Assure DeFi®

THE VERIFICATION GOLD STANDARD

Security Assessment

PredictingAI

Date: 16/04/2024

Audit Status: FAILED

Audit Edition: Advanced

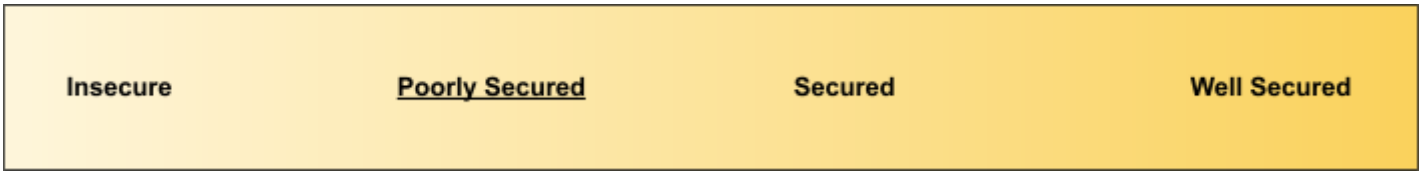
Risk Analysis

Vulnerability summary

Classification	Description
High	High-level vulnerabilities can result in the loss of assets or manipulation of data.
Medium	Medium-level vulnerabilities can be challenging to exploit, but they still have a considerable impact on smart contract execution, such as allowing public access to critical functions.
Low	Low-level vulnerabilities are primarily associated with outdated or unused code snippets that generally do not significantly impact execution, sometimes they can be ignored.
Informational	Informational vulnerabilities, code style violations, and informational statements do not affect smart contract execution and can typically be disregarded.

Executive Summary

According to the Assure assessment, the Customer's smart contract is **Poorly Secured.**



Scope

Target Code And Revision

For this audit, we performed research, investigation, and review of the PredictingAI contracts followed by issue reporting, along with mitigation and remediation instructions outlined in this report.

Target Code And Revision

Project	Assure
Language	Solidity
Codebase	PredictCryptoFinal2.sol [sha256] - *46a6ec5c9df5e9edec14e76567ae8139d18c66ff6e796b4292e66d32391fd5ab*
Audit Methodology	Static, Manual

Attacks made to the contract

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices.

Category	Item
Code review & Functional Review	• Compiler warnings. • Race conditions and Reentrancy. Cross-function race conditions. • Possible delays in data delivery. • Oracle calls. • Front running. • Timestamp dependence. • Integer Overflow and Underflow. • DoS with Revert. • DoS with block gas limit. • Methods execution permissions. • Economy model. • Private user data leaks. • Malicious Event log. • Scoping and Declarations. • Uninitialized storage pointers. • Arithmetic accuracy. • Design Logic. • Cross-function race conditions. • Safe Zeppelin module. • Fallback function security. • Overpowered functions / Owner privileges

AUDIT OVERVIEW

HIGH

---

1. Addressing High Fee Values in Sell Transfers for Test Contract

Contract: PREDICTCRYPTO.sol

Functions: launchSequence()

Issue: The function launchSequence() fails to update buy and sell taxes after a certain number of blocks, resulting in excessively high fee values for sell transfers.

Mitigation: Force to update sell fees after some blocks/transactions or limit the sell fee to be under 20%.

MEDIUM

No medium severity issues were found.

LOW

No low severity issues were found.

INFORMATIONAL

No Informational severity issues were found.

