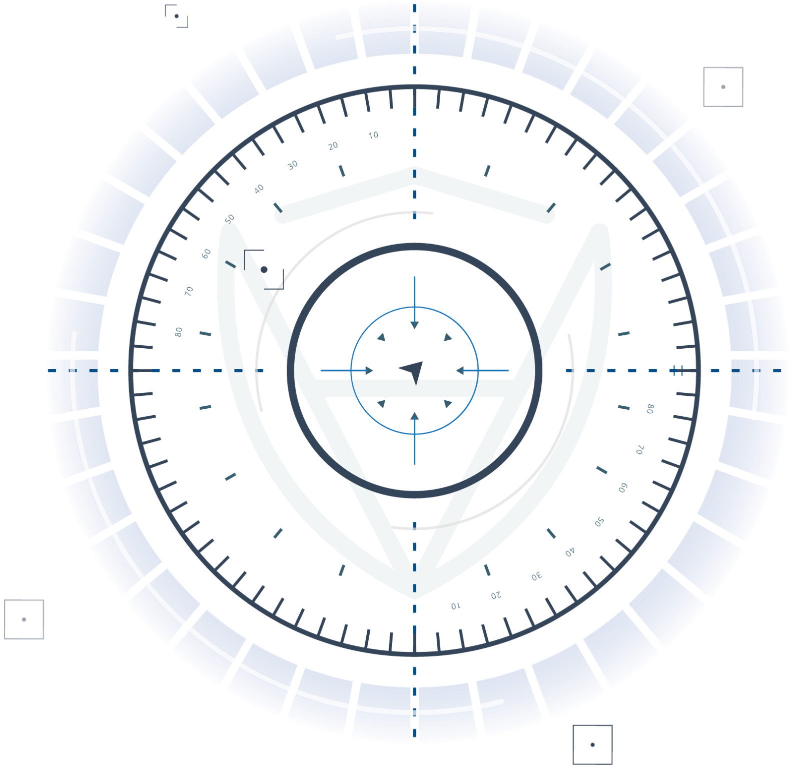
CERTIK
FOUNDATION

xWin

Skynet Scanning Report

Feb 25th, 2021



Summary
Scope of Works
Contract Walkthroughs
xWinToken
xWinDeFi
xWinFund-pancake
Scanning Results
Primitive Scores
Average Score | 91
Smart Contracts
Source-code Primitive Results
Disclaimer
About CertiK

Summary

This report is based on the results from CertiK Skynet Scanning, a proprietary security service that leverages automated scanning technologies to check smart contracts against a wide range of known vulnerabilities. Clients could reference the content to reason about the security score calculations. Automated static analysis can cover a wide range of known security issues and vulnerabilities, yet a full security assessment by security experts is always recommended to cover potential security concerns at business levels.

Scope of Works

The nature of CertiK Skynet is to provide real-time security intelligence, and scanning based on static analysis tool sets is one of the 6 Security Primitives. In summary:

1. Smart contracts run against CertiK's in-house tool chains (together with open source libraries for cross-checking purposes);
1. Manual efforts involved in reviewing the scanning outputs and filter out false alarms. We map scanning results into SWCs for better categorizing and we encourage the development team of the projects to visit the website and follow the recommendations: https://swc-registry.certik.foundation/;
2. Manual efforts on a high level walkthrough of code logics to better understand the project and its intentions that may benefit a future full security assessment.

Contract Walkthroughs

xWinToken

The token contract, typical BEP20 implementation with voting functionality. We've seen this implementation being used by major DeFi projects like SushiSwap. Since the contract has the ability to mint by mintUser, we believe the project has the vision to transfer ownership to the timelock enforced entity to mitigate centralized concerns or potential key-stolen of the mintUser wallet. Meanwhile, the XWIN token enforces a max supply, _cap, turns it into a capped mintable bep20 token.

xWinDeFi

The xWinDefi serves as the main connector with dApp front-end and vaults generated in xWinFund. The contract works similarly as MasterChef with many new features applied. Here are some observations that we found worth noting:

1. Functions like `emergencyWithdraw()` are publically available by end users but there is a modifier of a state controlled by the owner that may prevent from withdrawal when an emergency happens;
2. xWinFund could be updated by contract owner, and fund portfolio targets could be created via xWinFund managers;
3. `DepositFarm()` and `WithdrawFarm()` are typical functionalities for end users to deposit LP tokens in return for XWIN rewards;
4. `Subscribe()` is a public payable function that allows users to send BNB to provide fund into xWinFund for further investments;
5. For the struct param of `xWinLib.TradeParams`, there is a referral that would affect the state variable mapping of `xWinReferral` and such role also earns rewards. We assume the dApp front end side would handle the construction of the param and makes sure the referral role is in place.

xWinFund-pancake

The xWinFund contains the logic of how the rebalance, subscription and redemption works by connecting with other protocols, in our case, the Pancakeswap. It is like a traditional active fund that bases on its strategies to make trades or swaps. The contract itself is majorly centralized, which aligns with its nature to be handled by professionals on trading decisions. Here are some observations that we found worth noting:

1. When the `redeem()` happens, `_handleFeeTransfer()` would be invoked to consider the fee occurred by the platform and manager, while `updateManagerFee()` is privileged to the manager role itself. Thus in theory a manager can update the fee to a large amount which would tamper the final calculated amount to redeem. We assume xWin team will actively monitor the movements of managers and inform the community accordingly;
2. The investment strategy relies on the quote from PancakeSwap and presumably a chaotic situation on third party dependency may introduce unexpected behaviors when doing the `rebalance()`. priceImpactTolerance is introduced to mitigate the financial risks and we encourage the team to have a second review on whether more considerations are needed for a more stable state.

Scanning Results

Primitive Scores

Average Score | 91

- xWinToken | 96
- xWinDeFi | 89
- xWinFund-pancake | 88

Smart Contracts

- xWinToken
- xWinDefi
- xWinFund-pancake

Source-code Primitive Results

In summary, 2 issues were found out of 33 checks for **xWinToken**.

SWC-CTK-35	**-3 pts**
Title	Improper Strict Equalities
Contract	xWinToken
Location	Line#1533

SWC-120	**-1 pts**
Title	Weak Sources of Randomness from Chain Attributes
Contract	xWinToken
Location	Line#1428

In summary, 3 issues were found out of 33 checks for **xWinDefi**.

SWC-107	**-5 pts**
Title	Reentrancy
Contract	xWinDefi
Location	Line#959-966, 1017-1032, 1035-1050, 1054-1072, 1222-1241, 1329-1343

SWC-CTK-41	**-3 pts**
Title	Imprecise Arithmetic Operations Order
Contract	xWinDefi
Location	Line#1309, 1310

SWC-CTK-35	**-3 pts**
Title	Improper Strict Equalities
Contract	xWinDefi
Location	Line#1008, 1193, 1205, 1301, 1306, 1331, 1333

In summary, 4 issues were found out of 33 checks for **xWinFund**.

SWC-CTK-32	**-5 pts**
Title	Arbitrary Ether Send
Contract	xWinFund-pancake

Location	Line#1369

SWC-CTK-41	**-3 pts**
Title	Imprecise Arithmetic Operations Order
Contract	xWinFund-pancake
Location	Line#1584 & 1590, 1621 & 1625, 1728 & 1729, 1841 & 1844

SWC-CTK-35	**-3 pts**
Title	Improper Strict Equalities
Contract	xWinFund-pancake
Location	Line#1760, 1762, 1864, 1877, 1878

SWC-CTK-44	**-1 pts**
Title	Uninitialized Local Variables
Contract	xWinFund-pancake
Location	Line#1269, 1640, 1700

Disclaimer

Skynet Scanning could be leveraged as an automated toolset, however, it cannot replace a formal full security assessment, the toolset is best used synergistically alongside a full formal security audit. Security experts are extremely important in analyzing complex business logic and unknown vulnerabilities specific to each organization. QuickScan is a proprietary CertiK service, offered exclusively to existing and potential clients.

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/verification, and terms and conditions provided to 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 without CertiK's prior written consent.

About CertiK

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
Provable Trust For All