SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY

Xenify

AUDIT

SECURITY ASSESSMENT

15. November, 2023

FOR

XENIFY

Introduction

SolidProof.io is a brand of the officially registered company MAKE Network GmbH, based in Germany. We're mainly focused on Blockchain Security such as Smart Contract Audits and KYC verification for project teams.
Solidproof.io assess potential security issues in the smart contracts implementations, review for potential inconsistencies between the code base and the whitepaper/documentation, and provide suggestions for improvement.

Disclaimer

SolidProof.io reports are not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc'...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing 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. SolidProof's position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of the security or functionality of the technology we agree to analyze.

Project Overview

Summary

Project Name	Xenify
Website	https://xenify.io/swap
About the project	Xenify stands as a cross-chain meta-aggregator of aggregators, pioneering a new era of 'Swap to Earn'. Our groundbreaking protocol seamlessly integrates inventive tokenomics and advanced cross-chain functionality into a single, powerful package.
Chain	Arbitrum
Language	Solidity
Codebase Link	https://github.com/xenify-io/xenify-contracts/tree/develop (Private Repo)
Commit	199b7f8
Unit Tests	Provided

Social Medias

Telegram	https://www.youtube.com/@xenify-io
Twitter	https://twitter.com/xenify_io
Facebook	N/A
Instagram	N/A
Github	N/A
Reddit	N/A
Medium	https://medium.com/xenify
Discord	N/A
Youtube	https://www.youtube.com/@xenify-io
TikTok	N/A
LinkedIn	N/A

Audit Summary

Version	Delivery Date	Changelog
v1.0	24. August 2023	• Layout Project • Automated- /Manual-Security Testing • Summary
v1.1	01. September 2023	• Reaudit
v1.2	15. November 2023	• Reaudit

Note - The following audit report presents a comprehensive security analysis of the smart contract utilized in the project. This analysis did not include functional testing (or unit testing) of the contract/s logic. We cannot guarantee 100% logical correctness of the contract as we did not functionally test it.

File Overview

The Team provided us with the files that should be tested in the security assessment. This audit covered the following files listed below with an SHA-1 Hash.

File Name	SHA-1 Hash
contracts/YSL.sol	0bc9a5d662064d66dfd0be7be391cf0ba6247cf8
contracts/Auction.sol	4b9d107113cb752fc17fe906d2f1252fb905fd16
contracts/vXEN.sol	92a2c22e038affc08551706e1bc0ddc16f019f24
contracts/libs/Math.sol	3e595da008b45f45be2c4e7e5982f3f531bde834
contracts/libs/SignatureHelper.sol	163af6c201e5fc95cbee7e23d41b768adb4bfaec
contracts/libs/ERC2771Context.sol	fd9421098b1774e0a5a3d89d0b508afa5281b163
contracts/Recycle.sol	507723cbbc684d5245bf46c9738d7b76cc17e321
contracts/XNF.sol	3b1617d710bf755966e6f178b6b068491ed32485
contracts/veXNF.sol	e01853a7fabfa310c8fabe259250006ecd299297
contracts/factories/XNFFactory.sol	f7454be5bfc4f568ec1352d650a4ddb656cb01b5
contracts/factories/RecycleFactory.sol	bd2e279e3624bff5b430e25f1bc5078846e35795
contracts/factories/vXENFactory.sol	b3d03b8004f3e6de175d7fd980b19a88bcbf6d95
contracts/factories/AuctionFactory.sol	85e15939a825e56f0470204ab9114779b4aa5e1c
contracts/factories/YSLFactory.sol	c78226502afc97984c978f2a0c8ae8463d9511c6
contracts/factories/veXNFFactory.sol	b6be9f87303ab3590c3dc8f2ce2b29c78ae56f97
contracts/Factory.sol	5c1576ad81c77c890c04f6f143e0c5b69efae293

Please note: Files with a different hash value than in this table have been modified after the security check, either intentionally or unintentionally. A different hash value may (but need not) be an indication of a changed state or potential vulnerability that was not the subject of this scan.

Imported packages

Used code from other Frameworks/Smart Contracts (direct imports).