Testing coverage

During the testing phase, custom use cases were written to cover all the logic of contracts. *Check “Annexes” to see the testing code.*

Testing PredictingAI Contract:

```
tests/test_predict_crypto.py::test_transfer RUNNING
Transaction sent: 0x3a583576be507cab3a1557e497cdee2bc79f81b248a07df331d81e4e5bcffa2f
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 9
  UniswapV2Factory.constructor confirmed   Block: 12   Gas used: 2412730 (20.11%)
  UniswapV2Factory deployed at: 0xa3B53dDCd2E3fC28e8E130288F2aBD8d5EE37472

Transaction sent: 0x754bd5ff2830b5c240a927ab06bd5abc2d0cac46798f45c34caf5aad9603bele
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 10
  WETH9.constructor confirmed   Block: 13   Gas used: 476546 (3.97%)
  WETH9 deployed at: 0xb6286fAFd0451320ad6A8143089b216C2152c025

Transaction sent: 0x7a47d461f211cf4961df0cfff3f1a9810ef81b1c3e5cd5c80ef8867f6a4e7efd
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 11
  UniswapV2Router02.constructor confirmed   Block: 14   Gas used: 3895430 (32.46%)
  UniswapV2Router02 deployed at: 0x7a3d735ee6873f17Dbdcab1d51B604928dc10d92

Transaction sent: 0xa7ff10bf36a3d734318ff363ae4974b1539aa78ca07a6183fe4238eb5045cc3d
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 12
  PREDICTCRYPTO.constructor confirmed   Block: 15   Gas used: 4055268 (33.79%)
  PREDICTCRYPTO deployed at: 0x2c15A315610Bfa5248E4CbCbd693320e9D8E03Cc

Transaction sent: 0x3b8d1829225340027e53bf71ff7a179772601a1d1a57263aba6042df69d238d9
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0
  PREDICTCRYPTO.transfer confirmed (reverted)   Block: 16   Gas used: 22187 (0.18%)

Transaction sent: 0x50d26857814fe2fc48a6b3e6b9569a5e87d7140bda1f4d9c7b2530f67f7fb690
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2
  PREDICTCRYPTO.transfer confirmed (reverted)   Block: 17   Gas used: 21982 (0.18%)

Transaction sent: 0xefa867f7a01a7607c355a79fef6f3dfc56e9df2647bf0a76ee9ec8da6f1ef46e
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 3
  PREDICTCRYPTO.transfer confirmed (reverted)   Block: 18   Gas used: 22161 (0.18%)

Transaction sent: 0x38cb8dc66c833e3390505cbd4d521ec505d26334bc8c6cf08fe3c659634d752e
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 13
  PREDICTCRYPTO.blacklistAddress confirmed   Block: 19   Gas used: 46250 (0.39%)

Transaction sent: 0x4cfff8e95d771146cdd138e891c8450c591b1c73467d557983ba6a7af297a86d
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 4
  PREDICTCRYPTO.transfer confirmed (reverted)   Block: 20   Gas used: 24916 (0.21%)

Transaction sent: 0xf7ade8a607bdecd7191bd3e99664872809e2e5b0742f58f2eec57ee0e958b14f
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5
  PREDICTCRYPTO.transfer confirmed (reverted)   Block: 21   Gas used: 27572 (0.23%)

Transaction sent: 0x58bde6debe61e7f36d12e03555194412cd6fc370bd140c6d6ee93a775c1ca7a6
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 14
  PREDICTCRYPTO.transfer confirmed   Block: 22   Gas used: 54816 (0.46%)

Transaction sent: 0xa4d72dbb60a00c098569208a97454ef14f4f7fa6f7c2d5ac3f9d553cf3263c72
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6
  PREDICTCRYPTO.launchSequence confirmed (Ownable: caller is not the owner)   Block: 23   Gas used: 22285 (0.19%)

