



# Coinsult

## Advanced Manual Smart Contract Audit



**Project:** Kyiv Aid Presale Contract

**Website:** <https://www.kyivaid.com/>

**Low-risk**

3 low-risk code  
issues found

**Medium-risk**

0 medium-risk code  
issues found

**High-risk**

0 high-risk code  
issues found

**Contract address**

0x1fDC45B10A71CAe24F24AEEA6b7358329e6E5382

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

# 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.

## Source code

Coinsult was commissioned by KYIV AID to perform an audit based on the following smart contract:

<https://etherscan.io/address/0x1fDC45B10A71CAe24F24AEEA6b7358329e6E5382#code>

## Manual Code Review

### ● Low-risk

3 low-risk code issues found.

Could be fixed, will not bring problems.

- Sol frequently releases new compiler versions. Using an old version prevents access to new Solidity security checks.
  - Recommended: Deploy with any of the following Solidity versions:
    - 0.5.16 - 0.5.17
    - 0.6.11 - 0.6.12
    - 0.7.5 - 0.7.6 Use a simple pragma version that allows any of these versions. Consider using the latest version of Solidity for testing.

```
pragma solidity >=0.7.0 <0.9.0;
```

- The return value of an external transfer/transferFrom call is not checked
  - Recommended : Use SafeERC20, or ensure that the transfer/transferFrom return value is checked.

```
function purchase(uint256 amount) external {
    uint256 usdcBalance = IERC20(usdc).balanceOf(msg.sender);
    require (usdcBalance >= amount, "There is not enough usdc");
    require ((IERC20(kyiv).balanceOf(msg.sender) + amount) <= 20000
* (10**6), "Max amount is 20000");
    IERC20(usdc).transferFrom( address(msg.sender), treasuryAddress
, amount);

    emit TransferSent( address(msg.sender), treasuryAddress,
amount);

    IERC20(kyiv).transfer(address(msg.sender), amount);
}
```

- The return value of an external transfer/transferFrom call is not checked
  - Recommended : Use SafeERC20, or ensure that the transfer/transferFrom return value is checked.

```
function withdraw(uint256 amount) external onlyOwner{
    IERC20(kyiv).transfer( msg.sender, amount);
}
```

### ● **Medium-risk**

0 medium-risk code issues found.

Should be fixed, could bring problems.

### ● **High-risk**

0 high-risk code issues found

Must be fixed, and will bring problems.

### **Extra notes by the team**

- This audit is about the presale contract
- The ownership is not renounced.

