Web3 Token Security Benchmark

GOPLUS

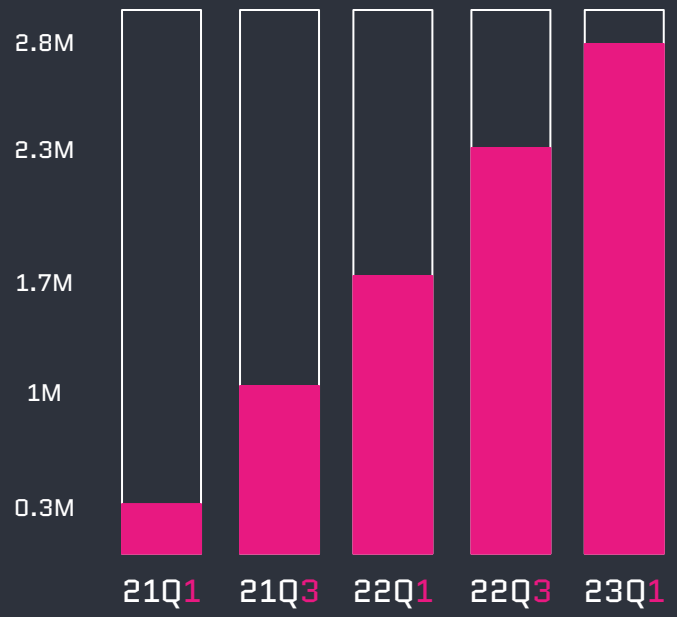
1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

</Courses Overview

- Overlooked User Security Situation
- TSB Introduction
- What can TSB do?
- Detection Tools
- Easter egg

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

</Overlooked User Security



The Number Of Malicious Scam Token Smart Contract Attacking Users

200M

scammed addresses

$108M

lost in the first half of 2023

</Reasons for the Scams Growth

Key Reasons

- **Ease of Entry**
  - Lower barriers to perform a scam
- **Direct User Targeting**
  - Direct-to-user approaches making it easier to breach
- **Tooling Gaps**
  - Lack of effective tools and measures
- **No Standard**
  - No user security standard

</TSB {Token Security Benchmark}

Background

The standard has been adopted by multiple partners of Goplus as well as members of the web3 security ecosystem, and has more than 2 years of practical experience.

BNB Chain	AVALANCHE	polygon	ARBITRUM	OPTIMISM	zkSync
STARKWARE	arweave	fantom	cronos	KCC	NEAR
CoinMarketCap	CONSENSYS	Linea	GeckoTerminal	Opera Crypto	alchemy
QuickNode	DEXTools	SafePal	TOKEN POCKET	BitKeep	ONTO
KEYSTONE	OneKey	Mask	ApeSpace	AveDex	COINBRAIN
CryptoGems	DexCheck	DEXSCREENER	SLOWMIST	BlockSec	chainbase
Footprint Analytics	Harmony	METIS	SYSCOIN	OKX	neo
X2Y2	O3Swap	LI.FI	METATRUST LABS	XREX	FLOOZ

Definition

The Token Security Benchmark (TSB) is a comprehensive framework designed to identify, classify, and document deliberate and deceitful patterns, such as honeypots and intentional backdoors, found in token smart contracts within the cryptocurrency ecosystem. By shedding light on these malicious practices, the TSB provides a reference standard against which crypto participants can evaluate, understand, and guard against the concealed threats inherent in certain smart contracts.

</Dive in the TSB

ID	Category
TSB-001	Honeypot
TSB-002	Mintable
TSB-003	OwnershipRetrieval
TSB-004	BalanceManipulation
TSB-005	HiddenOwnership
TSB-006	SelfDestruction
TSB-007	ExternalInvocation
TSB-008	PurchaseRestriction
TSB-009	FullSaleRestriction
TSB-010	SlippageModification
TSB-011	PauseableTransfer
TSB-012	TransactionBlacklisting
TSB-013	TransactionWhitelisting
TSB-014	AntiWhaleStatus
TSB-015	AntiWhaleModification
TSB-016	TradingCooldown
TSB-017	PersonalSlippageModification

TSB-002 Mintable

Description

Changing the percentage of a position by increasing the balance at a specific address.