Transaction sent: 0xb53ece0a84158542a86d4e05ee7f3711f6dfdea98a33656adb2a327d8e48464c
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 15
  PREDICTCRYPTO.launchSequence confirmed   Block: 24   Gas used: 35509 (0.30%)
```

```
Transaction sent: 0x75967109887989818179ed3a96b14b406fe92460782b10dec16aa72db8074d99
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7
  PREDICTCRYPTO.transfer confirmed   Block: 25   Gas used: 56592 (0.47%)

Transaction sent: 0x0fa849b20c1518492917cbd57ccd457cfed46e6f552f98436c6d940c1999d8ee
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8
  PREDICTCRYPTO.transfer confirmed   Block: 26   Gas used: 126838 (1.06%)

Transaction sent: 0xd79e8f1a0837aa458da25cc17c93a43ee2249330511523270a360b48af7c4fdf
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 9
  PREDICTCRYPTO.updateBuyFees confirmed (Ownable: caller is not the owner)   Block: 27   Gas used: 23212 (0.19%)

Transaction sent: 0x074b987f7007cefa7239e7b54e3612366eed02d3d6701fae8e7a447735fd473a
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 16
  PREDICTCRYPTO.updateBuyFees confirmed   Block: 28   Gas used: 33793 (0.28%)

Transaction sent: 0x83c3592ef2915171257f4c77892ca298c47b97c1a870ab418c7cfacf63f38eae
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 10
  PREDICTCRYPTO.transfer confirmed   Block: 29   Gas used: 66838 (0.56%)

Transaction sent: 0x1f8f329be81acc76bba4cb007f007dc154a0b0600184b76207e149e5207e6605
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1
  PREDICTCRYPTO.transfer confirmed   Block: 30   Gas used: 63435 (0.53%)

tests/test_predict_crypto.py::test_transfer PASSED
```

```
tests/test_predict_crypto.py::test_set_marketing_wallet RUNNING
Transaction sent: 0x547684818babedc1e5f592605688f0e8d134554ab13945faec6bf8306be33349
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 17
  UniswapV2Factory.constructor confirmed   Block: 31   Gas used: 2412730 (20.11%)
  UniswapV2Factory deployed at: 0xFbD588c72B438faD4Cf7cD879c8F730Faa213Da0

Transaction sent: 0x1e72f2849d6919db2ca9b16eb2ac5f4ca2c3e69cb763a504d5747e5b6c2a253c
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 18
  WETH9.constructor confirmed   Block: 32   Gas used: 476546 (3.97%)
  WETH9 deployed at: 0xed00238F9A0F7b4d93842033cdF56cCB32C781c2

Transaction sent: 0xf8cc052aa0f63d2e70039ace07069dd6aef5c06dd1a34b2bdf86a405a950d429
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 19
  UniswapV2Router02.constructor confirmed   Block: 33   Gas used: 3895418 (32.46%)
  UniswapV2Router02 deployed at: 0xDae02e4fE488952cFB8c95177154D188647a0146

Transaction sent: 0x06d59f1b5f42434043e4353c4e01453113e407f43912fdbcc66a5d60423c9f1a
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 20
  PREDICTCRYPTO.constructor confirmed   Block: 34   Gas used: 4055268 (33.79%)
  PREDICTCRYPTO deployed at: 0xdCF93F11ef216cEC9C07fd31dD801c9b2b39Afb4

Transaction sent: 0xf08ed9b258abee8c8e8be4c94b629e557a568cedf03d6dc2f935f97a9de2c057
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 11
  PREDICTCRYPTO.setMarketingWallet confirmed (Ownable: caller is not the owner)   Block: 35   Gas used: 22748 (0.19%)

Transaction sent: 0x452483ffc8379a34ad0ddf8ee5af716f6f679dd8b30e319021839ee7321a09ac
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 21
