# Security Verification Report

# Overview

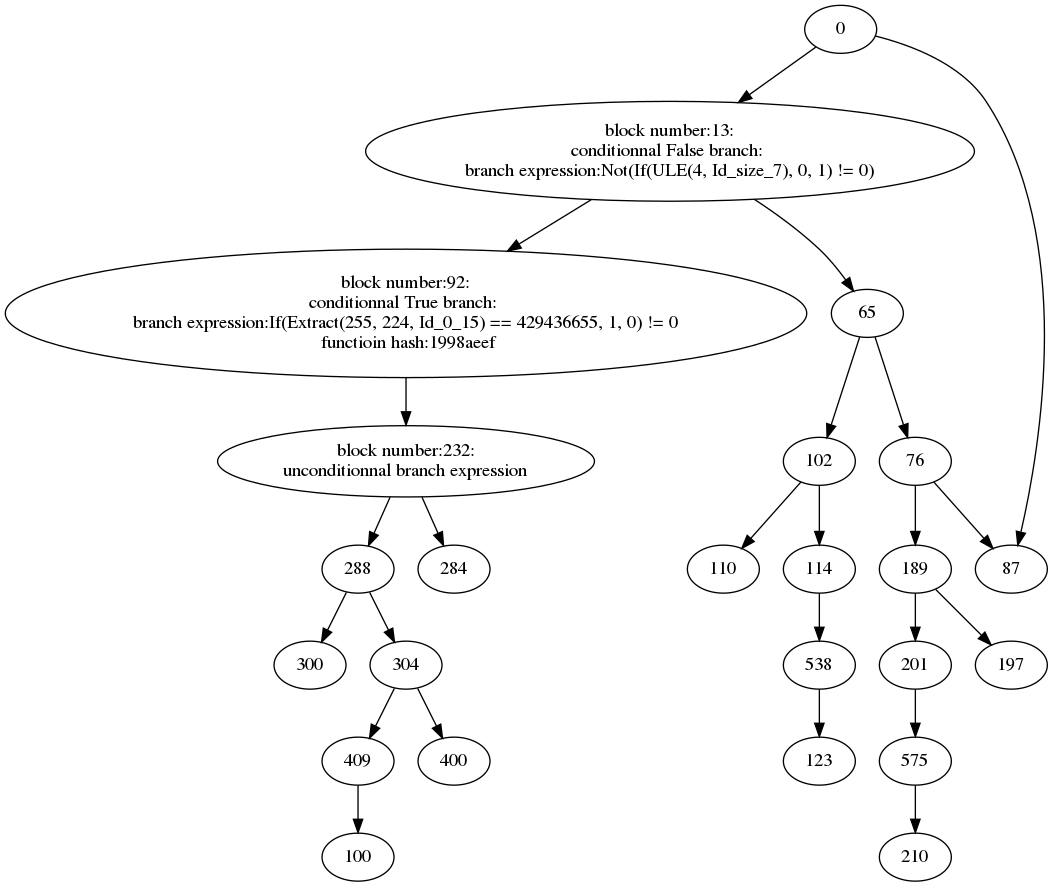
|  |  |
| --- | --- |
| Vulnerability Type | #Num |
| Reentrancy | 1 |
| Pseudorandom Generator | 0 |
| Integer Overflow | 0 |
| Integer Underflow | 0 |
| Transaction-Order Dependency | 0 |
| Denial-of-Service | 1 |
| Account Integrity Violation | 0 |

本次安全性分析是用seraph对智能合约进行自动化测试。Overview是对被测合约中存在的漏洞类型和对应数量的统计，其中，漏洞类型包括reentrancy，Pseudorandom Generator，Integer Overflow，Integer Underflow，Transaction-Order Dependency，Denial-of-Service和Account Integrity Violation。通过分析，在该测试合约中，存在1个reentrancy漏洞和1个Denial-of-Service漏洞。Details包括多个case是对于overview中的每个类别的每个漏洞进行详细的说明，在该合约的分析报告中Detail包含有针对这两个漏洞的case。

