HACKEN

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: Creampye
Date: May 3rd, 2021

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.

The report containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed - upon a decision of the Customer.

Document

Name	Smart Contract Code Review and Security Analysis Report for Creampye - Initial Audit
Approved by	Andrew Matiukhin | CTO Hacken OU
Type	BEP20 Token with Fees, LP
Platform	Binance Smart Chain / Solidity
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Deployed mainnet	https://bscscan.com/address/0xaad87f47cdea777faf87e7602e91e3a6afbe4d57#code
Timeline	30 APRIL 2021 - 03 MAY 2021
Changelog	03 MAY 2021 - INITIAL AUDIT

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Table of contents

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Introduction

Hacken OÜ (Consultant) was contracted by Creampye (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on May 3rd, 2021.

Scope

The scope of the project is the smart contract deployed in the Binance Smart Chain mainnet and the WhitePaper:

https://bscscan.com/address/0xaad87f47cdea777faf87e7602e91e3a6afbe4d57#code
&
https://drive.google.com/file/d/1lJXDmbDGoQUbgIqnSY8XxqEzaWO-2HXk/view
WhitePaper_v1.1.1.pdf (**md5:** 07f4d33bd5937b6bad7a6306b6ab6f35)

We have checked the smart contract for the accordance with the WhitePape. We have scanned these smart contracts for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that are considered:

Category	Check Item
Code review	▪ Reentrancy ▪ Ownership Takeover ▪ Timestamp Dependence ▪ Gas Limit and Loops ▪ DoS with (Unexpected) Throw ▪ DoS with Block Gas Limit ▪ Transaction-Ordering Dependence ▪ Style guide violation ▪ Costly Loop ▪ ERC20 API violation ▪ Unchecked external call ▪ Unchecked math ▪ Unsafe type inference ▪ Implicit visibility level ▪ Deployment Consistency ▪ Repository Consistency ▪ Data Consistency

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Functional review	▪ Business Logics Review ▪ Functionality Checks ▪ Access Control & Authorization ▪ Escrow manipulation ▪ Token Supply manipulation ▪ Asset’s integrity ▪ User Balances manipulation ▪ Kill-Switch Mechanism ▪ Operation Trails & Event Generation

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Executive Summary

According to the assessment, the Customer's smart contract is secured and fully according to the provided WhitePaper

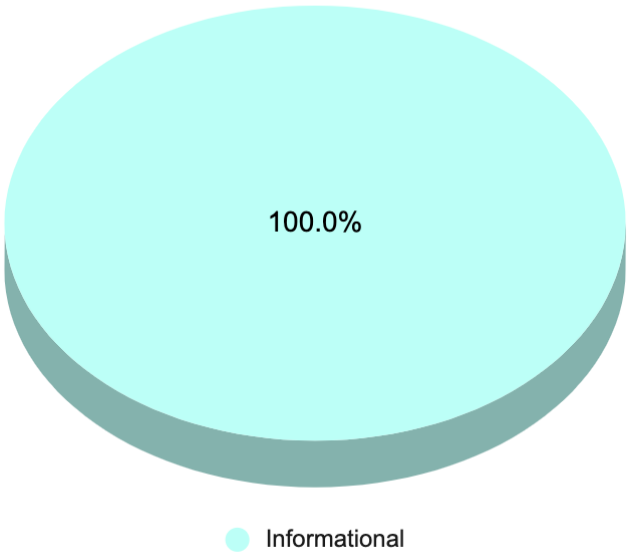
Insecure	Poor secured	Secured	Well-secured

You are here

Our team performed an analysis of code functionality, manual audit, and automated checks with Mythril and Slither. Also, the team has checked the accordance to the provided WhitePaper. All issues found during automated analysis were manually reviewed, and important vulnerabilities are presented in the Audit overview section. All found issues can be found in the Audit overview section.

Security engineers found **5** informational issues during the first review.

Graph 1. The distribution of vulnerabilities after the first review.



Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations, and info statements can't affect smart contract execution and can be ignored.

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Audit overview

Critical

No Critical severity issues were found.