  PREDICTCRYPTO.setMarketingWallet confirmed (reverted)   Block: 36   Gas used: 22495 (0.19%)

Transaction sent: 0x2ab561cd324e7b481cdc0d9f24bc56a3c9792ca97d6995f9304a8c3dd1e2e90c
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 22
  PREDICTCRYPTO.setMarketingWallet confirmed   Block: 37   Gas used: 42294 (0.35%)

tests/test_predict_crypto.py::test_set_marketing_wallet PASSED
```

```
tests/test_predict_crypto.py::test_set_liquidity_pool RUNNING
Transaction sent: 0xf30e17983657fa41ebfe82a700248229eea1657869527e6c7636247bc8100d0c
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 23
  UniswapV2Factory.constructor confirmed   Block: 38   Gas used: 2412730 (20.11%)
  UniswapV2Factory deployed at: 0x4D1B781ce59B8C184F63B99D39d6719A522f46B5

Transaction sent: 0xaaaafa95655ce2167e67aefbcf6bf50a63148a4100abb0f6991cafa5419331ed8
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 24
  WETH9.constructor confirmed   Block: 39   Gas used: 476546 (3.97%)
  WETH9 deployed at: 0xf9C8Cf55f2E520B08d869df7bc76aa3d3ddDF913

Transaction sent: 0x1502d9e27f19de190c9309e8b07ea9fc2b78c5f114a6de2a3b045f88cc2d456e
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 25
  UniswapV2Router02.constructor confirmed   Block: 40   Gas used: 3895430 (32.46%)
  UniswapV2Router02 deployed at: 0x654f70d8442EA18904FA1AD79114f7250F7E9336

Transaction sent: 0x9d060bc1799e0ae1bba3984d667893073adf79540a98493980cda34a07f05be5
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 26
  PREDICTCRYPTO.constructor confirmed   Block: 41   Gas used: 4055268 (33.79%)
  PREDICTCRYPTO deployed at: 0xADeD61D42dE86f9058386D1D0d739d20C7eAfC43

Transaction sent: 0xe301ec2b035139ce78e133a38a949adc879b770eb7a71a7569320fec0c3db769
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 12
  PREDICTCRYPTO.setLiquidityPool confirmed (Ownable: caller is not the owner)   Block: 42   Gas used: 22728 (0.19%)

Transaction sent: 0x73a6dad343e417f3fd9dcd26d8197a7f4cd47e0cc9317136df03d7170ea98f32
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 27
  PREDICTCRYPTO.setLiquidityPool confirmed (reverted)   Block: 43   Gas used: 22475 (0.19%)

Transaction sent: 0xcc7bdc1a52475b223be46be4208765c5d466c2b73c59aa5d1cf71feb5bled491
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 28
  PREDICTCRYPTO.setLiquidityPool confirmed   Block: 44   Gas used: 29687 (0.25%)

tests/test_predict_crypto.py::test_set_liquidity_pool PASSED
```

```
tests/test_predict_crypto.py::test_change_swap_back_settings RUNNING
Transaction sent: 0xa254638826cdc1136c1cd1165b68e7ded0fda535f21a47a485908cf6ee735fad
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 29
  UniswapV2Factory.constructor confirmed   Block: 45   Gas used: 2412730 (20.11%)
  UniswapV2Factory deployed at: 0x42E8D004c84E6B5Bad559D3b5CE7947AADb9E0bc

Transaction sent: 0x8c4376f2db454f388f7564e9c2083830a2cad7763b32e7c94c82845e2f18398c
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 30
  WETH9.constructor confirmed   Block: 46   Gas used: 476546 (3.97%)
  WETH9 deployed at: 0xF06D5f5BfFFCB6a52c84cfebc03AD35637728E73

Transaction sent: 0x6d5c0a2ffe18c70421d12536dd5be49f30fed2fed100d84cb05caaa3cb3451f7
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 31
