USDExchangeToken – Audit & Verification Report

Total Contracts Analyzed: 11

Generated on: 2025-06-16 23:50:22

Test Summary

Total Tests: 176

Passed: 176 (100.0%)

Failed: 0 (0.0%)

Test Results Chart

Test Name	Framework	Result
roleManager()	Echidna	**PASS**
name()	Echidna	**PASS**
approve(address,uint256)	Echidna	**PASS**
executeProposal(uint256)	Echidna	**PASS**
submitMultisigTransaction(address,uint256,bytes,string)	Echidna	**PASS**
setMetadataManager(address)	Echidna	**PASS**
setUSDPrice(uint256)	Echidna	**PASS**
setVestingManager(address)	Echidna	**PASS**
totalSupply()	Echidna	**PASS**
grantMultipleRoles(bytes32[],address)	Echidna	**PASS**
transferFrom(address,address,uint256)	Echidna	**PASS**
setDailyTransferLimit(address,uint256)	Echidna	**PASS**
BURNER_ROLE()	Echidna	**PASS**
confirmMultisigTransaction(uint256)	Echidna	**PASS**
isEmergencyRole(address)	Echidna	**PASS**
getMultisigTransaction(uint256)	Echidna	**PASS**
grantRole(bytes32,address)	Echidna	**PASS**
isOwner(address)	Echidna	**PASS**
decimals()	Echidna	**PASS**
increaseAllowance(address,uint256)	Echidna	**PASS**
isBlacklistManager(address)	Echidna	**PASS**
unpause()	Echidna	**PASS**

mint(address,uint256)	Echidna	**PASS**
BLACKLIST_MANAGER_ROLE()	Echidna	**PASS**
transferToVesting(address,uint256)	Echidna	**PASS**
burn(uint256)	Echidna	**PASS**
isBurner(address)	Echidna	**PASS**
isPauser(address)	Echidna	**PASS**
setFeeManager(address)	Echidna	**PASS**
createProposal(string)	Echidna	**PASS**
setSecurityBlacklistStatus(address,bool)	Echidna	**PASS**
getPendingMultisigTransactions()	Echidna	**PASS**
metadataManager()	Echidna	**PASS**
buyTokenWithStable(address,uint256)	Echidna	**PASS**
setStablecoinManager(address)	Echidna	**PASS**
isSecurityBlacklisted(address)	Echidna	**PASS**
counterManager()	Echidna	**PASS**
getWalletMetadata()	Echidna	**PASS**
paused()	Echidna	**PASS**
updateLogoURI(string)	Echidna	**PASS**
setMultisigWallet(address)	Echidna	**PASS**
getMultisigSigners()	Echidna	**PASS**
setFee(uint256)	Echidna	**PASS**
balanceOf(address)	Echidna	**PASS**
setFeeExemption(address,bool)	Echidna	**PASS**
burnFrom(address,uint256)	Echidna	**PASS**
revokeMultisigConfirmation(uint256)	Echidna	**PASS**
lockWallet(address,bool)	Echidna	**PASS**
setStableTokenWhitelist(address,bool)	Echidna	**PASS**
pause()	Echidna	**PASS**
changeAdmin(address)	Echidna	**PASS**
multisigWallet()	Echidna	**PASS**
setCounterManager(address)	Echidna	**PASS**
setSecurityManager(address)	Echidna	**PASS**
symbol()	Echidna	**PASS**
updateSocialLinks(string,string,string,string)	Echidna	**PASS**
DEFAULT_ADMIN_ROLE()	Echidna	**PASS**
lockTokens(address,uint256,uint256)	Echidna	**PASS**
decreaseAllowance(address,uint256)	Echidna	**PASS**
transfer(address,uint256)	Echidna	**PASS**
isMinter(address)	Echidna	**PASS**

