Cyberscope

A TAC Security Company

Audit Report

XNAP Token

January 2026

Network	BSC_TESTNET
Address	0xE46A3C711Ca7CF58B233a1F8FEE2e0De56056cB2
Audited by	© cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	MVN	Misleading Variables Naming	Unresolved
	NWES	Nonconformity with ERC-20 Standard	Unresolved
	CCR	Contract Centralization Risk	Unresolved
	L14	Uninitialized Variables in Local Scope	Unresolved

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
Critical	Highly Likely / High Impact
Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
Minor / Informative	Unlikely / Low to no Impact

Review

Audit Updates

Initial Audit	06 Oct 2025 https://github.com/cyberscope-io/audits/blob/main/xnap/v1/audit.pdf
Corrected Phase 2	20 Oct 2025 https://github.com/cyberscope-io/audits/blob/main/xnap/v2/audit.pdf
Corrected Phase 3	04 Nov 2025 https://github.com/cyberscope-io/audits/blob/main/xnap/v3/audit.pdf
Corrected Phase 4	31 Dec 2025 https://github.com/cyberscope-io/audits/blob/main/xnap/v4/audit.pdf
Corrected Phase 5	12 Jan 2026

Explorer	https://testnet.bscscan.com/address/0xe46a3c711ca7cf58b233a1f8fee2e0de56056cb2

Source Files

Filename	SHA256
XNAPToken.sol	bfb9d5cbbe620bb0cb485eb230afd4fdf7f532bca4861071668e27bee26c5705

Findings Breakdown

Critical	0
Medium	0
Minor / Informative	4

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	4	0	0	0

MVN - Misleading Variables Naming

Criticality	Minor / Informative
Location	XNAPToken.sol#L202
Status	Unresolved

Description

Variables can have misleading names if their names do not accurately reflect the value they contain or the purpose they serve. The contract uses some variable names that are too generic or do not clearly convey the information stored in the variable. Misleading variable names can lead to confusion, making the code more difficult to read and understand. Specifically, the BUY_BURN_BP and SELL_BURN_BP are used to calculate the burnAmount if the users perform a buy or a sell but they are also applied during the addition and removal of liquidity from the pair.

```shell
if (pancakePair != address(0)) {
   if (from == pancakePair) {
       burnAmount = (value * BUY_BURN_BP) /
BP_DENOM;
   } else if (to == pancakePair) {
       burnAmount = (value * SELL_BURN_BP) /
BP_DENOM;
   } else {
       burnAmount = (value * TRANSFER_BURN_BP) /
BP_DENOM;
   }

}
```

Recommendation

It's always a good practice for the contract to contain variable names that are specific and descriptive. The team is advised to keep in mind the readability of the code.

NWES - Nonconformity with ERC-20 Standard

Criticality	Minor / Informative
Location	XNAPToken.sol#L198
Status	Unresolved

Description

The contract does not fully conform to the ERC20 Standard. Specifically, according to the standard, transfers of 0 values must be treated as normal transfers and fire the Transfer event. However, the contract implements a conditional check that prohibits transfers of 0 values. This discrepancy between the contract's implementation and the ERC20 standard may lead to inconsistencies and incompatibilities with other contracts.

```
Shell
function _transfer(address from, address to,
uint256 value)
    ...

     require(value > 0, "zero");
```

Recommendation

The incorrect implementation of the ERC20 standard could potentially lead to problems when interacting with the contract, as other contracts or applications that expect the ERC20 interface may not behave as expected. The team is advised to review and revise the implementation of the transfer mechanism to ensure full compliance with the ERC20 standard. https://eips.ethereum.org/EIPS/eip-20.

CCR - Contract Centralization Risk

Criticality	Minor / Informative
Location	XNAPToken.sol#L137,163
Status	Unresolved

Description

The contract's functionality and behavior are heavily dependent on external parameters or configurations. While external configuration can offer flexibility, it also poses several centralization risks that warrant attention. Centralization risks arising from the dependence on external configuration include Single Point of Control, Vulnerability to Attacks, Operational Delays, Trust Dependencies, and Decentralization Erosion.

```
Shell
 function setExcluded(address account, bool
excluded) external onlyOwner
```

Recommendation

To address this finding and mitigate centralization risks, it is recommended to evaluate the feasibility of migrating critical configurations and functionality into the contract's codebase itself. This approach would reduce external dependencies and enhance the contract's self-sufficiency. It is essential to carefully weigh the trade-offs between external configuration flexibility and the risks associated with centralization.

