ETH-Gathering Reverse Bug Bounty

Aleksander Kryukov, Uri Kirstein, Nurit Dor

Agenda

- Instructions
- Go over contact to verify
- Think about properties
  - Write a few rules together
  - Understand counter example
- How to check the spec

- Get help
  - Docs

    docs.certora.com
  - Tutorials

    https://github.com/Certora/Tutorials
  - Discord

    https://discord.gg/3tyNA6Bh
  - Booth

certora

Properties

Conditions that must hold on a given system

Six main types of properties:

certora

Properties

Conditions that must hold on a given system

Six main types of properties:

- Unit-test

The door can close

Auction ends only when time reached

certora

Properties

Conditions that must hold on a given system

Six main types of properties:

- Unit-test
- Variable Transitions

Floor number changes when a floor is reached

Highest bid only goes up

certora

Properties

Conditions that must hold on a given system

Six main types of properties:

- Unit-test
- Variable Transitions
- State Transitions

Not busy when stopped and no further calls

Once auction ended it is always ended

certora

Properties

Conditions that must hold on a given system

Six main types of properties:

- Unit-test
- Variable Transitions
- State Transitions
- Valid State

The door is close while in motion

Others' bids are less than the highest

certora

Properties

Conditions that must hold on a given system

Six main types of properties:

- Unit-test
- Variable Transitions
- State Transitions
- Valid State
- High-Level Properties

Every call is eventually attended

Something about the assets...

certora

Properties

Conditions that must hold on a given system

Six main types of properties:

- Unit-test
- Variable Transitions
- State Transitions
- Valid State
- High-Level Properties
- Risk Assessment

Every call is eventually attended

What would be devastating...

certora

YOUR GOAL: COVERAGE

More than one category per property

Same bug can be uncovered by different properties

Valid state, high level properties gives better coverage than unit test properties

certora

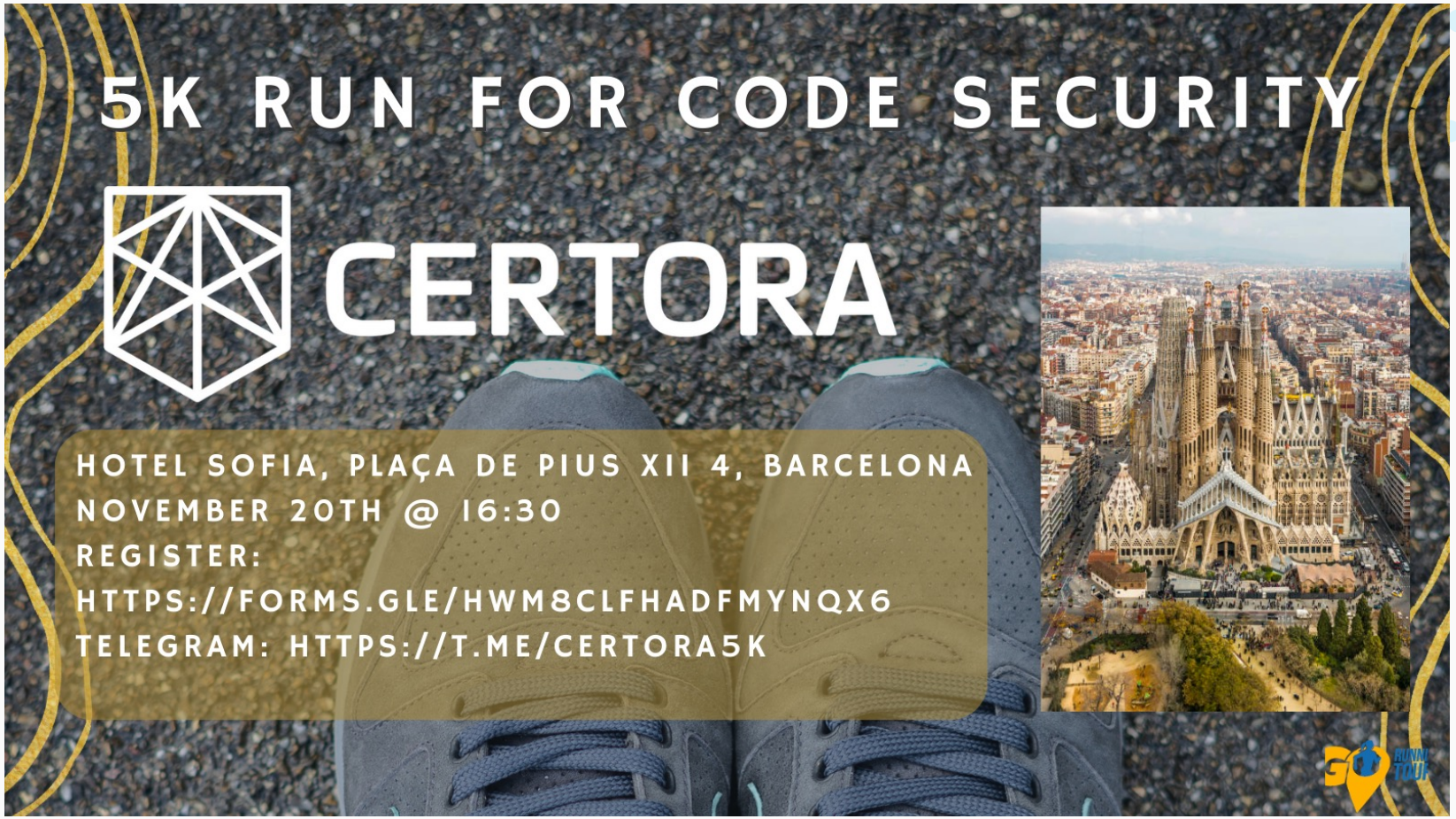
HOW TO TEST YOUR SPEC

--rule-sanity flag

Run on buggy version

Change the assert and look at “good” executions

certora


5K RUN FOR CODE SECURITY
CERTORA
HOTEL SOFIA, PLAÇA DE PIUS XII 4, BARCELONA
NOVEMBER 20TH @ 16:30
REGISTER:
HTTPS://FORMS.GLE/HWM8CLFHADFMYNQX6
TELEGRAM: HTTPS://T.ME/CERTORA5K

certora