setBotStatus(address,bool)	Echidna	**PASS**
getFullMetadata()	Echidna	**PASS**
executeMultisigTransaction(uint256)	Echidna	**PASS**
setTimelock(address)	Echidna	**PASS**
getProposal(uint256)	Echidna	**PASS**
stablecoinManager()	Echidna	**PASS**
vote(uint256,bool)	Echidna	**PASS**
unlockTokens(address)	Echidna	**PASS**
getVestingWallet(address)	Echidna	**PASS**
feeManager()	Echidna	**PASS**
governanceManager()	Echidna	**PASS**
timelock()	Echidna	**PASS**
MINTER_ROLE()	Echidna	**PASS**
revokeRole(bytes32,address)	Echidna	**PASS**
vestingManager()	Echidna	**PASS**
updateMetadata(string,string,string)	Echidna	**PASS**
allowance(address,address)	Echidna	**PASS**
securityManager()	Echidna	**PASS**
setGovernanceManager(address)	Echidna	**PASS**
PAUSER_ROLE()	Echidna	**PASS**
setFeeRecipient(address)	Echidna	**PASS**
setTransferLimit(address,uint256)	Echidna	**PASS**
setRoleManager(address)	Echidna	**PASS**
mintForStablecoin(address,uint256)	Echidna	**PASS**
revokeMultipleRoles(bytes32[],address)	Echidna	**PASS**
createVestingWallet(address,uint256)	Echidna	**PASS**
AssertionFailed(..)	Echidna	**PASS**
roleManager()	Scribble	**PASS**
name()	Scribble	**PASS**
approve(address,uint256)	Scribble	**PASS**
executeProposal(uint256)	Scribble	**PASS**
submitMultisigTransaction(address,uint256,bytes,string)	Scribble	**PASS**
setMetadataManager(address)	Scribble	**PASS**
setUSDPrice(uint256)	Scribble	**PASS**
setVestingManager(address)	Scribble	**PASS**
totalSupply()	Scribble	**PASS**
grantMultipleRoles(bytes32[],address)	Scribble	**PASS**
transferFrom(address,address,uint256)	Scribble	**PASS**
setDailyTransferLimit(address,uint256)	Scribble	**PASS**

BURNER_ROLE()	Scribble	**PASS**
confirmMultisigTransaction(uint256)	Scribble	**PASS**
isEmergencyRole(address)	Scribble	**PASS**
getMultisigTransaction(uint256)	Scribble	**PASS**
grantRole(bytes32,address)	Scribble	**PASS**
isOwner(address)	Scribble	**PASS**
decimals()	Scribble	**PASS**
increaseAllowance(address,uint256)	Scribble	**PASS**
isBlacklistManager(address)	Scribble	**PASS**
unpause()	Scribble	**PASS**
mint(address,uint256)	Scribble	**PASS**
BLACKLIST_MANAGER_ROLE()	Scribble	**PASS**
transferToVesting(address,uint256)	Scribble	**PASS**
burn(uint256)	Scribble	**PASS**
isBurner(address)	Scribble	**PASS**
isPauser(address)	Scribble	**PASS**
setFeeManager(address)	Scribble	**PASS**
createProposal(string)	Scribble	**PASS**
setSecurityBlacklistStatus(address,bool)	Scribble	**PASS**
getPendingMultisigTransactions()	Scribble	**PASS**
metadataManager()	Scribble	**PASS**
buyTokenWithStable(address,uint256)	Scribble	**PASS**
setStablecoinManager(address)	Scribble	**PASS**
isSecurityBlacklisted(address)	Scribble	**PASS**
counterManager()	Scribble	**PASS**
getWalletMetadata()	Scribble	**PASS**
paused()	Scribble	**PASS**
updateLogoURI(string)	Scribble	**PASS**
setMultisigWallet(address)	Scribble	**PASS**
getMultisigSigners()	Scribble	**PASS**
setFee(uint256)	Scribble	**PASS**
balanceOf(address)	Scribble	**PASS**
setFeeExemption(address,bool)	Scribble	**PASS**
burnFrom(address,uint256)	Scribble	**PASS**
revokeMultisigConfirmation(uint256)	Scribble	**PASS**
lockWallet(address,bool)	Scribble	**PASS**
setStableTokenWhitelist(address,bool)	Scribble	**PASS**
pause()	Scribble	**PASS**
changeAdmin(address)	Scribble	**PASS**