# Contract Snapshot

```
contract KyivPresale is Ownable {

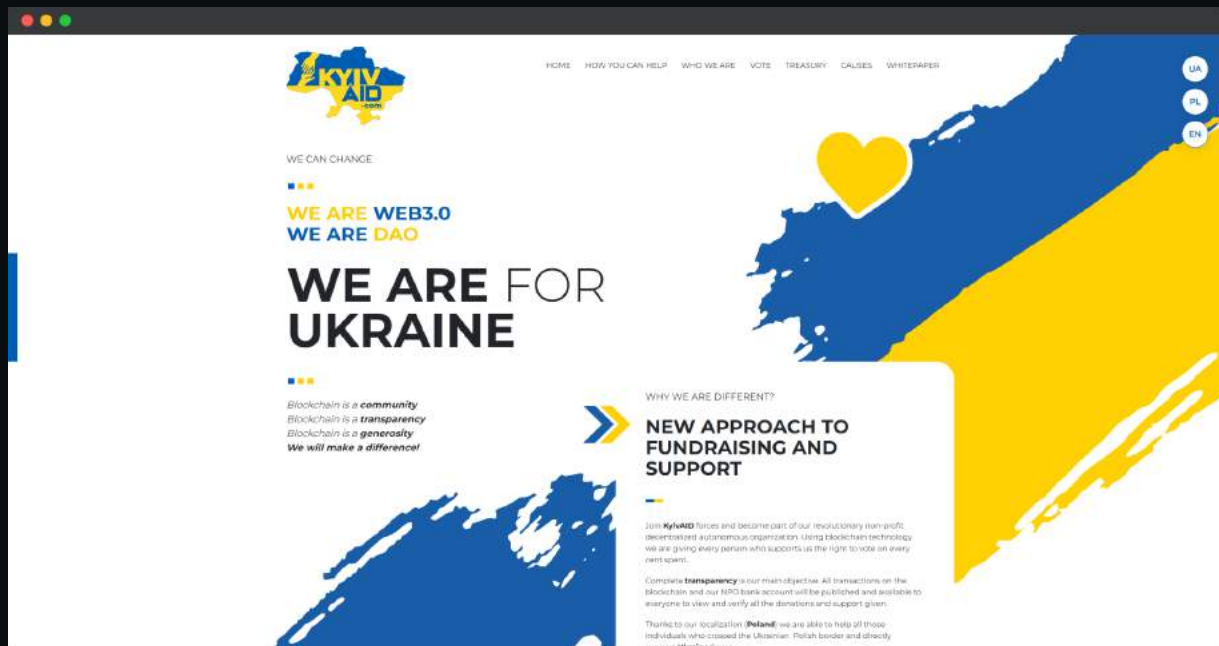
    event TransferSent(address _from, address _destAddr, uint256
_amount);

    address public treasuryAddress =
0x911853E88297fBb605c701f11E35Fef7E84224ad;
    address public usdc;
    address public kyiv;
    constructor(address _usdc, address _kyiv) {
        usdc = _usdc;
        kyiv = _kyiv;
    }
    function purchase(uint256 amount) external {
        uint256 usdcBalance = IERC20(usdc).balanceOf(msg.sender);
        require (usdcBalance >= amount, "There is not enough usdc");
        require ((IERC20(kyiv).balanceOf(msg.sender) + amount) <= 20000
* (10**6), "Max amount is 20000");
        IERC20(usdc).transferFrom( address(msg.sender), treasuryAddress
, amount);

        emit TransferSent( address(msg.sender), treasuryAddress,
amount);

        IERC20(kyiv).transfer(address(msg.sender), amount);
    }
    function remainBalance() public view returns(uint256){
        return IERC20(kyiv).balanceOf(address(this));
    }
    function withdraw(uint256 amount) external onlyOwner{
        IERC20(kyiv).transfer( msg.sender, 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
- Contains no jQuery errors
- SSL Secured
- No major spelling errors

**Note: Some icons are not loading correctly**

```
● Access to font at: "https://kylivaid.com/css/fontawesome/webfonts/fa-brands-400.woff2" from origin "https://www.kylivaid.com" has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.
● Failed to load resource: net::ERR_FAILED
● Access to font at: "https://kylivaid.com/css/fontawesome/webfonts/fa-brands-400.woff" from origin "https://www.kylivaid.com" has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.
● Failed to load resource: net::ERR_FAILED
● Access to font at: "https://kylivaid.com/css/fontawesome/webfonts/fa-brands-400.ttf" from origin "https://www.kylivaid.com" has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.
● Failed to load resource: net::ERR_FAILED
● Access to font at: "https://kylivaid.com/css/fontawesome/webfonts/fa-solid-900.woff2" from origin "https://www.kylivaid.com" has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.
● Failed to load resource: net::ERR_FAILED
● Access to font at: "https://kylivaid.com/css/fontawesome/webfonts/fa-solid-900.woff" from origin "https://www.kylivaid.com" has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.
● Failed to load resource: net::ERR_FAILED
● Access to font at: "https://kylivaid.com/css/fontawesome/webfonts/fa-solid-900.ttf" from origin "https://www.kylivaid.com" has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.
● Failed to load resource: net::ERR_FAILED
```

Loading speed: 85%

# Rug-pull Review (main token)

Based on the available information analyzed by us, we come to the following conclusions:

- Locked Liquidity (no liquidity yet)
- Large unlocked wallets
  - Note: Tokens not distributed yet
- Doxxed Team (on-website)

# Honeypot Review (main token)

Based on the available information analyzed by us, we come to the following conclusions:

- Ability to sell
- Owner is able to pause the contract
- Accurate liquidity pair

**Note:** Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by the project owner.