Zellic

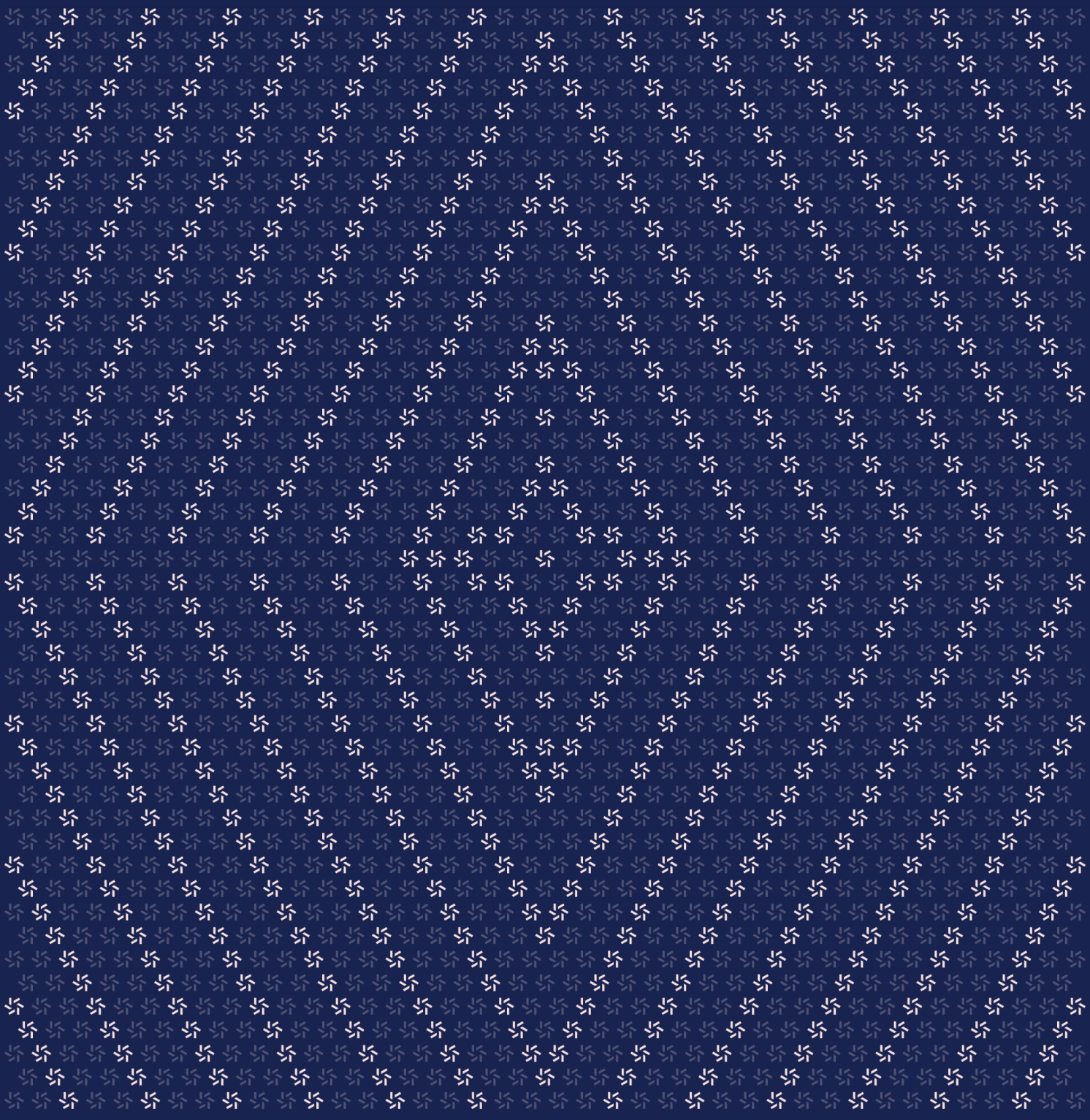
Prepared for
Andrei Grachev
Falcon Finance

Prepared by
Katerina Belotskaia
Quentin Lemauf
Zellic

September 19, 2025

Falcon Finance FF

Smart Contract Security Assessment



Contents

About Zellic

Zellic is a vulnerability research firm with deep expertise in blockchain security. We specialize in EVM, Move (Aptos and Sui), and Solana as well as Cairo, NEAR, and Cosmos. We review L1s and L2s, cross-chain protocols, wallets and applied cryptography, zero-knowledge circuits, web applications, and more.