multisigWallet()	Scribble	**PASS**
setCounterManager(address)	Scribble	**PASS**
setSecurityManager(address)	Scribble	**PASS**
symbol()	Scribble	**PASS**
updateSocialLinks(string,string,string,string)	Scribble	**PASS**
DEFAULT_ADMIN_ROLE()	Scribble	**PASS**
lockTokens(address,uint256,uint256)	Scribble	**PASS**
decreaseAllowance(address,uint256)	Scribble	**PASS**
transfer(address,uint256)	Scribble	**PASS**
isMinter(address)	Scribble	**PASS**
setBotStatus(address,bool)	Scribble	**PASS**
getFullMetadata()	Scribble	**PASS**
executeMultisigTransaction(uint256)	Scribble	**PASS**
setTimelock(address)	Scribble	**PASS**
getProposal(uint256)	Scribble	**PASS**
stablecoinManager()	Scribble	**PASS**
vote(uint256,bool)	Scribble	**PASS**
unlockTokens(address)	Scribble	**PASS**
getVestingWallet(address)	Scribble	**PASS**
feeManager()	Scribble	**PASS**
governanceManager()	Scribble	**PASS**
timelock()	Scribble	**PASS**
MINTER_ROLE()	Scribble	**PASS**
revokeRole(bytes32,address)	Scribble	**PASS**
vestingManager()	Scribble	**PASS**
updateMetadata(string,string,string)	Scribble	**PASS**
allowance(address,address)	Scribble	**PASS**
securityManager()	Scribble	**PASS**
setGovernanceManager(address)	Scribble	**PASS**
PAUSER_ROLE()	Scribble	**PASS**
setFeeRecipient(address)	Scribble	**PASS**
setTransferLimit(address,uint256)	Scribble	**PASS**
setRoleManager(address)	Scribble	**PASS**
mintForStablecoin(address,uint256)	Scribble	**PASS**
revokeMultipleRoles(bytes32[],address)	Scribble	**PASS**
createVestingWallet(address,uint256)	Scribble	**PASS**
AssertionFailed(..)	Scribble	**PASS**

