🛸 $UFO — WELL SECURED ✅ — HACKEN AUDIT

UFO Gaming Jul 23 · 3 min read

HACKEN

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: The Truth
Date: July 14th, 2021

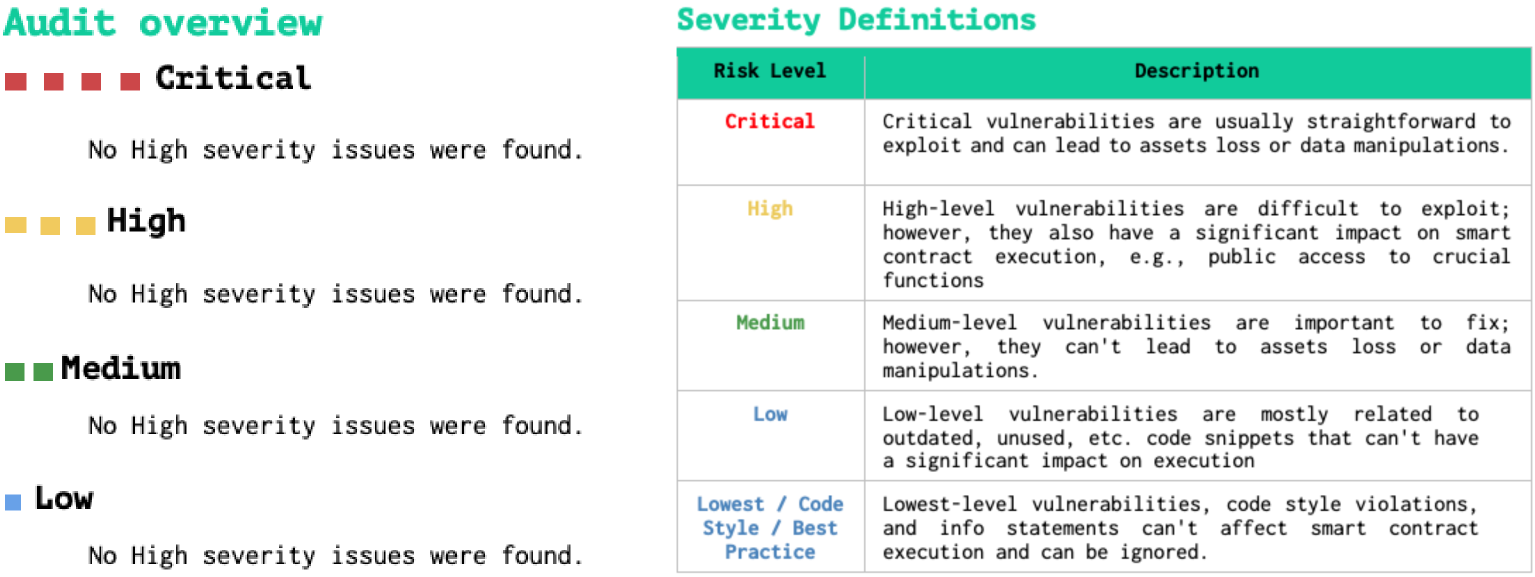
We submitted and received an audit from Hacken and passed with ease. The audit in its entirety will be available from Hacken's website shortly.

Hacken found **zero** notable issues.

This was our final step needed to initiate $UFO phase 2.

This includes pursuing our CEX listings to be available to a broader market, as well as the final stages of our whitepaper.

The whitepaper will contain details of what is going on in the background, plans for $UFO, and upcoming releases.🛸



Audit overview

🟥🟥🟥🟥 **Critical**

No High severity issues were found.

🟨🟨🟨 **High**

No High severity issues were found.

🟩🟩 **Medium**

No High severity issues were found.

🟦 **Low**

No High severity issues were found.

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations, and info statements can't affect smart contract execution and can be ignored.

There was a semantic matter of declaring public functions external to save gas. Informational issues such as these are of no consequence for smart contracts or the code itself.

Among the four possible severity issues of "Critical, High, Medium and Low," as shown above — **NO ISSUES** were found.

The Audit Process

Hacken OÜ (Consultant) was contracted by The Truth (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of Customer's smart contract and its code review conducted between July 12th, 2021 — July 14th, 2021.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools.

