Coinsult

Advanced Manual Smart Contract Audit

FitScrypt

Project: FitScrypt

Website: https://fitscrypt.com/

Low-Risk	Medium-Risk	High-Risk
2 low-risk code issues found	0 medium-risk code issues found	0 high-risk code issues found

Contract Address

0x6D13aA4FDB8C13916C32D54E9B8ECd40cD95d46C

Disclaimer

Coinsult is not responsible if a project turns out to be a scam, rug-pull or honeypot. We only provide a detailed analysis for your own research.

Coinsult is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

The information provided in this audit is for informational purposes only and should not be considered investment advice. Coinsult does not endorse, recommend, support or suggest to invest in any project.

Coinsult can not be held responsible for when a project turns out to be a rug-pull, honeypot or scam.

Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0xff1f960cc0da4e8796be118f7932a9c6f8004dc0	79,706,500,000	53.1377%
2	Unicrypt: Token Vesting	50,000,000,000	33.3333%
3	0x0b889ac95dd2afd9e9df8f865df168097e71908e	20,117,885,348.720521826392373307	13.4119%
4	0xe9746816aee9b580200ce02bfe5dc335a04e5df8	175,614,651.279478173607626693	0.1171%

Source Code

Coinsult was comissioned by FitScrypt to perform an audit based on the following smart contract:

https://bscscan.com/address/0x6d13aa4fdb8c13916c32d54e9b8ecd40cd95d46c#code

Manual Code Review

In this audit report we will highlight all these issues:

🟢 Low-Risk

2 low-risk code
issues found

🟡 Medium-Risk

0 medium-risk code
issues found

🔴 High-Risk

0 high-risk code
issues found

The detailed report continues on the next page...

🟢 **Low-Risk:** Could be fixed, will not bring problems.

Non-active mint function can be removed

```
function mint(address account, uint256 amount) external onlyOwner {
    require(canMint, "the mint function isn't activated");
    _mint(account, amount);
}
```

Recommendation

Even though the contract has a ‘public’ mint function. It cannot be used because the boolean ‘canMint’ is set to False, and can never be changed by the contract owner.

Automatic scanning tools will still pick this up as a mint function and this could cause FUD. It should therefore be removed from the contract.

🟢 **Low-Risk:** Could be fixed, will not bring problems.

Missing events arithmetic

Detect missing events for critical arithmetic parameters.

```
function burn(address account, uint256 amount) external onlyOwner {
    require(canBurn, "the burn function isn't activated");
    _burn(account, amount);
}
```

Recommendation

Emit an event for critical parameter changes.

Exploit scenario

```
contract C {

  modifier onlyAdmin {
    if (msg.sender != owner) throw;
    _;
  }

  function updateOwner(address newOwner) onlyAdmin external {
    owner = newOwner;
  }
}
```

`updateOwner()` has no event, so it is difficult to track off-chain changes in the buy price.

Owner privileges

- Owner cannot set fees higher than 25%
- Owner cannot pause trading
- Owner cannot change max transaction amount

⚠️ Owner can burn tokens using the burn function

⚠️ Owner can use the mint function, but it will revert since the ‘canMint’ boolean is set to False and cannot be changed

Extra notes by the team

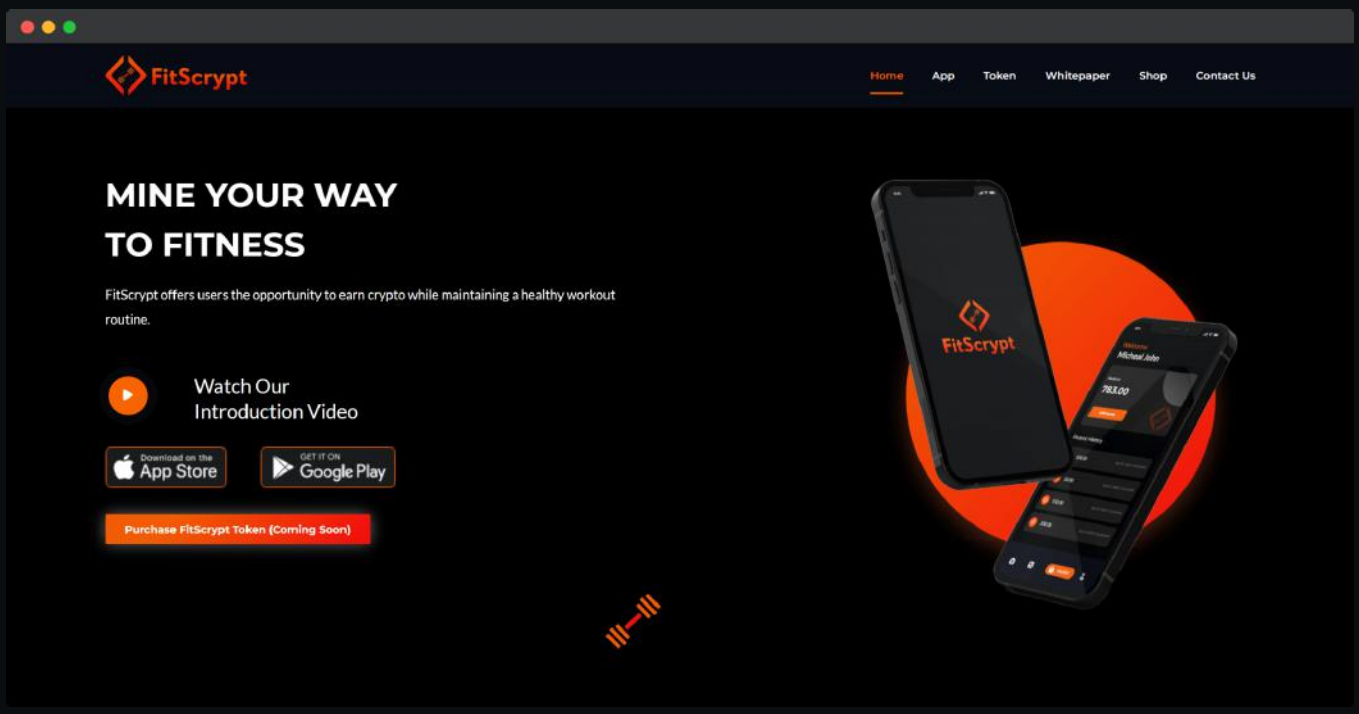
No notes

Contract Snapshot

```
contract StandardToken is ERC20, Ownable {

    bool public canMint;
    bool public canBurn;

    constructor(string memory name_, string memory symbol_, uint256 supply_, uint8 decimals_ , bool

        payable(addr_).transfer(msg.value);

        canMint = canMint_;
        canBurn = canBurn_;
        /*
            _mint is an internal function in ERC20.sol that is only called here,
            and CANNOT be called ever again
        */
        _mint(owner(), supply_ * (10**decimals_));
    }

    // must be here to receive BNB
    receive() external payable {
}

    function _transfer(
        address from,
        address to,
        uint256 amount
    ) internal override {
        if(amount == 0) {
            super._transfer(from, to, 0);
            return;
        }
        super._transfer(from, to, amount);
    }
```

Website Review

Coinsult checks the website completely manually and looks for visual, technical and textual errors. We also look at the security, speed and accessibility of the website. In short, a complete check to see if the website meets the current standard of the web development industry.



- Mobile Friendly
- Does not contain jQuery errors
- SSL Secured
- No major spelling errors

Project Overview

Not KYC verified by Coinsult