Coinsult

Advanced Manual Smart Contract Audit

Project: Contentcreators

Website: contentcreators.vip

🟢 Low-Risk	🟡 Medium-Risk	🔴 High-Risk
3 low-risk code issues found	0 medium-risk code issues found	0 high-risk code issues found

Contract Address

0xe0ad2a5ef8d37f42b308ef2fab7d44b23bed3894

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

Not available

Source Code

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

https://bscscan.com/address/0xe0ad2a5ef8d37f42b308ef2fab7d44b23bed3894#code

Manual Code Review

In this audit report we will highlight all these issues:

🟢 Low-Risk

3 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.

Avoid relying on block.timestamp

block.timestamp can be manipulated by miners.

```
function getEggsSinceLastHatch(address adr) public view returns(uint256) {
    uint256 secondsSinceLastHatch = SafeMath.sub(block.timestamp,lastHatch[adr]);
    uint256 cutoffTime = min(secondsSinceLastHatch, CUTOFF_STEP);

    uint256 secondsPassed=min(EGGS_TO_HATCH_1MINERS,cutoffTime);
    return SafeMath.mul(secondsPassed,hatcheryMiners[adr]);
}
```

Recommendation

Do not use `block.timestamp`, now or `blockhash` as a source of randomness

Exploit scenario

```
contract Game {

    uint reward_determining_number;

    function guessing() external{
      reward_determining_number = uint256(block.blockhash(10000)) % 10;
    }
}
```

Eve is a miner. Eve calls `guessing` and re-orders the block containing the transaction. As a result, Eve wins the game.

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

Too many digits

Literals with many digits are difficult to read and review.

```
uint256 private EGGS_TO_HATCH_1MINERS = 864000;//for final version should be seconds in a day
```

Recommendation

Use: Ether suffix, Time suffix, or The scientific notation

Exploit scenario

```
contract MyContract{
    uint 1_ether = 10000000000000000000;
}
```

While `1_ether` looks like `1 ether`, it is `10 ether`. As a result, it’s likely to be used incorrectly.

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

Missing events arithmetic

Detect missing events for critical arithmetic parameters.

```
function BONUS_COMPOUND_STEP(uint256 value) external onlyOwner {
    COMPOUND_STEP = value * 60 * 60;
}
```

