# Coinsult

# Advanced Manual Smart Contract Audit



**Project:** Infinity Gnomes

**Website:** https://infinitygnomes.com

🟢 **Low-Risk**

2 low-risk code issues found

🟡 **Medium-Risk**

0 medium-risk code issues found

🔴 **High-Risk**

0 high-risk code issues found

**Contract Address**

0xfD0307C6D7668cBac39A87B12D5004906A93d740

# Disclaimer

# Tokenomics

NFT Supply = 6666

# Source Code

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

https://etherscan.io/address/0xfD0307C6D7668cBac39A87B12D5004906A93d740#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

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

## Avoid relying on block.timestamp

block.timestamp can be manipulated by miners.

```
function _mint(
    address to,
    uint256 quantity,
    bytes memory _data,
    bool safe
) internal {
    uint256 startTokenId = _currentIndex;
    if (to == address(0)) revert MintToZeroAddress();
    if (quantity == 0) revert MintZeroQuantity();

    _beforeTokenTransfers(address(0), to, startTokenId, quantity);

    // Overflows are incredibly unrealistic.
    // balance or numberMinted overflow if current value of either + quantity &gt; 1.8e19 (2**64) -
    // updatedIndex overflows if _currentIndex + quantity &gt; 1.2e77 (2**256) - 1
    unchecked {
        _addressData[to].balance += uint64(quantity);
        _addressData[to].numberMinted += uint64(quantity);

        _ownerships[startTokenId].addr = to;
        _ownerships[startTokenId].startTimestamp = uint64(block.timestamp);
    }
```

## 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.

```
function _feeDenominator() internal pure virtual returns (uint96) {
    return 10000;
}
```

## 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.

# Owner privileges

⚠️ Owner can mint NFT's to address directly

⚠️ Owner can set max NFT's per wallet during presale and normal NFT trading

⚠️ Owner can change price of the NFT's

⚠️ Owner can change royalty fees

⚠️ Owner can withdraw NFT's

⚠️ Owner can change SaleState at any moment also during presale

# Extra notes by the team

No notes

# Contract Snapshot

```solidity
contract InfinityGnomes is ERC721A, Ownable, ERC2981 {
uint256 public price = 0.015 ether;
uint256 public presalePrice = 0.015 ether;
uint256 public maxPerWallet = 6;

uint256 public presaleMaxPerWallet = 6;


uint256 public immutable presaleSupply = 6666;
uint256 public immutable supply = 6666;
```

# 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.
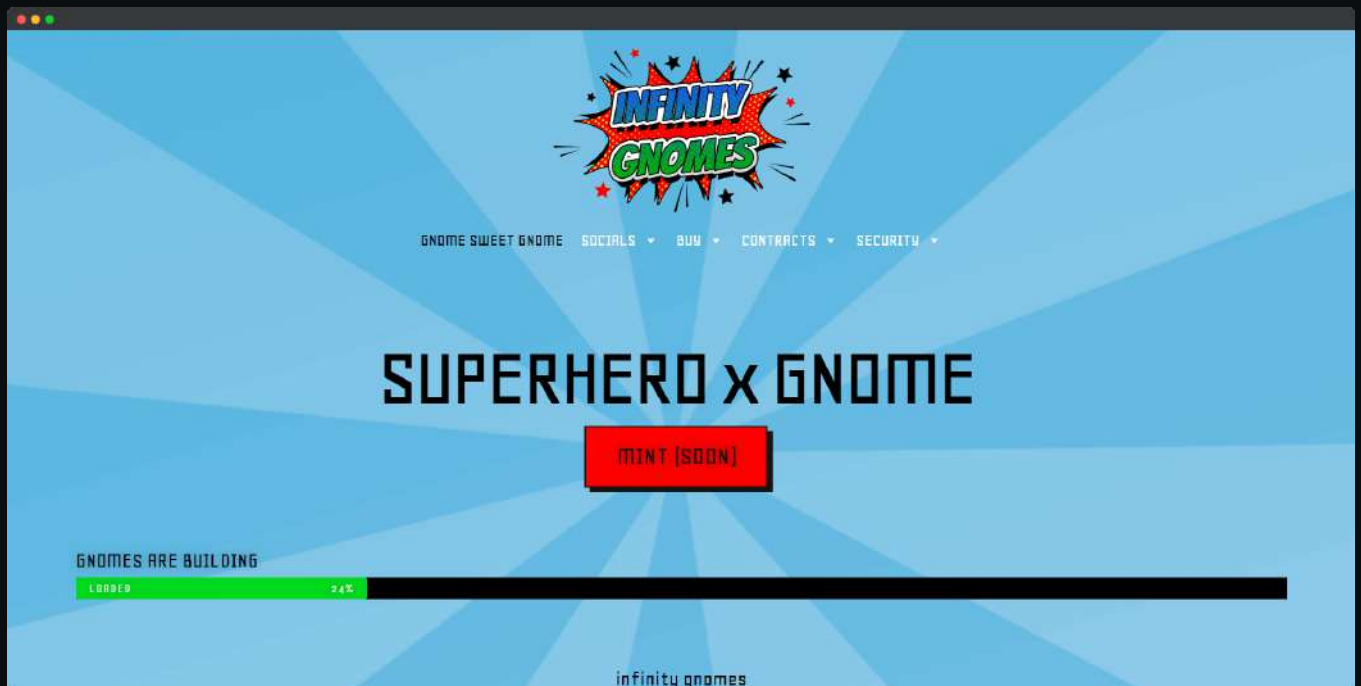


● Mobile Friendly

● Does not contain jQuery errors

● SSL Secured

● No major spelling errors

# Project Overview

● KYC verified by Coinsult

## Infinity Gnomes
### Completed KYC Verification at Coinsult.net



**Date: 5 August 2022**

✔ Project Owner Identified

✔ Contract: 0xfD0307C6D7668cBac39A87B12D5004906A93d740

## Infinity Gnomes
### Audited by Coinsult.net



**Date: 5 August 2022**

✔ Advanced Manual Smart Contract Audit