



# Smart Contract Security Audit

**Project: Glory of Cupid**

Sep 07, 2022



**Contract Address**

0xbB6C4E4Bf2808484512A4b30A072C9C2AC368aA

# Table of Contents

- 1 Disclaimer**
- 2 Audit Review**
- 3 Project Review**
- 4 Smart Contract Vulnerability Checks**
- 5 Manual Code Review**
- 6 Owner Privileges**
  - 6.1 Contract Ownership
  - 6.2 Liquidity Overview
- 7 Tokenomics**
- 8 Social Media Check**
- 9 Website Review**
- 10 Audit Conclusion**

## Disclaimer

The contents of this report reflect only the CRACKEN TECH audit team's understanding of the current progress and status of the security of the code audited, to verify the integrity of the code provided for the scope of this audit. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Given the size of the project, the findings detailed here are not to be considered exhaustive, and further testing and audit are recommended after the issues covered are fixed. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report.

The review does not address the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. If the audited source files are smart contract files, risks or issues introduced by using data feeds from off-chain sources are not extended by this review either.

## Audit Review

The source code of the Glory of Cupid was audited in order to acquire a clear impression of how the project was implemented. The Cracken Tech audit team conducted in-depth research, analysis, and scrutiny, resulting in a series of observations. A detailed list of each issue found, and vulnerabilities in the source code will be included in the audit report. The problems and potential solutions are given in this report, we will identify common sources for such problems and comments for improvement.

The auditing process will follow a routine as special considerations by Cracken:

- Review of the specifications, sources, and instructions provided to Cracken to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
- Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Cracken describe.
- Test coverage analysis determines whether the test cases are covering the code and how much code is exercised when we run the test cases.
- Symbolic execution is analyzing a program to determine what inputs cause each part of a program to execute.
- Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.

## Project Review

### Token Summary

Parameter	Result
Token Name	Glory of Cupid
Token Symbol	Cupid
Token Decimal	18
Total Supply	1,000,000,000
Platform	BSC
Buy Tax Fee	7%
Sell Tax Fee	8%
Contract Creation Date	Sep 06, 2022
Liquidity Status	Not available when Audit
Liquidity Lockup Time	Not available
Compiler Version	v0.8.16+commit.07a7930e
Optimization	Yes with 200 runs
Contract Address	0xbBb6C4E4Bf2808484512A4b30A072C9C2AC368aA
Deployer Address	0x94ae260e69ec8f07d7568dee536662b02768bc13
Owner Address	0xf843a45341825c8f92acbcf07166be01afef11c5

### Source Code

CRACKEN was commissioned by Glory of Cupid to perform an audit based on the following smart contract:

<https://bscscan.com/address/0xbBb6C4E4Bf2808484512A4b30A072C9C2AC368aA>





## Smart Contract Vulnerability Checks

Vulnerability	Auto-Scan	Manual-Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	Low / No Risk
Code With No Effects	Complete	Complete	Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	Low / No Risk
Hash Collisions with Multiple Variable Length Arguments	Complete	Complete	Low / No Risk
Unexpected Ether balance	Complete	Complete	Low / No Risk
Presence of unused variables	Complete	Complete	Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	Low / No Risk
Typographical Error	Complete	Complete	Low / No Risk
DoS With Block Gas Limit	Complete	Complete	Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	Low / No Risk
Insufficient Gas Grieving	Complete	Complete	Low / No Risk
Incorrect Inheritance Order	Complete	Complete	Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	Low / No Risk
Requirement Violation	Complete	Complete	Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	Low / No Risk
Authorization through tx. origin	Complete	Complete	Low / No Risk
Delegate call to Untrusted Callee	Complete	Complete	Low / No Risk





Vulnerability	Auto-Scan	Manual-Scan	Result
Use of Deprecated Solidity Functions	Complete	Complete	Low / No Risk
Assert Violation	Complete	Complete	Low / No Risk
Reentrancy	Complete	Complete	Low / No Risk
Unprotected SELF-DESTRUCT Instruction	Complete	Complete	Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	Low / No Risk
Outdated Compiler Version	Complete	Complete	Low / No Risk
Integer Overflow and Underflow	Complete	Complete	Low / No Risk
Function Default Visibility	Complete	Complete	Low / No Risk

## Manual Code Review

### Classification of Issues

Severity	Description
 High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
 Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
 Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
 Informational	A vulnerability that has an informational character but is not affecting any of the code.

