# Audit Report

# King

July 2024

File d23fdf0de9bbb6353a8af27d8bc29dc6e7bf1e2415c2f68c317175eb5534b60b

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 |
|---|---|---|---|
| ● | EVIR | Ether Value Inefficient Representation | Unresolved |
| ● | PAV | Pair Address Validation | 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

| | |
|---|---|
| **Contract Name** | KingToken |
| **Testing Deploy** | https://testnet.bscscan.com/address/0x28823eda688f85f37a2a14c0f8cbc70b1cbd16be |
| **Symbol** | KING |
| **Decimals** | 18 |
| **Total Supply** | 10,000,000 |
| **Badge Eligibility** | Yes |

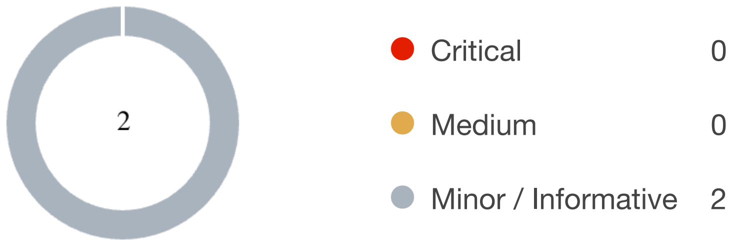
## Audit Updates

| | |
|---|---|
| **Initial Audit** | 17 Jul 2024 |

## Source Files

| Filename | SHA256 |
|---|---|
| contracts/testingDeploy/KING.sol | d23fdf0de9bbb6353a8af27d8bc29dc6e7bf1e2415c2f68c317175eb5534b60b |
| @openzeppelin/contracts/utils/Context.sol | 847fda5460fee70f56f4200f59b82ae622bb03c79c77e67af010e31b7e2cc5b6 |
| @openzeppelin/contracts/token/ERC20/IERC20.sol | 6f2faae462e286e24e091d7718575179644dc60e79936ef0c92e2d1ab3ca3cee |
| @openzeppelin/contracts/token/ERC20/ERC20.sol | 2d874da1c1478ed22a2d30dcf1a6ec0d09a13f897ca680d55fb49fbcc0e0c5b1 |
| @openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol | 1d079c20a192a135308e99fa5515c27acfbb071e6cdb0913b13634e630865939 |
| @openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol | 2e6108a11184dd0caab3f3ef31bd15fed1bc7e4c781a55bc867ccedd8474565c |
| @openzeppelin/contracts/interfaces/draft-IERC6093.sol | 4aea87243e6de38804bf8737bf86f750443d3b5e63dd0fd0b7ad92f77cdbd3e3 |
| @openzeppelin/contracts/access/Ownable.sol | 38578bd71c0a909840e67202db527cc6b4e6b437e0f39f0c909da32c1e30cb81 |

# Findings Breakdown




| Severity | Unresolved | Acknowledged | Resolved | Other |
|---|---|---|---|---|
| Critical | 0 | 0 | 0 | 0 |
| Medium | 0 | 0 | 0 | 0 |
| Minor / Informative | 2 | 0 | 0 | 0 |

## EVIR - Ether Value Inefficient Representation

| | |
|---|---|
| **Criticality** | Minor / Informative |
| **Location** | KING.sol#L199 |
| **Status** | Unresolved |

### Description

The contract uses the `setThreshold` function that includes a check to ensure that the new threshold value does not exceed 1 ETH. This check is implemented using the expression 1 *10* * 18, which accurately represents 1 ETH in wei (the smallest unit of ether). However, Solidity provides a more intuitive and readable way to represent ether values using the ether keyword. Utilizing 1 ether instead of 1 *10* * 18 enhances code readability and reduces the likelihood of errors associated with manual calculations of ether values.

```
require(newThreshold <= 1 * 10 ** 18, "Threshold can't exceed 1 ETH");
```

### Recommendation

The team is advised to replace the expression `1 * 10 ** 18` with `1 ether` to improve code readability and maintainability. The ether keyword is specifically designed for such use cases and provides a clear, self-explanatory representation of ether values.

## PAV - Pair Address Validation

| | |
|---|---|
| **Criticality** | Minor / Informative |
| **Location** | KING.sol#L175 |
| **Status** | Unresolved |

### Description

The contract is missing address validation in the pair address argument. The absence of validation reveals a potential vulnerability, as it lacks proper checks to ensure the integrity and validity of the pair address provided as an argument. The pair address is a parameter used in certain methods of decentralized exchanges for functions like token swaps and liquidity provisions.

The absence of address validation in the pair address argument can introduce security risks and potential attacks. Without proper validation, if the owner's address is compromised, the contract may lead to unexpected behavior like loss of funds.

```
function setPair(address pair, bool value) public onlyOwner {
  require(isPair[pair] != value, "Pair is already set to this
value");
  isPair[pair] = value;
  emit SetPair(pair, value);
}
```

### Recommendation

To mitigate the risks associated with the absence of address validation in the pair address argument, it is recommended to implement comprehensive address validation mechanisms. A recommended approach could be to verify pair existence in the decentralized application. Prior to interacting with the pair address contract, perform checks to verify the existence and validity of the contract at the provided address. This can be achieved by querying the provider's contract or utilizing external libraries that provide contract verification services.

# Functions Analysis

| Contract | Type | Bases | | |
|---|---|---|---|---|
| | **Function Name** | **Visibility** | **Mutability** | **Modifiers** |
| | | | | |
| **IRouter** | Interface | | | |
| | factory | External | | - |
| | swapExactTokensForETH | External | ✓ | - |
| | swapExactETHForTokensSupportingFeeOnTransferTokens | External | Payable | - |
| | | | | |
| **IFactory** | Interface | | | |
| | getPair | External | | - |
| | | | | |
| **KingToken** | Implementation | ERC20Burnable, Ownable | | |
| | | Public | ✓ | ERC20 Ownable |
| | _update | Internal | ✓ | |
| | handleTax | Private | ✓ | lockTheSwap |
| | swapTokensForETH | Private | ✓ | |
| | burnPREME | Private | ✓ | |
| | setSwapPair | Private | ✓ | |
| | setPair | Public | ✓ | onlyOwner |
| | setSwapAtPercentage | Public | ✓ | onlyOwner |
| | setThreshold | Public | ✓ | onlyOwner |

| | | | | |
|---|---|---|---|---|
| | setTax | Public | ✓ | onlyOwner |
| | teamTax | External | | - |
| | setExcludedFromTaxStatus | Public | ✓ | onlyOwner |
| | setTeamWallet | Public | ✓ | onlyOwner |
| | transferOwnership | Public | ✓ | onlyOwner |
| | manualSwap | External | ✓ | onlyOwner |
| | | External | Payable | - |

# Summary

King Gabe contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. King Gabe is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users’ transactions. There is also a limit of max 3% fees.

# 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 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.

**The Cyberscope team**

https://www.cyberscope.io