CERTIK

Security Assessment

Golff Finance IV

Sept 21st, 2021

Table of Contents

Summary

This report has been prepared for Golff Finance to discover issues and vulnerabilities in the source code of the Golff Finance IV project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	Golff Finance IV
Platform	Ethereum
Language	Solidity
Codebase	https://github.com/golfffinance/golff-lock
Commit	806a97eb4da2557545d3a4144165f31e3776378c

Audit Summary

Delivery Date	Sept 21, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

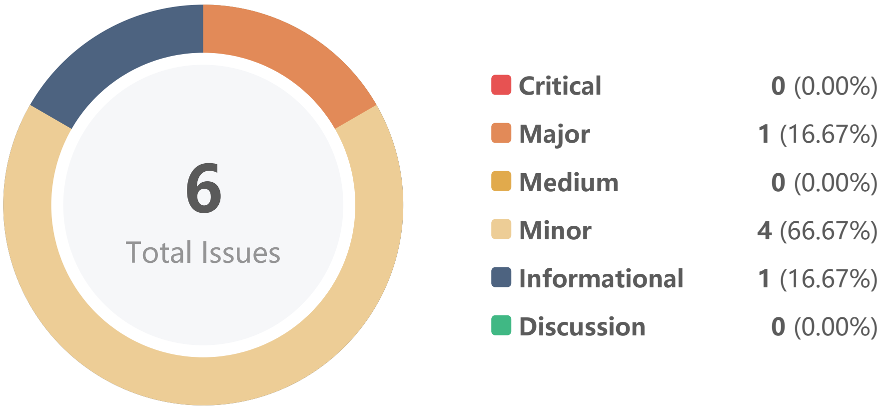
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
Major	1	0	0	1	0	0
Medium	0	0	0	0	0	0
Minor	4	0	0	4	0	0
Informational	1	0	0	1	0	0
Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
BAS	Base64.sol	d3d5a42f5541a06b0f9a68fa71d4c02dd6fd33774656f8c61c9ee1aaedf39ff7
GPE	GolffPet.sol	e0c97a76dbb9db5deb16a641665aa7336e395e4178a607f8d828f708b41ec918
IGN	IGofNft.sol	80940b3935094b448705dad174a5067e70d5c0f5b6ab03913dedd8a6a45c5e32
LPE	LockPool.sol	f4f5ce91c5c3c2981b56f0973641ebfbb36b05c6e557d03713dd5bb0dce3db64

Findings



ID	Title	Category	Severity	Status
GOF-01	Inconsistent Solidity Version	Compiler Error	Minor	ⓘ Acknowledged
BAS-01	Ambiguous `assembly` Usage	Logical Issue	Minor	ⓘ Acknowledged
GPE-01	Centralization Risk	**Centralization / Privilege**	**Major**	ⓘ Acknowledged
GPE-02	Risk For Weak Randomness	Logical Issue	Minor	ⓘ Acknowledged
GPE-03	Redundant `abi.encodePacked` Utilization	Gas Optimization	Informational	ⓘ Acknowledged
LPE-01	No Upper Limit For `rewardRate`	Volatile Code	Minor	ⓘ Acknowledged

GOF-01 | Inconsistent Solidity Version

Category	Severity	Location	Status
Compiler Error	Minor	Global	Acknowledged

Description

The contracts use different versions like the below list:

- Base64.sol and GolffPet.sol - pragma solidity ^0.8.0
- IGofNft.sol - pragma solidity ^0.6.12
- LockPool.sol - pragma solidity ^0.6.6

Recommendation

It is okay to try different compiler versions during the development stage.

However, we recommend locking the contract version when it reaches the production stage, and in this case, seems 0.8.0 is more compatible.

Alleviation

Golff team acknowledged this finding.

BAS-01 | Ambiguous `assembly` Usage

Category	Severity	Location	Status
Logical Issue	Minor	Base64.sol: 20	Acknowledged

Description

The statement ambiguously uses assembly to update the in-memory `result` string variable. And below listed statement does not cover all `mod` possible results.

```
switch mod(mload(data), 3)
  case 1 { mstore(sub(resultPtr, 2), shl(240, 0x3d3d)) }
  case 2 { mstore(sub(resultPtr, 1), shl(248, 0x3d)) }
```

Recommendation

We advise avoiding using `evm` assembly, as it is error-prone.

Alleviation

[Golff Finance]: Currently 99 NTF tokens have been minted, and there is no impact at present.

GPE-01 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	**Major**	GolffPet.sol: 200, 204	Acknowledged

Description

In the contract `GolffPet`, the role `owner` has the authority over the following function:

- setRevealedCollectionBaseURL - Modify the value of variable `revealedCollectionBaseURL`.
- addMinters - Maintain the members of the list `minters` which is used to verify the permission to call `claim()`.

Any compromise to the `owner` account may allow the hacker to take advantage of this.

Recommendation

We advise the client to carefully manage the `owner` account's private key to avoid any potential risks of being hacked.

In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

Indicatively, here is some feasible suggestions that would also mitigate the potential risk at the different level in term of short-term and long-term:

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

Golff team removed function `addMinters`, and usually function `setRevealedCollectionBaseURL` is only called when the contract is deployed.

GPE-02 | Risk For Weak Randomness

Category	Severity	Location	Status
Logical Issue	Minor	GolffPet.sol: 177	Acknowledged

Description

The `sumLuckyPower` is obtained by encoding an increment `tokenIndex` to generate the remainder of `greatness`. The values of `_tokenIds.current()` can be queried from function `surplus()`, so we think the private variable `attributeIndex[tokenId]` based on inner operations can be predicted.

If the parameter passed to `pluck()` is not a random number, then the result is not a random number.

Recommendation

Consider refactoring the function `random()` and mixing a seed value based on the chainlink random service(https://docs.chain.link/docs/get-a-random-number/).

Alleviation

Golff team acknowledged this finding.

GPE-03 | Redundant `abi.encodePacked` Utilization

Category	Severity	Location	Status
Gas Optimization	● Informational	GolffPet.sol: 108~109	ⓘ Acknowledged

Description

All variables included in the `abi.encodePacked` invocation cannot be packed under a single 256-bit slot and as such, the invocation is equivalent to `abi.encode` which is more gas efficient. Additionally, when calculating hashes as identifiers it is wise to utilize `abi.encode` instead of `abi.encodePacked` as unaccounted-for tight packs can lead to the same ID being generated with different input variables.

Recommendation

We advise favorring utilizing `abi.encode` over `abi.encodePacked`.

Alleviation

Golff team acknowledged this finding.

LPE-01 | No Upper Limit For `rewardRate`

Category	Severity	Location	Status
Volatile Code	Minor	LockPool.sol: 156	Acknowledged

Description

The owner can set the `rewardRate` when deploying the contract and there is no upper limit on what the rate can be. In the extreme case, the rate can be as high as 100%, which would imply that users cannot get any token back after depositing the token into the contract.

Recommendation

We recommend setting an reasonable upper limit for the `rewardRate` variable.

Alleviation

[Golff Finance]: `rewardRate` is the number of rewarded tokens generated per second. If the reward of the pool is not enough, our team would transfer more tokens to the pool.

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Compiler Error

Compiler Error findings refer to an error in the structure of the code that renders it impossible to compile using the specified version of the project.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK' s prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK' s position is that each company and individual are responsible for their own due diligence and continuous security. CertiK' s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we’ re able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.

CERTIK