High

No High severity issues were found.

Medium

No Medium severity issues were found.

Low

No Low severity issues were found.

Lowest / Code style / Best Practice

1. **Vulnerability:** Function Initializing State

   The immediate initialization of state variables through function calls that are not pure or constant.

   Recommendation: Please consider removing initialization of state variables via non-constant state variables or function calls. Specify them as immutable and initialize in the constructor instead.

   Lines: #691-693

```
uint256 private constant MAX = ~uint256(0);
uint256 private _tTotal = 1000000000 * 10**6 * 10**18;
uint256 private _rTotal = (MAX - (MAX % _tTotal));
```

2. **Vulnerability:** Too many digits

   Literals with many digits are difficult to read and review. Please consider using *Ether Units* or *Scientific Notation* for better readability. Ex.:
   - 500_000_000_000 ether
   - 5e11 ether

   Lines: #692

```
uint256 private _tTotal = 1000000000 * 10**6 * 10**18;
```

Lines: #712

```
uint256 private numTokensSellToAddToLiquidity = 500000000000 * 10**18;
```

3. **Vulnerability:** State variable that should be constant

   Constant state variables should be declared constant to save gas.

   Lines: #692

   ```
   uint256 private _tTotal = 1000000000 * 10**6 * 10**18;
   ```

   Lines: #696-698

   ```
   string private _name = "CREAMPYE";
   string private _symbol = "PYE";
   uint8 private _decimals = 18;
   ```

   Lines: #712

   ```
   uint256 private numTokensSellToAddToLiquidity = 500000000000 * 10**18;
   ```

4. **Vulnerability:** Public function that could be declared external

   public functions that are never called by the contract should be declared **external** to save gas.

   Lines: #748

   ```
   function name() public view returns (string memory) {
   ```

   Lines: #752

   ```
   function symbol() public view returns (string memory) {
   ```

   Lines: #756

   ```
   function decimals() public view returns (uint8) {
   ```

   Lines: #760

   ```
   function totalSupply() public view override returns (uint256) {
   ```

   Lines: #769

   ```
   function transfer(address recipient, uint256 amount) public override
   returns (bool) {
   ```

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Lines: #774

```
function allowance(address owner, address spender) public view override
returns (uint256) {
```

Lines: #778

```
function approve(address spender, uint256 amount) public override
returns (bool) {
```

Lines: #783

```
function transferFrom(address sender, address recipient, uint256
amount) public override returns (bool) {
```

Lines: #789

```
function increaseAllowance(address spender, uint256 addedValue) public
virtual returns (bool) {
```

Lines: #794

```
function decreaseAllowance(address spender, uint256 subtractedValue)
public virtual returns (bool) {
```

Lines: #799

```
function isExcludedFromReward(address account) public view returns
(bool) {
```

Lines: #803

```
function totalFees() public view returns (uint256) {
```

Lines: #808

```
function reflectionFromToken(uint256 tAmount, bool deductTransferFee)
public view returns(uint256) {
```

Lines: #825

```
function excludeFromReward(address account) public onlyOwner() {
```

Lines: #848

```
function excludeFromFee(address account) public onlyOwner {
```

Lines: #852

```
function includeInFee(address account) public onlyOwner {
```

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Lines: #872

```
function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {
```

Lines: #979

```
function isExcludedFromFee(address account) public view returns(bool) {
```

5. Lines 733, 783, 785, 794, 795, 808, 887-889, 901, 918 and 1101 are above the recommended maximum line length.

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Conclusion

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security engineers found **5** informational issues during the first review.

Category	Check Items	Comments
Code Review	Style guide violation	➔ public function that could be declared external ➔ state variable should be constant ➔ too many digits ➔ maximum line length ➔ function initializing state

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Disclaimers

Hacken Disclaimer

The smart contracts given for audit have been analyzed in accordance with the best industry practices at the date of this report, in relation to cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only - we recommend proceeding with several independent audits and a public bug bounty program to ensure security of smart contracts.

Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have its vulnerabilities that can lead to hacks. Thus, the audit can't guarantee the explicit security of the audited smart contracts.