Report for:

PWN Finance

PWN Safe Audit

February 2023

Version 1.0

Email	Telephone
info@extropy.io	+44 1865261424

Document Version Control

Data Classification	Client Confidential
Client Name	PWN Finance
Document Title	PWN Protocol Audit Final Report
Author	Extropy Audit Team

1. Executive Summary

Extropy was contracted to conduct a code review and vulnerability assessment of the project.
The review was carried out between 18th and 30th January 2023.
The contracts are well designed and the code is of high quality with obvious attention to security.
A retest was carried between 25th January and 3rd February.

Assessment Summary

The high risk issue was found to be a false positive, and has been closed.
The remaining issues have either been fixed, or deemed to be acceptable at this stage.

Issue Count

Stage	Critical	Medium	Low	Informational
Initial Report	0	0	6	1

Scope

The code audited is taken from repo [Github repo]
(https://github.com/PWNFinance/pwn_safe)

at commit c584b20fc0550b5ba9688f50cbe0bebffd9914cc

Contracts in scope

Whitelist.sol
TokenizedAssetManager.sol
AssetTransferRights.sol
RecipientPermissionManager.sol
IPWNSafeValidator.sol
PWNSafeFactory.sol
OperatorsContext.sol
AssetTransferRightsGuard.sol
IAssetTransferRightsGuard.sol
AssetTransferRightsGuardProxy.sol
DefaultCallbackHandler.sol
CompatibilityFallbackHandler.sol

Technical Findings

The remainder of this document is technical in nature and provides additional detail about the items already discussed, for the purposes of remediation and risk assessment.

Potential un authorised transfer

Risk	High

After discussion with the development team is was concluded that this attack vector, although possible in theory, would not cause significant impact, therefore this issue has been closed.

Status

Closed

Whitelist is optional

Risk	Low
Affects	Whitelist.sol

Status

This is the intended behaviour

External call return values not checked

Risk	Low
Affects	OperatorsContext.sol
	TokenizedAssetManager.sol

Status

This only affects interactions with standard libraries and is therefore not considered problematic.

ERC-20 interface fallback

Risk	Low
Affects	AssetTransfeRights.sol

Status

This issue is known to the development team, but there is no simple fix that would fit with the existing design, so no change will be made at the moment.

Missing checks for zero address

Risk	Low
Affects	PWNSafeFactory.sol
	AssetTransferRightsGuard.sol

Status

Fixed.

Asset with zero balance may be tokenized

Risk	Low
Affects	TokenizedAssetManager.sol

Status

Not considered a problem, but has been noted for potential change in future versions.

Missing setter functions

Risk	Low
Affects	IPWNSafeValidator
	IAssetTransferRightsGuard
	Whitelist

Status

A design choice by the development team to increase immutability.

Unnecessary use of Initializable

Risk	Informational
Affects	AssetTransferRights

Status

Changed to informational as not a security issue and the development team is happy with the design.

Duplicated if statement

Risk	Low
Affects	AssetTransferRights

Status

The duplicated statement has been kept so as to maintain readability.

Throw error if function selector not found

Risk	Low
Affects	AssetTransferRights

Status

This is a design choice to allow flexibility.

Revoked nonce event logic

Risk	Low
Affects	RecipientPermissionManager.sol

Status

Fixed.

Misleading function name

Risk	Informational
Affects	RecipientPermissionManager.sol

Status

Fixed.

Appendix A

Tools used

Static Analysis was performed, using Slither

Appendix B

General Audit Goals

We audit the code in accordance with the following criteria:

Sound Architecture

This audit includes assessments of the overall architecture and design choices. Given the subjective nature of these assessments, it will be up to the development team to determine whether any changes should be made.

Smart Contract Best Practices

This audit will evaluate whether the codebase follows the current established best practices for smart contract development.

Code Correctness

This audit will evaluate whether the code does what it is intended to do.

Code Quality

This audit will evaluate whether the code has been written in a way that ensures readability and maintainability.

Security

This audit will look for any exploitable security vulnerabilities, or other potential threats to the users.

Although we have commented on the application design, issues of crypto economics, game theory and suitability for business purposes as they relate to this project are beyond the scope of this audit.