|  |  |  |
| --- | --- | --- |
| **区块链合约层脆弱性发现工具准确率测试** | | |
| **用例编号** | **测试指标** | **测试方法** |
| 1 | 测试solidity语言智能合约测试集，误报率不超过10%，漏报率不超过2% | 1. 打开solidity语言智能合约测试集：  https://github.com/my-code-cloud/EvaluationCases/tree/main/solidity%E5%90%88%E7%BA%A6%E6%95%B0%E6%8D%AE%E9%9B%86  2. 打开网页<http://39.103.152.161/>，分别将solidity语言智能合约测试集中的每个智能合约的代码复制到该网页中  3. 选择Solidity，漏洞检测  4. 点击Analyze Now进行分析  5. 统计检测出来的漏洞，与solidity智能合约测试集的漏洞情况进行对比，计算得到漏报率和误报率 |
| 2 | 测试golang语言智能合约测试集，误报率不超过10%，漏报率不超过2% | 在指定软硬件环境下，运行智能合约安全漏洞检测原型系统，检验误报率和漏报率的功能 |

针对用例1：

检测到漏洞总数量：64

* 漏报数量：1
  + 相关solidity智能合约：

<https://github.com/my-code-cloud/EvaluationCases/blob/main/solidity%E5%90%88%E7%BA%A6%E6%95%B0%E6%8D%AE%E9%9B%86/deposit_box_fixed.sol>

* + 漏报漏洞：uninitialized-state
  + 说明：第二行mapping(address => uint) balance是一个未初始化map结构
* 误报数量：4
  + solidity智能合约：

<https://github.com/my-code-cloud/EvaluationCases/blob/main/solidity%E5%90%88%E7%BA%A6%E6%95%B0%E6%8D%AE%E9%9B%86/crypto_roulette_fixed.sol>

* 误报漏洞：incorrect-equality



* 说明：该智能合约实现了一个猜数字游戏，第32行必须通过等式进行比较
  + solidity智能合约：
* <https://github.com/my-code-cloud/EvaluationCases/blob/main/solidity%E5%90%88%E7%BA%A6%E6%95%B0%E6%8D%AE%E9%9B%86/crypto_roulette.sol>
* 误报漏洞：incorrect-equality



* 说明：该智能合约实现了一个有奖竞猜功能，第32行必须通过等式进行比较
  + solidity智能合约：
* https://github.com/my-code-cloud/EvaluationCases/blob/main/solidity%E5%90%88%E7%BA%A6%E6%95%B0%E6%8D%AE%E9%9B%86/guess\_the\_random\_number.sol
* 误报漏洞：incorrect-equality



* 说明：该智能合约实现了一个猜随机数的游戏，第16行必须通过等式进行比较
  + solidity智能合约：
* <https://github.com/my-code-cloud/EvaluationCases/blob/main/solidity%E5%90%88%E7%BA%A6%E6%95%B0%E6%8D%AE%E9%9B%86/guess_the_random_number_fixed.sol>
* 误报漏洞：incorrect-equality



* 说明：该智能合约实现了一个赌博小游戏功能，第27行必须通过等式进行比较

综上，solidity漏洞检测在

https://github.com/my-code-cloud/EvaluationCases/tree/main/solidity%E5%90%88%E7%BA%A6%E6%95%B0%E6%8D%AE%E9%9B%86

数据集上的误报率是4/64=6.25%，漏报率是1/64=1.56%