Dependency / Import Path	Count
@axelar-network/axelar-gmp-sdk-solidity/contracts/executable/AxelarExecutable.sol	3
@axelar-network/axelar-gmp-sdk-solidity/contracts/interfaces/IAxelarGasService.sol	3
@axelar-network/axelar-gmp-sdk-solidity/contracts/utils/AddressString.sol	3
@layerzerolabs/lz-evm-sdk-v1-0.7/contracts/interfaces/ILayerZeroEndpoint.sol	3
@openzeppelin/contracts/interfaces/IERC165.sol	1
@openzeppelin/contracts/security/ReentrancyGuard.sol	3
@openzeppelin/contracts/token/ERC20/ERC20.sol	3
@openzeppelin/contracts/token/ERC20/IERC20.sol	2
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	2
@openzeppelin/contracts/token/ERC721/IERC721.sol	1
@openzeppelin/contracts/token/ERC721/IERC721Receiver.sol	1
@openzeppelin/contracts/token/ERC721/extensions/IERC721Metadata.sol	1
@openzeppelin/contracts/utils/Context.sol	1
@openzeppelin/contracts/utils/Strings.sol	1
@openzeppelin/contracts/utils/cryptography/MerkleProof.sol	2
@openzeppelin/contracts/utils/introspection/ERC165.sol	2
@uniswap/v3-core/contracts/interfaces/IUniswapV3Pool.sol	1
@uniswap/v3-core/contracts/libraries/TickMath.sol	1
@uniswap/v3-periphery/contracts/interfaces/INonfungiblePositionManager.sol	2
@uniswap/v3-periphery/contracts/interfaces/ISwapRouter.sol	1
@uniswap/v3-periphery/contracts/libraries/TransferHelper.sol	2

Note for Investors: We only audited contracts mentioned in the scope above. All contracts related to the project apart from that are not a part of the audit, and we cannot comment on its security and are not responsible for it in any way

Audit Information

Vulnerability & Risk Level

Risk represents the probability that a certain source threat will exploit vulnerability and the impact of that event on the organization or system. The risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon aspossible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to check the repository for security-related issues, code quality, and compliance with specifications and best practices. To this end, our team of experienced pen-testers and smart contract developers reviewed the code line by line and documented any issues discovered.

We check every file manually. We use automated tools only so that they help us achieve faster and better results.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
    a. Reviewing the specifications, sources, and instructions provided to SolidProof to ensure we understand the size, scope, and functionality of the smart contract.
    b. Manual review of the code, i.e., reading the source code line by line to identify potential vulnerabilities.
    c. Comparison to the specification, i.e., verifying that the code does what is described in the specifications, sources, and instructions provided to SolidProof.

2. Testing and automated analysis that includes the following:
    a. Test coverage analysis determines whether test cases cover code and how much code is executed when those test cases are executed.
    b. Symbolic execution, which is analysing a program to determine what inputs cause each part of a program to execute.

3. Review best practices, i.e., review smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on best practices, recommendations, and research from industry and academia.

4. Concrete, itemized and actionable recommendations to help you secure your smart contracts.

Overall Security

Upgradeability

Contract is not an upgradeable	✅ **Deployer cannot update the contract with new functionalities**
Description	The contract is not an upgradeable contract. The deployer is not able to change or add any functionalities to the contract after deploying.
Comment	Contracts are not directly upgradeable by the proxy method.

Ownership

The ownership is absent	✅ The owner has no privileges
Description	The owner has not renounced the ownership that means that the owner retains control over the contract's operations, including the ability to execute functions that may impact the contract's users or stakeholders. This can lead to several potential issues, including: • Centralizations • The owner has significant control over contract's operations
Comment	There are no direct ownership state changing privileges in the contract.

Ownership Privileges

These functions can be dangerous. Please note that abuse can lead to financial loss. We have a guide where you can learn more about these Functions.

Minting tokens

Minting tokens refer to the process of creating new tokens in a cryptocurrency or blockchain network. This process is typically performed by the project's owner or designated authority, who has the ability to add new tokens to the network's total supply.

Contract owner cannot mint new tokens	✅ **The owner cannot mint new tokens**
Description	The owner is not able to mint new tokens once the contract is deployed.
Comment	N/A

Burning tokens

Burning tokens is permanently destroying a certain number of tokens, reducing the total supply of a cryptocurrency or token. This is usually done to increase the value of the remaining tokens, as the reduced supply can create scarcity and potentially drive up demand.

Contract owner cannot burn tokens	✅ **The owner cannot burn tokens**
Description	The owner is not able burn tokens without any allowances.
Comment	N/A

Blacklist addresses

Blacklisting addresses in smart contracts is the process of adding a certain address to a blacklist, effectively preventing them from accessing or participating in certain functionalities or transactions within the contract. This can be useful in preventing fraudulent or malicious activities, such as hacking attempts or money laundering.

Contract owner cannot blacklist addresses	✅ **The owner cannot blacklist addresses**
Description	The owner is not able blacklist addresses to lock funds.
Comment	N/A

Fees and Tax

In some smart contracts, the owner or creator of the contract can set fees for certain actions or operations within the contract. These fees can be used to cover the cost of running the contract, such as paying for gas fees or compensating the contract's owner for their time and effort in developing and maintaining the contract.