Contract: USDExchangeToken.sol

Slither

```
'forge config --json' running
Could not detect solc version from Foundry config. Falling back to system version...
'solc --version' running
'solc @openzeppelin 2/=node_modules/@openzeppelin 2/ @openzeppelin/=node_modules/@openzeppelin/ eth-gas-repor
INFO:Detectors:
Reentrancy in USDeXchangeToken.transfer(address,uint256) (contracts/USDExchangeToken.sol#180-189):
 External calls:
 - (fee,net) = feeManager.collectFee(msg.sender,to,amount) (contracts/USDExchangeToken.sol#182)
 - super.transfer(feeManager.feeRecipient(),fee) (contracts/USDExchangeToken.sol#184)
  - securityManager.updateTransferStats(from,amount) (contracts/USDExchangeToken.sol#175)
 - super.transfer(to,net) (contracts/USDExchangeToken.sol#185)
  - securityManager.updateTransferStats(from,amount) (contracts/USDExchangeToken.sol#175)
 State variables written after the call(s):
 - super.transfer(to,net) (contracts/USDExchangeToken.sol#185)
  - _balances[from] = fromBalance - amount (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#231)
  - _balances[to] += amount (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#234)
 ERC20._balances (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#39) can be used in cross functio
 - ERC20._burn(address,uint256) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#277-293)
 - ERC20._mint(address,uint256) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#251-264)
 - ERC20._transfer(address,address,uint256) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#222-2
 - ERC20.balanceOf(address) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#101-103)
Reentrancy in USDeXchangeToken.transferFrom(address,address,uint256) (contracts/USDExchangeToken.sol#190-199)
 External calls:
 - (fee,net) = feeManager.collectFee(from,to,amount) (contracts/USDExchangeToken.sol#192)
 - super.transferFrom(from,feeManager.feeRecipient(),fee) (contracts/USDExchangeToken.sol#194)
  - securityManager.updateTransferStats(from,amount) (contracts/USDExchangeToken.sol#175)
 - super.transferFrom(from,to,net) (contracts/USDExchangeToken.sol#195)
  - securityManager.updateTransferStats(from,amount) (contracts/USDExchangeToken.sol#175)
 State variables written after the call(s):
 - super.transferFrom(from,to,net) (contracts/USDExchangeToken.sol#195)
  - _allowances[owner][spender] = amount (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#312)
 ERC20._allowances (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#41) can be used in cross funct
 - ERC20._approve(address,address,uint256) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#308-31
 - ERC20.allowance(address,address) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#122-124)
 - super.transferFrom(from,to,net) (contracts/USDExchangeToken.sol#195)
  - _balances[from] = fromBalance - amount (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#231)
  - _balances[to] += amount (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#234)
 ERC20._balances (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#39) can be used in cross functio
 - ERC20._burn(address,uint256) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#277-293)
 - ERC20._mint(address,uint256) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#251-264)
 - ERC20._transfer(address,address,uint256) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#222-2
 - ERC20.balanceOf(address) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#101-103)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-1
INFO:Detectors:
USDeXchangeToken._beforeTokenTransfer(address,address,uint256) (contracts/USDExchangeToken.sol#165-171) ignor
USDeXchangeToken.getVestingWallet(address) (contracts/USDExchangeToken.sol#223-226) ignores return value by v
USDeXchangeToken.getFullMetadata() (contracts/USDExchangeToken.sol#304-307) ignores return value by metadataM
USDeXchangeToken.getProposal(uint256) (contracts/USDExchangeToken.sol#330-333) ignores return value by govern
USDeXchangeToken.getMultisigTransaction(uint256) (contracts/USDExchangeToken.sol#419-422) ignores return valu
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-return
INFO:Detectors:
Reentrancy in USDeXchangeToken.burn(uint256) (contracts/USDExchangeToken.sol#152-155):
 External calls:
 - _burn(msg.sender,amount) (contracts/USDExchangeToken.sol#153)
  - securityManager.updateTransferStats(from,amount) (contracts/USDExchangeToken.sol#175)
 Event emitted after the call(s):
 - TokensBurned(msg.sender,amount) (contracts/USDExchangeToken.sol#154)
Reentrancy in USDeXchangeToken.burnFrom(address,uint256) (contracts/USDExchangeToken.sol#156-162):
 External calls:
 - _burn(account,amount) (contracts/USDExchangeToken.sol#160)
  - securityManager.updateTransferStats(from,amount) (contracts/USDExchangeToken.sol#175)
 Event emitted after the call(s):
 - TokensBurned(account,amount) (contracts/USDExchangeToken.sol#161)
Reentrancy in USDeXchangeToken.changeAdmin(address) (contracts/USDExchangeToken.sol#360-366):
 External calls:
 - roleManager.grantRole(DEFAULT_ADMIN_ROLE,newAdmin) (contracts/USDExchangeToken.sol#364)
 Event emitted after the call(s):
 - AdminChanged(oldAdmin,newAdmin,msg.sender,block.timestamp) (contracts/USDExchangeToken.sol#365)
Reentrancy in USDeXchangeToken.grantMultipleRoles(bytes32[],address) (contracts/USDExchangeToken.sol#346-352)
 External calls:
 - roleManager.grantMultipleRoles(roles,account) (contracts/USDExchangeToken.sol#348)
 Event emitted after the call(s):
 - RoleGranted(roles[i],account,msg.sender,block.timestamp) (contracts/USDExchangeToken.sol#350)
Reentrancy in USDeXchangeToken.grantRole(bytes32,address) (contracts/USDExchangeToken.sol#336-340):
 External calls:
 - roleManager.grantRole(role,account) (contracts/USDExchangeToken.sol#338)
 Event emitted after the call(s):
 - RoleGranted(role,account,msg.sender,block.timestamp) (contracts/USDExchangeToken.sol#339)
Reentrancy in USDeXchangeToken.revokeMultipleRoles(bytes32[],address) (contracts/USDExchangeToken.sol#353-359
 External calls:
 - roleManager.revokeMultipleRoles(roles,account) (contracts/USDExchangeToken.sol#355)
 Event emitted after the call(s):
 - RoleRevoked(roles[i],account,msg.sender,block.timestamp) (contracts/USDExchangeToken.sol#357)
Reentrancy in USDeXchangeToken.revokeRole(bytes32,address) (contracts/USDExchangeToken.sol#341-345):
 External calls:
 - roleManager.revokeRole(role,account) (contracts/USDExchangeToken.sol#343)
 Event emitted after the call(s):
 - RoleRevoked(role,account,msg.sender,block.timestamp) (contracts/USDExchangeToken.sol#344)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
```

```
INFO:Detectors:
2 different versions of Solidity are used:
 - Version constraint ^0.8.28 is used by:
  -^0.8.28 (contracts/USDExchangeToken.sol#2)
  -^0.8.28 (contracts/interfaces/ICounter.sol#2)
  -^0.8.28 (contracts/interfaces/IFeeManager.sol#2)
  -^0.8.28 (contracts/interfaces/IGovernanceManager.sol#2)
  -^0.8.28 (contracts/interfaces/IMetadataManager.sol#2)
  -^0.8.28 (contracts/interfaces/IMultisigWallet.sol#2)
  -^0.8.28 (contracts/interfaces/IRoleManager.sol#2)
  -^0.8.28 (contracts/interfaces/ISecurityManager.sol#2)
  -^0.8.28 (contracts/interfaces/IStablecoinManager.sol#2)
  -^0.8.28 (contracts/interfaces/IVestingManager.sol#2)
 - Version constraint ^0.8.0 is used by:
  -^0.8.0 (node_modules/@openzeppelin/contracts/security/ReentrancyGuard.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/IERC20.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
INFO:Detectors:
Context._contextSuffixLength() (node_modules/@openzeppelin/contracts/utils/Context.sol#25-27) is never used a
Context._msgData() (node_modules/@openzeppelin/contracts/utils/Context.sol#21-23) is never used and should be
ReentrancyGuard._reentrancyGuardEntered() (node_modules/@openzeppelin/contracts/security/ReentrancyGuard.sol#
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Version constraint ^0.8.0 contains known severe issues (https://solidity.readthedocs.io/en/latest/bugs.html)
 - FullInlinerNonExpressionSplitArgumentEvaluationOrder
 - MissingSideEffectsOnSelectorAccess
 - AbiReencodingHeadOverflowWithStaticArrayCleanup
 - DirtyBytesArrayToStorage
 - DataLocationChangeInInternalOverride
 - NestedCalldataArrayAbiReencodingSizeValidation
 - SignedImmutables
 - ABIDecodeTwoDimensionalArrayMemory
 - KeccakCaching.
It is used by:
 - ^0.8.0 (node_modules/@openzeppelin/contracts/security/ReentrancyGuard.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/IERC20.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
USDeXchangeToken (contracts/USDExchangeToken.sol#16-439) should inherit from IMetadataManager (contracts/inte
USDeXchangeToken (contracts/USDExchangeToken.sol#16-439) should inherit from IVestingManager (contracts/inter
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-inheritance
INFO:Detectors:
Parameter USDeXchangeToken.setTimelock(address)._timelock (contracts/USDExchangeToken.sol#78) is not in mixed
Parameter USDeXchangeToken.setCounterManager(address)._counterManager (contracts/USDExchangeToken.sol#86) is
Parameter USDeXchangeToken.setStablecoinManager(address)._stablecoinManager (contracts/USDExchangeToken.sol#9
Parameter USDeXchangeToken.setVestingManager(address)._vestingManager (contracts/USDExchangeToken.sol#97) is
Parameter USDeXchangeToken.setSecurityManager(address)._securityManager (contracts/USDExchangeToken.sol#102)
Parameter USDeXchangeToken.setFeeManager(address)._feeManager (contracts/USDExchangeToken.sol#107) is not in
Parameter USDeXchangeToken.setMetadataManager(address)._metadataManager (contracts/USDExchangeToken.sol#112)
Parameter USDeXchangeToken.setGovernanceManager(address)._governanceManager (contracts/USDExchangeToken.sol#1
Parameter USDeXchangeToken.setRoleManager(address)._roleManager (contracts/USDExchangeToken.sol#122) is not i
Parameter USDeXchangeToken.setMultisigWallet(address)._multisigWallet (contracts/USDExchangeToken.sol#127) is
Parameter USDeXchangeToken.setFee(uint256)._feePercent (contracts/USDExchangeToken.sol#273) is not in mixedCa
Parameter USDeXchangeToken.setFeeRecipient(address)._feeRecipient (contracts/USDExchangeToken.sol#278) is not
Parameter USDeXchangeToken.updateSocialLinks(string,string,string,string)._telegram (contracts/USDExchangeTok
Parameter USDeXchangeToken.updateSocialLinks(string,string,string,string)._twitter (contracts/USDExchangeToke
Parameter USDeXchangeToken.updateSocialLinks(string,string,string,string)._discord (contracts/USDExchangeToke
Parameter USDeXchangeToken.updateSocialLinks(string,string,string,string)._github (contracts/USDExchangeToken
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conve
INFO:Slither:contracts/USDExchangeToken.sol analyzed (15 contracts with 100 detectors), 37 result(s) found
```