  UniswapV2Router02.constructor confirmed   Block: 47   Gas used: 3895430 (32.46%)
  UniswapV2Router02 deployed at: 0x82c83b7f88aef2eD99d4869D547b6ED28e69C8df

Transaction sent: 0xf92a992c0f58b201995e8b4ddf22feb23fdbe9b950f3be685d6d059eda012bb0
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 32
  PREDICTCRYPTO.constructor confirmed   Block: 48   Gas used: 4055268 (33.79%)
  PREDICTCRYPTO deployed at: 0x724Ca58E1e6e64BFB1E15d7Eec0fe1E5f581c7bD

Transaction sent: 0xe4bf55bbd0e9952f198f955a906081707f3580af29d40a7d4112a8b5126911d1
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 13
  PREDICTCRYPTO.changeSwapBackSettings confirmed (Ownable: caller is not the owner)   Block: 49   Gas used: 22766 (0.19%)

Transaction sent: 0xed6e5ac3232881205d9794b4b7c66b18fd33488ab1aec237fcbc5c5b4f267cea
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 33
  PREDICTCRYPTO.changeSwapBackSettings confirmed (reverted)   Block: 50   Gas used: 22708 (0.19%)

Transaction sent: 0x22ca95699ec107b7fe61cd9970c259114edc93ac6d1b7b99218ca862d0bc99ca
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 34
  PREDICTCRYPTO.changeSwapBackSettings confirmed   Block: 51   Gas used: 30718 (0.26%)

tests/test_predict_crypto.py::test_change_swap_back_settings PASSED
```

```
tests/test_predict_crypto.py::test_clear_stuck_eth RUNNING
Transaction sent: 0x88bcc5ec517fc6d00a705470aa0a513ea0540221260b2fb0052b506871d46dbc
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 35
  UniswapV2Factory.constructor confirmed   Block: 52   Gas used: 2412730 (20.11%)
  UniswapV2Factory deployed at: 0xbc8eCccb89650c3E796e803CB009BF9b898CB359

Transaction sent: 0x293c7e58e0f21cd1fc43bf5a9f7fddf0cffda62ea3254daa77ad9a81fa8351b5
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 36
  WETH9.constructor confirmed   Block: 53   Gas used: 476546 (3.97%)
  WETH9 deployed at: 0x741e3E1f81041c62C2A97d0b6E567AcaB09A6232

Transaction sent: 0xde7b0e43a9155250a11264cdaba2f9ad3063225982c2e13ee3dece033c7182eb
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 37
  UniswapV2Router02.constructor confirmed   Block: 54   Gas used: 3895430 (32.46%)
  UniswapV2Router02 deployed at: 0x4B0FccF53589c1F185B35db88bB315a0bBF9a3e0

Transaction sent: 0xd1330b787b5f8decbae17cf26fdddc3e4d5216375c6151e2b8e596626f7f378e
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 38
  PREDICTCRYPTO.constructor confirmed   Block: 55   Gas used: 4055258 (33.79%)
  PREDICTCRYPTO deployed at: 0xFE0F4Cf81B5c0a6Fd65a610FD9488F33aE9095cB

Transaction sent: 0x1313eb8a47e73c9134f77bf2e421ff17e9929b1d263887b4aa9191ac9223a7e1
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 14
  PREDICTCRYPTO.clearStuckETH confirmed (Ownable: caller is not the owner)   Block: 56   Gas used: 22283 (0.19%)

Transaction sent: 0xb20ca1ad725d752ecda4c3927b3f4dd159234df847b267d98acf2b40a98cad2b
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 39
  PREDICTCRYPTO.clearStuckETH confirmed (reverted)   Block: 57   Gas used: 22254 (0.19%)

Transaction sent: 0x35e10dad45b9d337d74900c48c221f3a5a18c5a22533868e374096727e8c1b7c
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 40
  PREDICTCRYPTO.clearStuckETH confirmed   Block: 59   Gas used: 56637 (0.47%)

tests/test_predict_crypto.py::test_clear_stuck_eth PASSED
```