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

Extra notes by the team

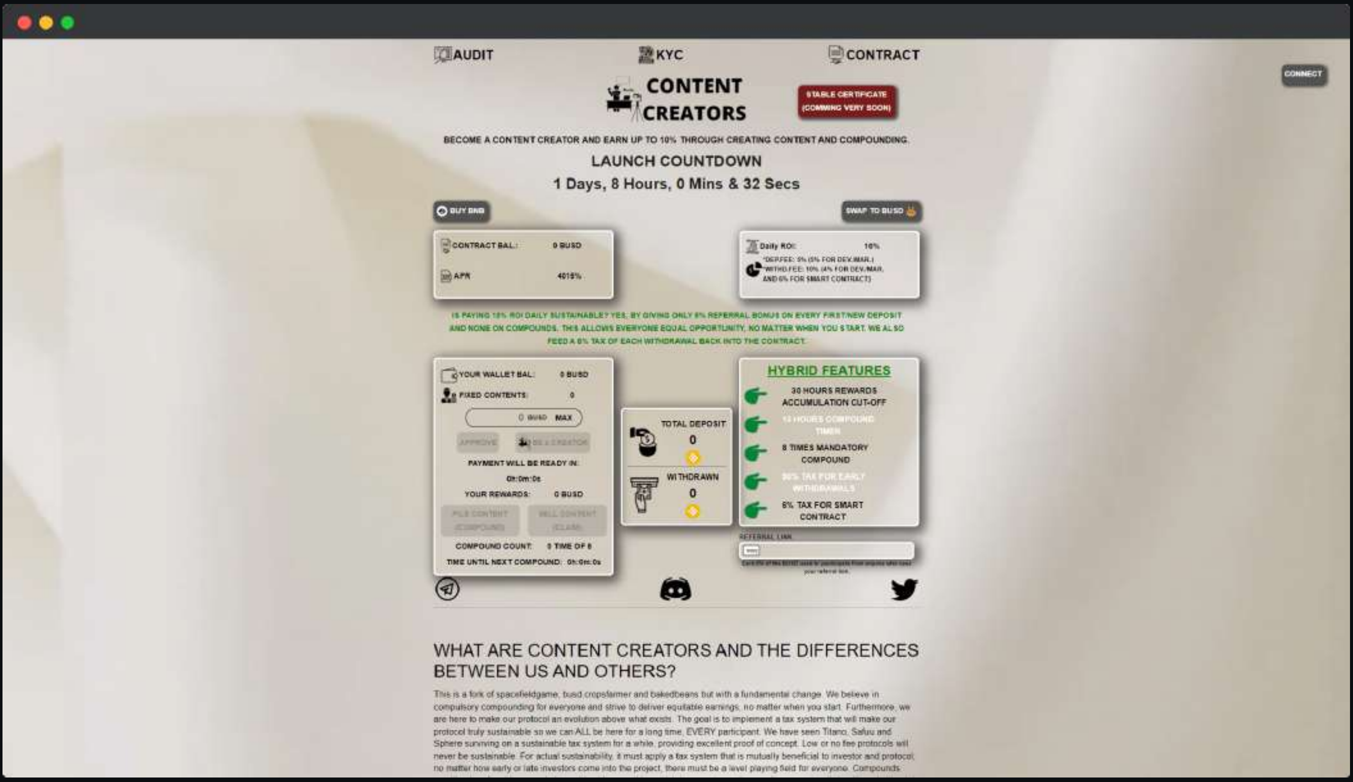
No notes

Contract Snapshot

```
contract ContentCreators is Context, Ownable {
    using SafeMath for uint256;

    address busd = 0xe9e7CEA3DedcA5984780Bafc599bD69ADd087D56;
    address private devAddress;
    uint256 private EGGS_TO_HATCH_1MINERS = 864000;//for final version should be seconds in a day
    uint256 private PSN = 10000;
    uint256 private PSNH = 5000;
    bool private initialized = false;

    uint256 public PERCENTS_DIVIDER = 1000;
uint256 public CUTOFF_STEP = 30 * 60 * 60; /** 30 hours  **/
    uint256 public COMPOUND_STEP = 13 * 60 * 60; /** every 13 hours. **/
    uint256 public COMPOUND_FOR_NO_TAX_WITHDRAWAL = 8; // compound times, for no tax withdrawal.
    uint256 public WITHDRAWAL_TAX = 900;

    mapping (address =&gt; uint256) private hatcheryMiners;
    mapping (address =&gt; uint256) private claimedEggs;
    mapping (address =&gt; uint256) private lastHatch;
    mapping (address =&gt; address) private referrals;
    mapping (address =&gt; uint256) private compoundCount;
    mapping (address =&gt; uint256) private totalDeposit;
    mapping (address =&gt; uint256) private totalWithdraw;
```

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.



BECOME A CONTENT CREATOR AND EARN UP TO 10% THROUGH CREATING CONTENT AND COMPOUNDING.

LAUNCH COUNTDOWN

1 Days, 8 Hours, 0 Mins & 32 Secs

CONTRACT BAL.:	0 BUSD
APR	4015%

Daily ROI:	10%

*DEP.FEE: 9% (5% FOR DEV.MAR.)
*WITHD.FEE: 10% (4% FOR DEV./MAR. AND 6% FOR SMART CONTRACT)

IS PAYING 10% ROI DAILY SUSTAINABLE? YES. BY GIVING ONLY 8% REFERRAL BONUS ON EVERY FIRST/NEW DEPOSIT AND NONE ON COMPOUNDS. THIS ALLOWS EVERYONE EQUAL OPPORTUNITY, NO MATTER WHEN YOU START. WE ALSO FEED A 6% TAX OF EACH WITHDRAWAL BACK INTO THE CONTRACT.

YOUR WALLET BAL.:	0 BUSD
FIXED CONTENTS:	0

PAYMENT WILL BE READY IN:
0h:0m:0s

YOUR REWARDS:	0 BUSD

PILE CONTENT (COMPOUND) — SELL CONTENT (CLAIM)

COMPOUND COUNT:	0 TIME OF 8
TIME UNTIL NEXT COMPOUND:	0h:0m:0s

TOTAL DEPOSIT
0

WITHDRAWN
0

HYBRID FEATURES

- 30 HOURS REWARDS ACCUMULATION CUT-OFF
- 12 HOURS COMPOUND TIMER
- 8 TIMES MANDATORY COMPOUND
- 50% TAX FOR EARLY WITHDRAWALS
- 6% TAX FOR SMART CONTRACT

WHAT ARE CONTENT CREATORS AND THE DIFFERENCES BETWEEN US AND OTHERS?

This is a fork of spacefieldgame, busd cropsfarmer and bakedbeans but with a fundamental change. We believe in compulsory compounding for everyone and strive to deliver equitable earnings, no matter when you start. Furthermore, we are here to make our protocol an evolution above what exists. The goal is to implement a tax system that will make our protocol truly sustainable so we can ALL be here for a long time, EVERY participant. We have seen Titano, Safuu and Sphere surviving on a sustainable tax system for a while, providing excellent proof of concept. Low or no fee protocols will never be sustainable. For actual sustainability, it must apply a tax system that is mutually beneficial to investor and protocol, no matter how early or late investors come into the project, there must be a level playing field for everyone. Compounds

● Mobile Friendly

● Does not contain jQuery errors

● SSL Secured

● No major spelling errors

Project Overview

● KYC verified by Coinsult