|  |  |  |
| --- | --- | --- |
| **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go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go语言智能合约测试集：  https://github.com/my-code-cloud/EvaluationCases/tree/main/%E7%AC%AC7%E9%83%A8%E5%88%86%20go%E6%BC%8F%E6%8A%A5%E8%AF%AF%E6%8A%A5%E6%95%B0%E6%8D%AE%E9%9B%862. 打开网页<http://39.103.152.161/>，分别将go语言智能合约测试集中的三组智能合约的名称及代码复制到该网页中  3. 选择Go，漏洞检测  4. 点击Analyze Now进行分析  5. 统计检测出来的漏洞，与go语言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分别是0和9.2% |

三组solidity智能合约的检测结果如下

第一组：12个智能合约，检出漏洞54个，9个误报，漏报率0误报率16.7%

第二组：12个智能合约，检出漏洞51个，漏报率0误报率0%

第三组：11个智能合约，检出漏洞58个，6个误报，漏报率0误报率10.3%

检测到漏洞总数量：163

综上，go漏洞检测的误报率是15/163=9.2%%

* 总误报数量：15
  + 相关智能合约见：

https://github.com/my-code-cloud/EvaluationCases/tree/main/%E7%AC%AC7%E9%83%A8%E5%88%86%20go%E6%BC%8F%E6%8A%A5%E8%AF%AF%E6%8A%A5%E6%95%B0%E6%8D%AE%E9%9B%862.

* + 误报漏洞：chaincode-math-overflow
  + 说明：对于for循环而言，循环变量是有边界的，对循环变量的加减是安全的，并不会造成漏洞