Annexes

Testing code:

Test_predict_crypto.py:

```
from brownie import (
    reverts,
)

from brownie.network.contract import Contract

from scripts.helpful_scripts import (
    ZERO_ADDRESS,
    DAY_TIMESTAMP,
    get_account,
    get_timestamp,
    get_chain_number,
    increase_timestamp
)

from scripts.deploy import (
    deploy_weth,
    deploy_router,
    deploy_factory,
    deploy_liquidity,
    deploy_predict
)

def test_blacklist(only_local):
```

```
    # Arrange
    owner = get_account(0)
    other = get_account(1)
    extra = get_account(2)

    # Deploy contracts
    factory = deploy_factory(owner, owner)
    weth = deploy_weth(owner)
    router = deploy_router(owner, factory.address, weth.address)
    predict = deploy_predict(owner, router.address)

    with reverts("Ownable: caller is not the owner"):
        predict.blacklistAddress(ZERO_ADDRESS, False, {"from": other})
    with reverts("InvalidAddress: "):
        predict.blacklistAddress(ZERO_ADDRESS, False, {"from": owner})
    with reverts("InvalidAddress: "):
        predict.blacklistAddress(predict.pair(), False, {"from": owner})

    tx = predict.blacklistAddress(extra, True, {"from": owner})
    assert tx.events['Blacklisted'][0]['_wallet'] == extra
    assert tx.events['Blacklisted'][0]['_status'] == True

    with reverts("Ownable: caller is not the owner"):
        predict.disableBlacklist({"from": other})
    predict.disableBlacklist({"from": owner})
    with reverts("Unavailable: "):
        predict.blacklistAddress(extra, False, {"from": owner})
```

```python
def test_transfer(only_local):
    # Arrange
    owner = get_account(0)
    other = get_account(1)
    extra = get_account(2)
    blacklisted = get_account(4)

    # Deploy contracts
    factory = deploy_factory(owner, owner)
    weth = deploy_weth(owner)
    router = deploy_router(owner, factory.address, weth.address)
    predict = deploy_predict(owner, router.address)

    with reverts("TransferFromZeroAddress: "):
        predict.transfer(other, 1e18, {"from": ZERO_ADDRESS})
    with reverts("TransferToZeroAddress: "):
        predict.transfer(ZERO_ADDRESS, 1e18, {"from": other})
    with reverts("InvalidAmount: "):
        predict.transfer(extra, 0, {"from": other})
    predict.blacklistAddress(blacklisted, True, {"from": owner})
    with reverts("Unavailable: "):
        predict.transfer(blacklisted, 1e18, {"from": other})
    with reverts("Unavailable: "):
        predict.transfer(extra, 1e18, {"from": other})
    tx = predict.transfer(other, 5e18, {"from": owner})
    assert tx.events['Transfer'][0]['from'] == owner
    assert tx.events['Transfer'][0]['to'] == other
    assert tx.events['Transfer'][0]['value'] == 5e18
```

```
with reverts("Ownable: caller is not the owner"):
    predict.launchSequence({"from": other})
predict.launchSequence({"from": owner})
tx = predict.transfer(extra, 1e18, {"from": other})
assert tx.events['Transfer'][0]['from'] == other
assert tx.events['Transfer'][0]['to'] == extra
assert tx.events['Transfer'][0]['value'] == 1e18

# sell
tx = predict.transfer(predict.pair(), 1e18, {"from": other})
assert tx.events['Transfer'][0]['from'] == other
assert tx.events['Transfer'][0]['to'] == predict.address
assert tx.events['Transfer'][0]['value'] == 0.25e18
assert tx.events['Transfer'][1]['from'] == other
assert tx.events['Transfer'][1]['to'] == predict.pair()
assert tx.events['Transfer'][1]['value'] == 0.75e18

with reverts("Ownable: caller is not the owner"):
    predict.updateBuyFees(300, 200, 300, 200, {"from": other})
predict.updateBuyFees(300, 200, 300, 200, {"from": owner})

tx = predict.transfer(predict.pair(), 1e18, {"from": other})
assert tx.events['Transfer'][0]['from'] == other
assert tx.events['Transfer'][0]['to'] == predict.address
assert tx.events['Transfer'][0]['value'] == 0.05e18
assert tx.events['Transfer'][1]['from'] == other
assert tx.events['Transfer'][1]['to'] == predict.pair()
```

```
    assert tx.events['Transfer'][1]['value'] == 0.95e18


    # buy
    tx = predict.transfer(other, 1e18, {"from": predict.pair()})
    assert tx.events['Transfer'][0]['from'] == predict.pair()
    assert tx.events['Transfer'][0]['to'] == predict.address
    assert tx.events['Transfer'][0]['value'] == 0.05e18
    assert tx.events['Transfer'][1]['from'] == predict.pair()
    assert tx.events['Transfer'][1]['to'] == other
    assert tx.events['Transfer'][1]['value'] == 0.95e18