Hacken scanned these smart contracts for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that are considered:

Code review

▪ Reentrancy ▪ Ownership Takeover ▪ Timestamp Dependence

▪ Gas Limit and Loops ▪ DoS with (Unexpected) Throw

▪ DoS with Block Gas Limit ▪ Transaction-Ordering Dependence

▪ Style guide violation ▪ Costly Loop ▪ ERC20 API violation

▪ Unchecked external call ▪ Unchecked math ▪ Unsafe type inference

▪ Implicit visibility level ▪ Deployment Consistency ▪ Repository Consistency

▪ Data Consistencywww.hacken.io Functional review

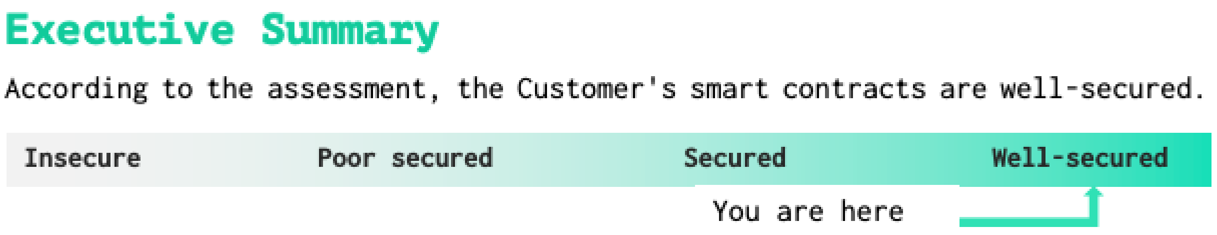
▪ Business Logics Review ▪ Functionality Checks

▪ Access Control & Authorization ▪ Escrow manipulation

▪ Token Supply manipulation ▪ Asset's integrity ▪ User Balances manipulation

▪ Kill-Switch Mechanism ▪ Operation Trails & Event Generation

Conclusion

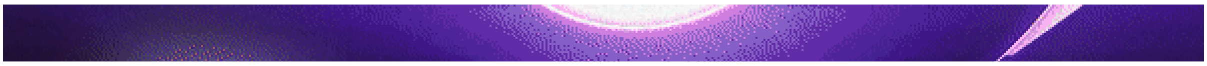


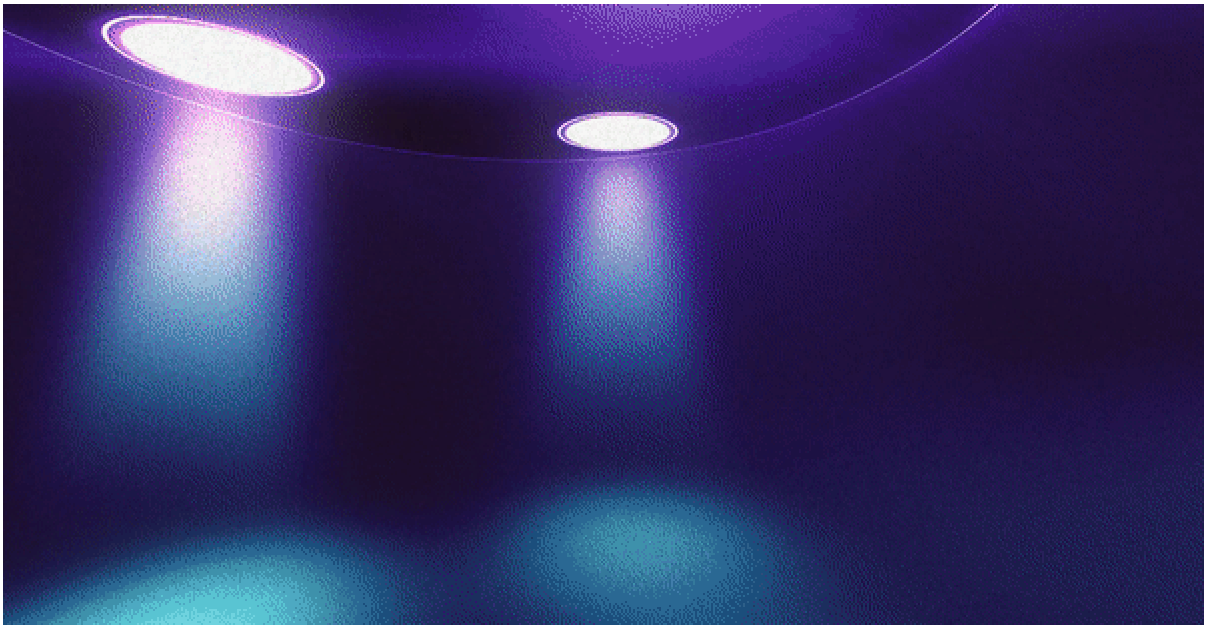
Executive Summary

According to the assessment, the Customer's smart contracts are well-secured.

The audit report contains all found security vulnerabilities and other issues in the reviewed code.

In conclusion, the smart contracts are **well-secured**, at the top of the possible security score.





☮ UFO Token official links

- UFO Token Website
- Telegram (Group)
- Telegram (Announcements)
- Twitter
- Dextools
- Uniswap
- Etherscan
- CoinGecko
- CoinMarketCap
- Liquidity Locked (etherscan) | Team.Finance
- 50% supply burned

Crypto Blockchain UFO