### Findings

Severity	Found
 High-Risk	0
 Medium-Risk	0
 Low-Risk	0
 Informational	3
Total	3



● Informational: Implementation of certain corrective actions or accepting the risk.

## Set max buy tax fee

Description:

**The owner cannot change the buy fees up to 7% for 14 days after launch.**

```
function updateBuyFees(uint256 _liquidityFeeOnBuy,uint256 _marketingFeeOnBuy, uint256
_mmarketingFee2_OnBuy) external onlyOwner {

    require(_liquidityFeeOnBuy + _marketingFeeOnBuy +
    _marketingFee2_OnBuy<= 7, "Fees cannot be more than 7%");

    if (_liquidityFeeOnBuy + _marketingFeeOnBuy + _marketingFee2_OnBuy >
buyFee) {

        require(launchTime + 14 days < block.timestamp, "Fees cannot be increased
for 14 days after launch");

    }

    liquidityFeeOnBuy = _liquidityFeeOnBuy;

    marketingFeeOnBuy = _marketingFeeOnBuy;

    marketingFee2_OnBuy = _marketingFee2_OnBuy;

    buyFee = _liquidityFeeOnBuy + _marketingFeeOnBuy + _marketingFee2_OnBuy;

    emit BuyFeesUpdated(_liquidityFeeOnBuy, _marketingFeeOnBuy,
_mmarketingFee2_OnBuy);

}
```

● **Informational:** Implementation of certain corrective actions or accepting the risk.

## Set max sell tax fee

Description:

**The owner cannot change the sell fees up to 8% for 14 days after launch.**

```
function updateSellFees(uint256 _liquidityFeeOnSell,uint256 _marketingFeeOnSell, uint256
_marketingFee2_OnSell) external onlyOwner {

    require(_liquidityFeeOnSell + _marketingFeeOnSell + _marketingFee2_OnSell <=
8, "Fees cannot be more than 8%");

    if (_liquidityFeeOnSell + _marketingFeeOnSell + _marketingFee2_OnSell >
sellFee) {

        require(launchTime + 14 days < block.timestamp, "Fees cannot be increased
for 14 days after launch");

    }

    liquidityFeeOnSell = _liquidityFeeOnSell;

    marketingFeeOnSell = _marketingFeeOnSell;

    marketingFee2_OnSell = _marketingFee2_OnSell;

    sellFee = _liquidityFeeOnSell + _marketingFeeOnSell + _marketingFee2_OnSell;

    emit SellFeesUpdated(_liquidityFeeOnSell, _marketingFeeOnSell,
_marketingFee2_OnSell);

}
```

- Informational: Implementation of certain corrective actions or accepting the risk.

## The transfer between wallets

Description:

**The owner cannot change the wallet transfer fee up to 8% for 14 days after launch.**

```
function updateWalletToWalletFee(uint256 _walletToWalletFee) external onlyOwner {  
    require(_walletToWalletFee <= 8, "Fees cannot be more than 8%");  
    if (_walletToWalletFee > walletToWalletFee) {  
        require(launchTime + 14 days < block.timestamp, "Fees cannot be increased  
for 14 days after launch");  
    }  
    walletToWalletFee = _walletToWalletFee;  
}
```

## Privileged Functions

onlyOwner

Function Name	Parameters	Visibility
changeMarketingWallet	address _marketingWallet	External
changeMarketingWallet2	address _marketingWallet2	External
claimStuckTokens	address token	External
decreaseAllowance	address spender, uint256 subtractedValue	Public
enableWalletToWalletTransferWithoutFee	bool enable	External
excludeFromFees	address account, bool excluded	Public
increaseAllowance	address spender, uint256 addedValue	Public
renounceOwnership		Public
setSwapTokensAtAmount	uint256 amount	External
transfer	address recipient, uint256 amount	External
transferFrom	address sender, address recipient, uint256 amount	Public
transferOwnership	address newOwner	Public

## Contract Ownership

The contract ownership of Glory of Cupid is not currently being renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address `0xf843a45341825c8f92acbcf07166be01afef11c5` which can be viewed: [HERE](#)

The owner wallet has the power to call the functions displayed on the privileged functions list above, if the owner wallet is compromised these privileges could be exploited.