Mythril

```
/Users/irfangedik/Desktop/sozlesme_deneme/USDTg_UltraSecureToken/.venv/lib/python3.9/site-packages/urllib3/__
  warnings.warn(
mythril.interfaces.cli [ERROR]: Input file not found [Errno 2] No such file or directory: '@openzeppelin/cont
```

Surya Analysis Summary

```
Total functions: 49
Public: 10, External: 39
Protected by 'onlyMultisigOrTimelock': 15
Protected by 'onlyRole': 21
Unprotected (no critical modifier) public/external functions: 4

Unprotected functions:
- [32m[Pub][39m [90m[39m[31m #[39m
- [34m[Ext][39m mintForStablecoin[31m #[39m
- [32m[Pub][39m transfer[31m #[39m
- [32m[Pub][39m transferFrom[31m #[39m
```

Surya Function Map

```
 +  USDeXchangeToken [90m(ERC20, ReentrancyGuard)[39m
    - [32m[Pub][39m [90m[39m[31m #[39m
       - modifiers: ERC20
    - [34m[Ext][39m setTimelock[31m #[39m
       - modifiers: onlyMultisigOrTimelock
    - [34m[Ext][39m setCounterManager[31m #[39m
       - modifiers: onlyMultisigOrTimelock
    - [34m[Ext][39m setStablecoinManager[31m #[39m
       - modifiers: onlyMultisigOrTimelock
    - [34m[Ext][39m setVestingManager[31m #[39m
       - modifiers: onlyMultisigOrTimelock
    - [34m[Ext][39m setSecurityManager[31m #[39m
       - modifiers: onlyMultisigOrTimelock
    - [34m[Ext][39m setFeeManager[31m #[39m
       - modifiers: onlyMultisigOrTimelock
    - [34m[Ext][39m setMetadataManager[31m #[39m
       - modifiers: onlyMultisigOrTimelock
    - [34m[Ext][39m setGovernanceManager[31m #[39m
       - modifiers: onlyMultisigOrTimelock
    - [34m[Ext][39m setRoleManager[31m #[39m
       - modifiers: onlyMultisigOrTimelock
    - [34m[Ext][39m setMultisigWallet[31m #[39m
       - modifiers: onlyMultisigOrTimelock
    - [32m[Pub][39m pause[31m #[39m
       - modifiers: onlyRole
    - [32m[Pub][39m unpause[31m #[39m
       - modifiers: onlyRole
    - [32m[Pub][39m mint[31m #[39m
       - modifiers: onlyRole,whenNotPaused
    - [34m[Ext][39m mintForStablecoin[31m #[39m
       - modifiers: whenNotPaused
    - [32m[Pub][39m burn[31m #[39m
       - modifiers: onlyRole,whenNotPaused
    - [32m[Pub][39m burnFrom[31m #[39m
       - modifiers: onlyRole,whenNotPaused
    - [90m[Int][39m _beforeTokenTransfer[31m #[39m
    - [90m[Int][39m _afterTokenTransfer[31m #[39m
    - [32m[Pub][39m transfer[31m #[39m
       - modifiers: whenNotPaused,nonReentrant
    - [32m[Pub][39m transferFrom[31m #[39m
       - modifiers: whenNotPaused,nonReentrant
    - [34m[Ext][39m buyTokenWithStable[31m #[39m
    - [34m[Ext][39m setStableTokenWhitelist[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setUSDPrice[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m createVestingWallet[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m getVestingWallet
    - [34m[Ext][39m transferToVesting[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setSecurityBlacklistStatus[31m #[39m
    - [34m[Ext][39m setBotStatus[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setTransferLimit[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setDailyTransferLimit[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m lockTokens[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m unlockTokens[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m lockWallet[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setFee[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setFeeRecipient[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setFeeExemption[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m updateMetadata[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m updateSocialLinks[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m updateLogoURI[31m #[39m