# Details

1. Case: Reentrancy

Bug Abstract: 273: CALLtaint direct happen

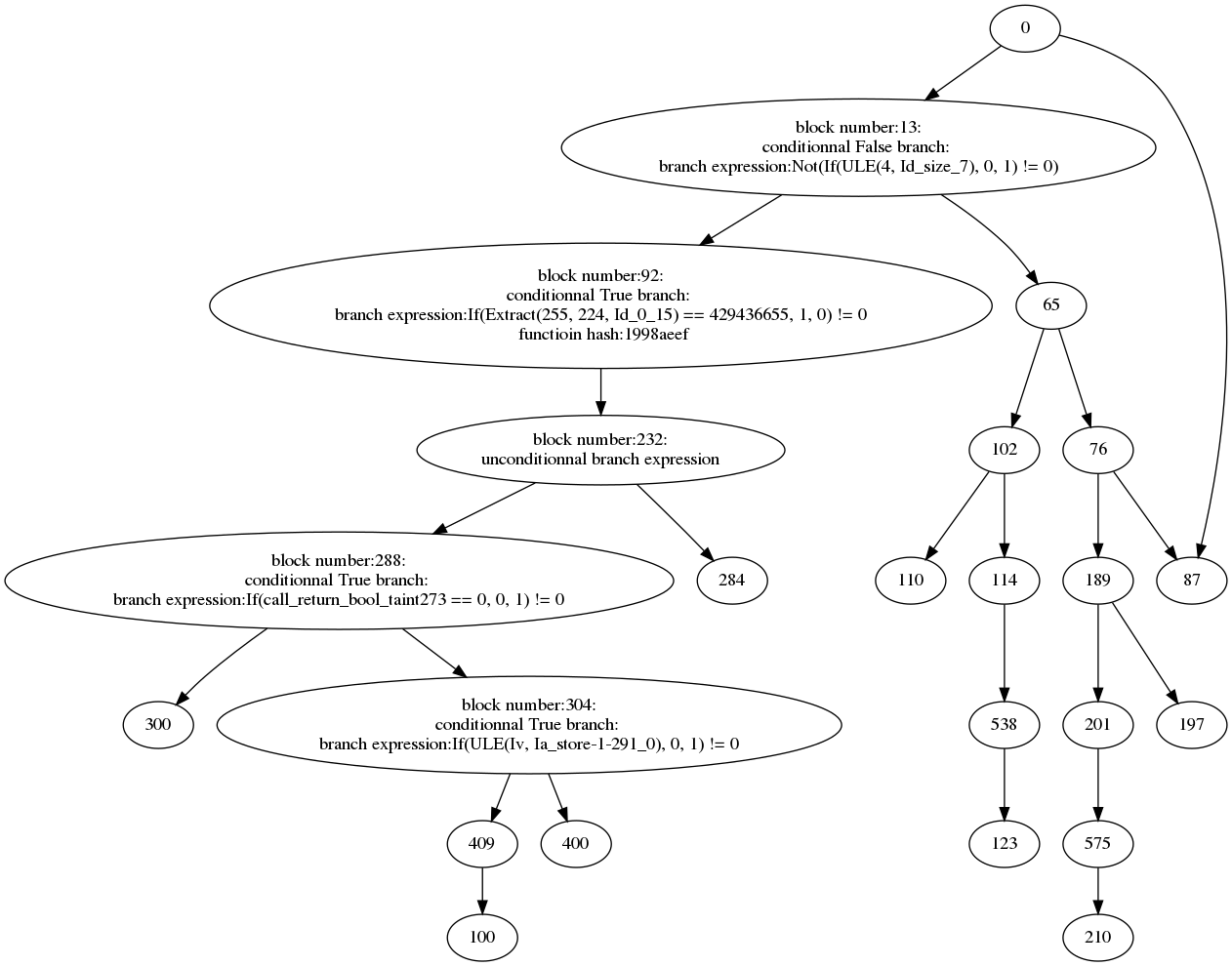


Bug test case: {'callReturn': {}, 'input': {'Id\_0\_15': '11577589315719569134531689797804244115822131984567730048070185093847035412480', 'Id\_size\_7': '57896044618658097711785492504343953926634992332820282019728792003956564819968'}, 'state': {}, 'other': {}, 'block': {}}

Case: Reentrancy是对单个reentrancy漏洞的详细说明，reentrancy漏洞通常发生在对call指令的使用中。Bug Abstract表示该漏洞的子类(call taint direct happen) 和发生漏洞处对应的执行pc(273)， Bug Abstract 同时展示合约的控制流图，控制流图展示了合约分析的所有可能执行的数据流，节点由blocknumber（执行pc）进行标记。其中，触发合约漏洞的数据流，其执行路径的数据流节点由blocknumber和源码共同标记提供参考。Bug test case用于展示一个随机生成的可以触发该漏洞的测试用例。

1. Case: Denial-of-Service

Bug Abstract: 399: JUMPI : a function wait for call return bool to continue otherwise revert



Bug test case: {'callReturn': {'call\_return\_bool\_taint273': '1'}, 'input': {'Id\_0\_15': '11577589315719569134531689797804244115822131984567730048070185093847035412480', 'Id\_size\_7': '57896044618658097711785492504343953926634992332820282019728792003956564819968'}, 'state': {'init\_Ia': '0', 'Ia\_store-1-291\_0': '0', 'Iv': '28948022309329048855892746252171976963317496166410141009864396001978282409985'}, 'other': {}, 'block': {}}

Case: Denial-of-Service表示对单个Denial-of-Service漏洞的详细说明，Denial-of-Service发生于智能合约的状态改变依赖于外部函数执行的结果，又未对执行一直失败的情况做出防护的情况。Bug Abstract表示该漏洞的子类(JUMPI : a function wait for call return bool to continue otherwise revert) 和发生漏洞处对应的执行pc(399)， Bug Abstract 同时展示合约的控制流图，控制流图展示了该合约所有可能执行的数据流，节点由blocknumber（执行pc）进行标记。其中，触发合约漏洞的数据流，其触发路径的数据流节点由blocknumber（执行pc）和源码共同标记以提供参考。Bug test case用于展示一个随机生成的可以触发该漏洞的测试用例。