We recommend the team renounce ownership at the right timing if possible, or gradually migrate to a time lock with governing functionalities in respect of transparency and safety considerations.

## Liquidity Overview

### Liquidity Information

Parameter	Result
Pair Address	0x03e9cae6268c44d223fc0b2a39aaea412caefa59
Cupid Reserves	0.00 Cupid
BNB Reserves	0.00 BNB
Liquidity Value	\$0.00 USDT
Liquidity Ownership	The token does not have liquidity at the moment of the audit


## Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0xf843a45341825c8f92acbcf07166be01afef11c5	1,000,000,000	100.0000%

## Social Media Check

Social Media Type	Link	Result
Website	<a href="https://www.glorycupid.win/">https://www.glorycupid.win/</a>	Checked
Twitter	<a href="https://twitter.com/GloryofCupid/">https://twitter.com/GloryofCupid/</a>	Checked
Telegram	<a href="https://t.me/glorycupid/">https://t.me/glorycupid/</a>	Checked
Discord	<a href="https://discord.com/invite/jGYWDqdXNq">https://discord.com/invite/jGYWDqdXNq</a>	Checked

## Website Review

 Glory of Cupid


HOME GAME CENTER AUDIT REPORT TEAM KYC WHITE PAPER PINK PRESALE CONTACT US

GAMEFI ECOSYSTEM

### There are some \$CUPID you don't want to miss.

The wisdom model of Glory of Cupid is the most novel flow chain game at present. It will launch the first wisdom cultivation chain game of the blockchain: Glory of Cupid

The game application of Glory of Cupid can participate in zero threshold to obtain token rewards, and can also obtain higher token rewards through pass breaking mode, PK competition and challenge. You can also submit a reward in the mutual aid market, and let the super master help you complete the challenge. If the accumulated points meet the conditions, you can divide the huge bonus pool.

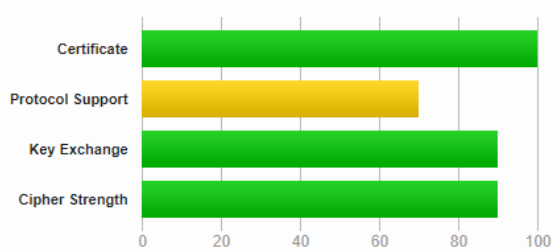


[PLAY NOW](#)

Super Bonus pool: **95,674,662** CUPID

### Summary

#### Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports TLS 1.1. Grade capped to B. [MORE INFO »](#)

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

## Certificate #1: RSA 2048 bits (SHA256withRSA)



### Server Key and Certificate #1



Subject	www.glorycupid.win Fingerprint SHA256: a83bde16c3147f68fa3eed0aecf076f0b2e760c8bee9cafa3265e23e4997785d Pin SHA256: iUCi1Rpuuykr/sPD8jHaU5k7pt/yRVewURPeHWpAs0=
Common names	www.glorycupid.win
Alternative names	www.glorycupid.win
Serial Number	03e31d10babae07d62699d95caa71aef9aa5
Valid from	Fri, 02 Sep 2022 02:34:50 UTC
Valid until	Thu, 01 Dec 2022 02:34:49 UTC (expires in 2 months and 23 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: <a href="http://r3.i.lencr.org/">http://r3.i.lencr.org/</a>
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: <a href="http://r3.o.lencr.org">http://r3.o.lencr.org</a>
Revocation status	Good (not revoked)
DNS CAA	No ( <a href="#">more info</a> )
Trusted	Yes <a href="#">Mozilla</a> <a href="#">Apple</a> <a href="#">Android</a> <a href="#">Java</a> <a href="#">Windows</a>

- Mobile Friendly
- Contains no code errors
- SSL is secured
- No spelling errors



## Audit Conclusion

- The owner cannot pause trading.
- The owner cannot mint new tokens.
- The owner cannot add blacklist users.
- The owner cannot set the max transaction amount.
- The owner cannot change the buy fee up to 7% for 14 days after launch.
- The owner cannot change the sell fee up to 8% for 14 days after launch.
- The owner cannot change the wallet transfer fee up to 8% for 14 days after launch.

(All functions cannot be used if the ownership is renounced)

## AUDIT IS PASSED