Prior to Zellic, we founded the #1 CTF (competitive hacking) team ↗ worldwide in 2020, 2021, and 2023. Our engineers bring a rich set of skills and backgrounds, including cryptography, web security, mobile security, low-level exploitation, and finance. Our background in traditional information security and competitive hacking has enabled us to consistently discover hidden vulnerabilities and develop novel security research, earning us the reputation as the go-to security firm for teams whose rate of innovation outpaces the existing security landscape.

For more on Zellic's ongoing security research initiatives, check out our website zellic.io ↗ and follow @zellic_io ↗ on Twitter. If you are interested in partnering with Zellic, contact us at hello@zellic.io ↗.

1. Overview

1.1. Executive Summary

Zellic conducted a security assessment for Falcon Finance on September 18th, 2025. During this engagement, Zellic reviewed Falcon Finance FF's code for security vulnerabilities, design issues, and general weaknesses in security posture.

1.2. Goals of the Assessment

In a security assessment, goals are framed in terms of questions that we wish to answer. These questions are agreed upon through close communication between Zellic and the client. In this assessment, we sought to answer the following questions:

- Does the transfer logic lack sufficient allowance or balance validation, potentially leading to unchecked transfers?
- Could a compromised privileged key or a logic flaw lead to unexpected additional mints?
- Is there a risk that a malicious call or misconfigured privilege could trigger unauthorized token burns?

1.3. Non-goals and Limitations

We did not assess the following areas that were outside the scope of this engagement:

- Front-end components
- Infrastructure relating to the project
- Key custody

Due to the time-boxed nature of security assessments in general, there are limitations in the coverage an assessment can provide.

1.4. Results

During our assessment on the scoped Falcon Finance FF contracts, there were no security vulnerabilities discovered.

Breakdown of Finding Impacts

Impact Level	Count
Critical	0
High	0
Medium	0
Low	0
Informational	0

2. Introduction

2.1. About Falcon Finance FF

Falcon Finance contributed the following description of Falcon Finance FF:

> Falcon Finance is building a universal collateral infrastructure that turns any liquid asset, including digital assets, currency-backed tokens, and tokenized real-world assets, into USD-pegged onchain liquidity. $FF is the protocol's native token and it serves as the gateway to governance, staking rewards, community incentives, and exclusive access to unique products and features.

2.2. Methodology

During a security assessment, Zellic works through standard phases of security auditing, including both automated testing and manual review. These processes can vary significantly per engagement, but the majority of the time is spent on a thorough manual review of the entire scope.

Alongside a variety of tools and analyzers used on an as-needed basis, Zellic focuses primarily on the following classes of security and reliability issues:

Basic coding mistakes. Many critical vulnerabilities in the past have been caused by simple, surface-level mistakes that could have easily been caught ahead of time by code review. Depending on the engagement, we may also employ sophisticated analyzers such as model checkers, theorem provers, fuzzers, and so on as necessary. We also perform a cursory review of the code to familiarize ourselves with the contracts.

Business logic errors. Business logic is the heart of any smart contract application. We examine the specifications and designs for inconsistencies, flaws, and weaknesses that create opportunities for abuse. For example, these include problems like unrealistic tokenomics or dangerous arbitrage opportunities. To the best of our abilities, time permitting, we also review the contract logic to ensure that the code implements the expected functionality as specified in the platform's design documents.

Integration risks. Several well-known exploits have not been the result of any bug within the contract itself; rather, they are an unintended consequence of the contract's interaction with the broader DeFi ecosystem. Time permitting, we review external interactions and summarize the associated risks: for example, flash loan attacks, oracle price manipulation, MEV/sandwich attacks, and so on.

Code maturity. We look for potential improvements in the codebase in general. We look for violations of industry best practices and guidelines and code quality standards. We also provide suggestions for possible optimizations, such as gas optimization, upgradability weaknesses, centralization risks, and so on.

