization auctions during congestion
- Sports Auctions

Where can you find us?

- https://github.com/ashokdv/CSE-6324-Smart-Contracts-for-EVM

References

- https://dl.acm.org/doi/10.1145/3319535.3363230
- https://www.onecause.com/
- https://www.silentauctionpro.com/
- https://github.com/shellphish/driller