18 types of bugs injection methods

Pnegcheng Zhang, Feng Xiao, Xiapu Luo, Hai Dong

Jan 2021

1 introduction

In our paper, we introduce the methods of injecting *re-entrancy* bugs and *integer overflow and underflow* bugs into *HuangGai* in detail. And we write this doc to help users understand how *HuangGai* injects 18 other types of bugs.

2 Predefined extraction criteria and injection methods of 18 types of bugs

Table 1: Predefined extraction criteria and injection methods of 18 types of bugs

Bug type	Predefined extraction criteria	
Transaction order dependence	The contract needs to be developed based on *ERC-20 token standard* and includes the *approve* function	*I* is set f
Results of contract execution affected by miners	100.0%	
Unhandled exception	100.0%	
Integer overflow and underflow	94.1%	
Use *tx.origin* for authentication	100.0%	
Re-entrancy	96.7%	
Wasteful contracts	98.0%	
Short address attack	100.0%	
Suicide contracts	100.0%	
Locked ether	100.0%	
Forced to receive ether	100.0%	
Pre-sent ether	100.0%	
Uninitialized local/state variables	99.9%	
Hash collisions with multiple variable length arguments	100.0%	
Specify *function* variable as any type	100.0%	
Dos by complex *fallback* function	100.0%	
Public function that could be declared *external*	99.8%	
Non-public variables are accessed by *public/external* function	99.8%	
Nonstandard naming	99.8%	
Unlimited compiler versions	100.0%	