For each finding, Zellic assigns it an impact rating based on its severity and likelihood. There is no hard-and-fast formula for calculating a finding's impact. Instead, we assign it on a case-by-case

basis based on our judgment and experience. Both the severity and likelihood of an issue affect its impact. For instance, a highly severe issue's impact may be attenuated by a low likelihood. We assign the following impact ratings (ordered by importance): Critical, High, Medium, Low, and Informational.

Zellic organizes its reports such that the most important findings come first in the document, rather than being strictly ordered on impact alone. Thus, we may sometimes emphasize an "Informational" finding higher than a "Low" finding. The key distinction is that although certain findings may have the same impact rating, their *importance* may differ. This varies based on various soft factors, like our clients' threat models, their business needs, and so on. We aim to provide useful and actionable advice to our partners considering their long-term goals, rather than a simple list of security issues at present.

2.3. Scope

The engagement involved a review of the following targets:

Falcon Finance FF Contracts

Type	Solidity
Platform	EVM-compatible
Target	falcon-token
Repository	https://github.com/falconfinance/falcon-token ↗
Version	`a04fa81d6ab5fa7c9c3db65a8b0ef5ea5f26de73`
Programs	FF

2.4. Project Overview

Zellic was contracted to perform a security assessment for a total of 0.3 person-weeks. The assessment was conducted by two consultants over the course of one calendar day.

Contact Information

The following project managers were associated with the engagement:

Jacob Goreski
Engagement Manager
jacob@zellic.io

Chad McDonald
Engagement Manager
chad@zellic.io

Pedro Moura
Engagement Manager
pedro@zellic.io

The following consultants were engaged to conduct the assessment:

Katerina Belotskaia
Engineer
kate@zellic.io

Quentin Lemauf
Engineer
quentin@zellic.io

2.5. Project Timeline

The key dates of the engagement are detailed below.

September 18, 2025	Start of primary review period
September 18, 2025	End of primary review period

3. System Design

This provides a description of the high-level components of the system and how they interact, including details like a function's externally controllable inputs and how an attacker could leverage each input to cause harm or which invariants or constraints of the system are critical and must always be upheld.

Not all components in the audit scope may have been modeled. The absence of a component in this section does not necessarily suggest that it is safe.

3.1. Component: Falcon Finance token

Description

The Falcon Finance (FF) token is implemented using the immutable OpenZeppelin ERC20 ↗ contract with ERC20Permit ↗ support. This token uses 18 default decimals. The total supply is fixed at 10,000,000,000 FF tokens and cannot be increased. The FF token is supposed to be deployable to any EVM-compatible chain.

Invariants

- The total supply must equal the sum of all account balances.
- For all accounts, `balanceOf(account) >= 0`.
- Allowances do not grant more transfer rights than intended; `transferFrom` must check allowance and deduct it correctly.
- The `Transfer` event is emitted on every balance change; `Approval` is emitted on allowance changes.

Test coverage

Cases covered

- Deployment: `name == 'Falcon Finance'`, `symbol == 'FF'`, `decimals == 18`, `totalSupply == 10,000,000,000 FF`, and `balanceOf(recipient) == 10,000,000,000 FF`.
- Both `transfer` and `transferFrom` succeed and update balances.
- When allowance is insufficient, `transferFrom` should revert.
- The `approve` allowance increases correctly.
- `approve` with zero amount succeeds.
- `transfer` with zero amount succeeds.
- When `balance < amount`, `transfer` should revert.

4. Assessment Results

During our assessment on the scoped Falcon Finance FF contracts, there were no security vulnerabilities discovered.

4.1. Disclaimer

This assessment does not provide any warranties about finding all possible issues within its scope; in other words, the evaluation results do not guarantee the absence of any subsequent issues. Zellic, of course, also cannot make guarantees about any code added to the project after the version reviewed during our assessment. Furthermore, because a single assessment can never be considered comprehensive, we always recommend multiple independent assessments paired with a bug bounty program.

For each finding, Zellic provides a recommended solution. All code samples in these recommendations are intended to convey how an issue may be resolved (i.e., the idea), but they may not be tested or functional code. These recommendations are not exhaustive, and we encourage our partners to consider them as a starting point for further discussion. We are happy to provide additional guidance and advice as needed.

Finally, the contents of this assessment report are for informational purposes only; do not construe any information in this report as legal, tax, investment, or financial advice. Nothing contained in this report constitutes a solicitation or endorsement of a project by Zellic.