def test_set_marketing_wallet(only_local):
    # Arrange
    owner = get_account(0)
    other = get_account(1)
    extra = get_account(2)


    # Deploy contracts
    factory = deploy_factory(owner, owner)
    weth = deploy_weth(owner)
    router = deploy_router(owner, factory.address, weth.address)
    predict = deploy_predict(owner, router.address)


    with reverts("Ownable: caller is not the owner"):
        predict.setMarketingWallet(extra, {"from": other})
    with reverts("InvalidAddress: "):
        predict.setMarketingWallet(ZERO_ADDRESS, {"from": owner})
```

```
    assert predict.marketingWallet() != other
    predict.setMarketingWallet(other, {"from": owner})
    assert predict.marketingWallet() == other


def test_set_liquidity_pool(only_local):
    # Arrange
    owner = get_account(0)
    other = get_account(1)
    fake_liquidity = get_account(2)

    # Deploy contracts
    factory = deploy_factory(owner, owner)
    weth = deploy_weth(owner)
    router = deploy_router(owner, factory.address, weth.address)
    predict = deploy_predict(owner, router.address)

    with reverts("Ownable: caller is not the owner"):
        predict.setLiquidityPool(fake_liquidity, {"from": other})
    with reverts("InvalidAddress: "):
        predict.setLiquidityPool(ZERO_ADDRESS, {"from": owner})

    assert predict.liquidityPool() != fake_liquidity
    predict.setLiquidityPool(fake_liquidity, {"from": owner})
    assert predict.liquidityPool() == fake_liquidity


def test_change_swap_back_settings(only_local):
    # Arrange
    owner = get_account(0)
```

```
    other = get_account(1)


    # Deploy contracts
    factory = deploy_factory(owner, owner)
    weth = deploy_weth(owner)
    router = deploy_router(owner, factory.address, weth.address)
    predict = deploy_predict(owner, router.address)


    with reverts("Ownable: caller is not the owner"):
        predict.changeSwapBackSettings(True, 12000e18, {"from": other})
    with reverts("InvalidAmount: "):
        predict.changeSwapBackSettings(True, 10e18, {"from": owner})


    predict.changeSwapBackSettings(True, 11000e18, {"from": owner})
    assert predict.swapThreshold() == 11000e18


def test_clear_stuck_eth(only_local):
    # Arrange
    owner = get_account(0)
    other = get_account(1)


    # Deploy contracts
    factory = deploy_factory(owner, owner)
    weth = deploy_weth(owner)
    router = deploy_router(owner, factory.address, weth.address)
    predict = deploy_predict(owner, router.address)


    with reverts("Ownable: caller is not the owner"):
```

```
        predict.clearStuckETH({"from": other})

    with reverts("InvalidAmount: "):

        predict.clearStuckETH({"from": owner})



    other.transfer(predict.address, "1 ether")

    tx = predict.clearStuckETH({"from": owner})

    assert tx.events['StuckETHCleared'][0]['_amount'] == 1e18
```

Technical Findings Summary

Findings

Vulnerability Level	Total	Pending	Not Apply	Acknowledged	Partially Fixed	Fixed
High	1					
Medium	0					
Low	0					
Informational	0					

Assessment Results

Score Results

Review	Score
Global Score	**80/100**
Assure KYC	https://assuredefi.com/projects/predictingai
Audit Score	75/100

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 84 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below. The Global Score is a combination of the evaluations obtained between having or not having KYC and the type of contract audited together with its manual audit.

Audit FAILED

Following our comprehensive security audit of the token contract for PredictingAI project,
We regret to inform you that the project has not met the required security standards due to identified high vulnerability within the contract functions. The issue that was identified must be resolved before deployment.

Disclaimer

Assure Defi has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocating for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any person reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided ‘as is, and Assure Defi is under no covenant to audit completeness, accuracy, or solidity of the contracts. In no event will Assure Defi or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by Assure Defi are subject to dependencies and are under continuing development. You agree that your access 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 with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.