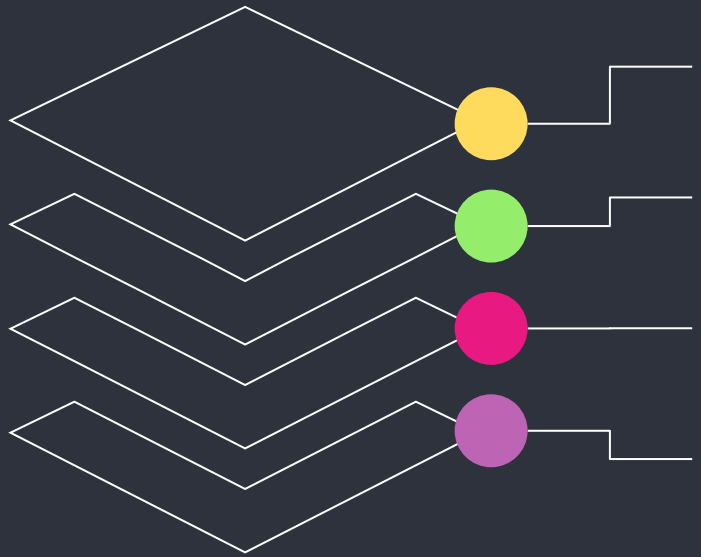
Risk Pattern

```
function mint(unit256 amount) external onlyowner {
  _balances[_msgSender()] += amount;
}
```

Risk Samples

- 01.sol
- 02.sol
- 03.sol
- 04.sol

</What can TSB do?



{A Shield against Scams}

{A Testing Ground for Developers}

{A Catalyst for Research}

{An Educational Asset}

</How to access the TSB data

Contract Security

Contract source code verified

This token contract is open source. You can check the contract code for details. Unsourced token contracts are likely to have malicious functions to defraud their users of their assets.

No proxy

There is no proxy in the contract. The proxy contract means contract owner can modifiy the function of the token and possibly effect the price.

No mint function

Mint function is transparent or non-existent. Hidden mint functions may increase the amount of tokens in circulation and effect the price of the token.

No function found that retrieves ownership

If this function exists, it is possible for the project owner to regain ownership even after relinquishing it

Owner can't change balance

The contract owner is not found to have the authority to modify the balance of tokens at other addresses.

Basic Info

Token Symbol	PEMER
Token Name	Pepe The Homer
Token Contract Address	0x4357...AF69Be
Contract Creator	0x92ee...057ed1
Contract Owner	0x92ee...057ed1

Top 10 Holders

Token Holders: 4

Total Supply: 4000000000000.00

Top10 Holders Ratio

100.00%

0x92...7ed1	2.861T (71.54%)
0x43...69be	1.11T (27.75%)
0x7f...0c2c	28.529G (0.71%)
UniswapV2	0 (0.00%)

Owner's Holdings: 2861471132805.92 Percent: 71.54%

Creator's Holdings: 2861471132805.92 Percent: 71.54%

</Detection methods

- **Slither**

Slither converts the smart contract source code into an intermediate representation of SlithIR. SlithIR uses a static single allocation (SSA) form and a reduced instruction set to simplify the contract analysis process while preserving the semantic information of the source code.

- **String Pattern Match**

Because the contracts we attempt to analyze are all of the token erc-20 type, these contracts are generally more stable and the paths that trigger risks are quite clear. Therefore, using regular expressions to perform string matching can also achieve certain effects.

- **Transaction simulation**

Transaction simulation is a method where transactions are executed in a virtual environment without actually broadcasting them to the real blockchain network. This allows for understanding the potential outcome of a transaction before it becomes irreversible on the blockchain.

</Easter egg

</Q&A and Resources

Telegram: https://t.me/+ALSf1R8UsXsxZjll

Github: https://github.com/cryptousersecurity/token-security-benchmark

Goplus Website: https://gopluslabs.io/

Goplus Twitter: https://twitter.com/GoPlusSecurity