Contract owner cannot set fees more than 25%	✅ **The owner cannot levy unfair taxes**
Description	The owner is not able to set the fees above 25%
Comment	N/A

Lock User Funds

In a smart contract, locking refers to the process of restricting access to certain tokens or assets for a specified period of time. When tokens or assets are locked in a smart contract, they cannot be transferred or used until the lock-up period has expired or certain conditions have been met.

Owner cannot lock the contract	✅ **The owner cannot lock the contract**
Description	The owner is not able to lock the contract by any functions or updating any variables.
Comment	N/A

External/Public functions

External/public functions are functions that can be called from outside of a contract, i.e., they can be accessed by other contracts or external accounts on the blockchain. These functions are specified using the function declaration's external or public visibility modifier.

State variables

State variables are variables that are stored on the blockchain as part of the contract's state. They are declared at the contract level and can be accessed and modified by any function within the contract. State variables can be defined with a visibility modifier, such as public, private, or internal, which determines the access level of the variable.

Components

📝 Contracts	📚 Libraries	🔍 Interfaces	🎨 Abstract
13	2	0	1

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

🌐 Public	💰 Payable
106	27

External	Internal	Private	Pure	View
78	129	0	4	45

StateVariables

Total	🌐 Public
104	88

Capabilities

Solidity Versions observed	Transfers ETH	Can Receive Funds	ECRecover	Uses Hash Functions
`0.8.18`	Yes	Yes	Yes	Yes

Inheritance Graph

An inheritance graph is a graphical representation of the inheritance hierarchy among contracts. In object-oriented programming, inheritance is a mechanism that allows one class (or contract, in the case of Solidity) to inherit properties and methods from another class. It shows the relationships between different contracts and how they are related to each other through inheritance.

Centralization Privileges

Centralization can arise when one or more parties have privileged access or control over the contract's functionality, data, or decision-making. This can occur, for example, if a single entity controls the contract or if certain participants have special permissions or abilities that others do not.

In the project, some authorities have access to the following functions:

File	Privileges
All	• There are no ownership privileges

Recommendations

To avoid potential hacking risks, it is advisable for the client to manage the private key of the privileged account with care. Additionally, we recommend enhancing the security practices of centralized privileges or roles in the protocol through a decentralized mechanism or smart-contract-based accounts, such as multi-signature wallets.

Here are some suggestions of what the client can do:

- Consider using multi-signature wallets: Multi-signature wallets require multiple parties to sign off on a transaction before it can be executed, providing an extra layer of security e.g. Gnosis Safe
- Use of a timelock at least with a latency of e.g. 48-72 hours for awareness of privileged operations
- Introduce a DAO/Governance/Voting module to increase transparency and user involvement
- Consider Renouncing the ownership so that the owner cannot modify any state variables of the contract anymore. Make sure to set up everything before renouncing.

Audit Results

Critical issues

No critical issues

High issues

No high issues

Medium issues

#1 | Logic Flow

File	Severity	Location	Status
Auction	Medium	L487, 534	Fixed

Description - The msg.value for the current user will be overridden if the same user calls the function more than once. Generally, the value should be added to the previous value and not overwritten.

Remediation - We recommend incrementing the "msg.value" for the existing user.

#2 | Missing Timelock

File	Severity	Location	Status
Auction	Medium	L673	Fixed

Description - The contract misses a timelock in the claim native function. This means that the claim function can be called recursively.

Remediation - We recommend putting a timelock or a limit per user so that the claim function cannot be called by an external contract recursively, and only legitimate users will be able to claim natives.

Low issues

#1 | Missing Zero Address Validation

File	Severity	Location	Status
Auction	Low	L345—349	Fixed

Description - Make sure to validate that the address passed in the function parameters is “non-zero”.

Informational issues

#1 | NatSpec documentation missing

File	Severity	Location	Status
All	Informational	N/A	Fixed

Description - If you started to comment on your code, comment on all other functions, variables etc. The documentation only refers to the parameters of the functions, and not the whole functionality

#2 | Floating Pragma

File	Severity	Location	Status
All	Informational	N/A	Fixed

Description - The contracts should be deployed with the same compiler version and flag that they have been tested thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using other versions.

#3 | General recommendation

File	Severity	Location	Status
Auction	Informational	N/A	ACK

Description - The external call via the '_sendViaCall' function should be handled properly while dealing with external contracts, as dealing with external contracts' calls may be risky.

Legend for the Issue Status

Attribute or Symbol	Meaning
Open	The issue is not fixed by the project team.
Fixed	The issue is fixed by the project team.
Acknowledged(ACK)	The issue has been acknowledged or declared as part of business logic.

Blockchain Security | Smart Contract Audits | KYC Development | Marketing

MADE IN GERMANY