L14 - Uninitialized Variables in Local Scope

Criticality	Minor / Informative
Location	contracts/XNAPToken.sol#L200
Status	Unresolved

Description

Using an uninitialized local variable can lead to unpredictable behavior and potentially cause errors in the contract. It's important to always initialize local variables with appropriate values before using them.

```
Shell
uint256 burnAmount;
```

Recommendation

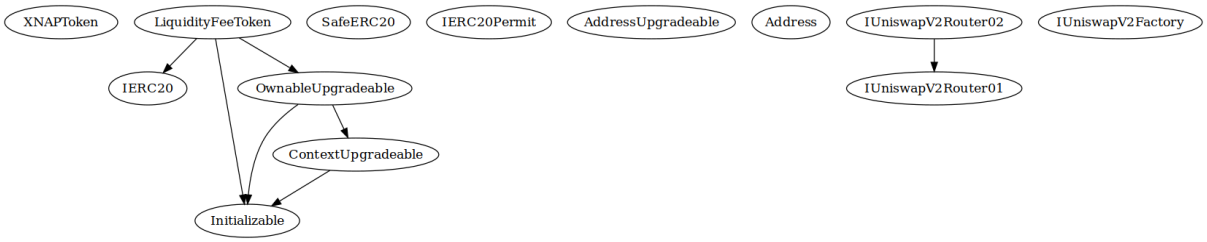
By initializing local variables before using them, the contract ensures that the functions behave as expected and avoid potential issues.

Functions Analysis

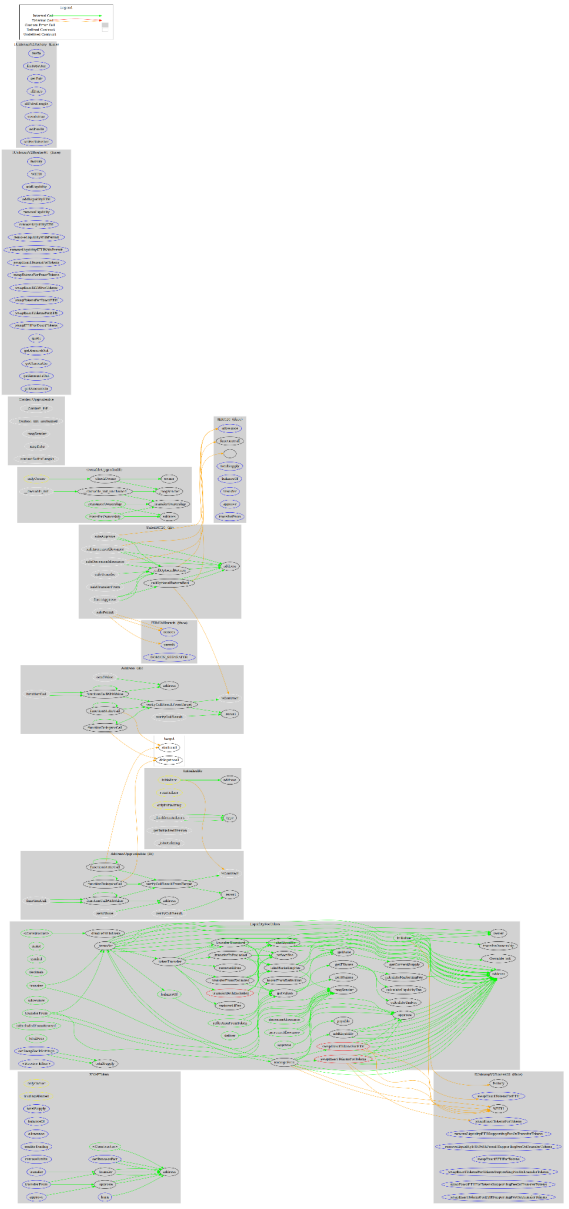
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
XNAPToken	Implementation			
		Public	✓	-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	setPancakePair	External	✓	onlyOwner
	enableTrading	External	✓	onlyOwner
	removeLimits	External	✓	onlyOwner
	transfer	External	✓	-
	approve	External	✓	-
	transferFrom	External	✓	-
	_transfer	Internal	✓	tradingAllowed
	_approve	Internal	✓	
	burn	External	✓	-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-

	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-

Inheritance Graph



Flow Graph



Summary

XNAP Token contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. XNAP Token is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. 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 Cyberscope's prior written consent. 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 regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document 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 represents an extensive assessment 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 Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope'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 Cyberscope are subject to dependencies and are 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.

About Cyberscope

Cyberscope is a TAC blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

A **TAC Security** Company

The Cyberscope team

cyberscope.io