```

```
        - modifiers: onlyRole
     - [34m[Ext][39m getFullMetadata
     - [34m[Ext][39m getWalletMetadata
     - [34m[Ext][39m createProposal[31m #[39m
     - [34m[Ext][39m vote[31m #[39m
     - [34m[Ext][39m executeProposal[31m #[39m
     - [34m[Ext][39m getProposal
     - [32m[Pub][39m grantRole[31m #[39m
        - modifiers: onlyMultisigOrTimelock
     - [32m[Pub][39m revokeRole[31m #[39m
        - modifiers: onlyMultisigOrTimelock
     - [34m[Ext][39m grantMultipleRoles[31m #[39m
        - modifiers: onlyMultisigOrTimelock
     - [34m[Ext][39m revokeMultipleRoles[31m #[39m
        - modifiers: onlyMultisigOrTimelock
     - [34m[Ext][39m changeAdmin[31m #[39m
        - modifiers: onlyMultisigOrTimelock
     - [34m[Ext][39m isOwner
     - [34m[Ext][39m isMinter
     - [34m[Ext][39m isBurner
     - [34m[Ext][39m isPauser
     - [34m[Ext][39m isBlacklistManager
     - [34m[Ext][39m isEmergencyRole
     - [34m[Ext][39m submitMultisigTransaction[31m #[39m
     - [34m[Ext][39m confirmMultisigTransaction[31m #[39m
     - [34m[Ext][39m revokeMultisigConfirmation[31m #[39m
     - [34m[Ext][39m executeMultisigTransaction[31m #[39m
     - [34m[Ext][39m getMultisigTransaction
     - [34m[Ext][39m getMultisigSigners
     - [34m[Ext][39m getPendingMultisigTransactions
     - [34m[Ext][39m isSecurityBlacklisted


 [33m ($)[39m = payable function
 [31m #[39m = non-constant function
```

Contract: SecurityManager.sol

Slither

```
'forge config --json' running
Could not detect solc version from Foundry config. Falling back to system version...
'solc --version' running
'solc @openzeppelin 2/=node_modules/@openzeppelin 2/ @openzeppelin/=node_modules/@openzeppelin/ eth-gas-repor
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) has bi
  - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-exponentiation
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#120)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#121)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#122)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#123)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#124)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#125)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - prod0 = prod0 / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#104)
 - result = prod0 * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#131)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
RoleManager.constructor(address)._tokenContract (contracts/access/RoleManager.sol#28) lacks a zero-check on :
  - tokenContract = _tokenContract (contracts/access/RoleManager.sol#29)
SecurityManager.constructor(address,address)._tokenContract (contracts/security/SecurityManager.sol#42) lacks
  - tokenContract = _tokenContract (contracts/security/SecurityManager.sol#43)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
SecurityManager.lockTokens(address,uint256,uint256) (contracts/security/SecurityManager.sol#79-83) uses times
 Dangerous comparisons:
 - require(bool,string)(unlockTimestamp > block.timestamp,Future unlock only) (contracts/security/SecurityMan
SecurityManager.unlockTokens(address) (contracts/security/SecurityManager.sol#85-89) uses timestamp for compa
 Dangerous comparisons:
 - require(bool,string)(block.timestamp >= lockedBalances[account].unlockTimestamp,Too early) (contracts/secu
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Strings.toString(uint256) (node_modules/@openzeppelin/contracts/utils/Strings.sol#19-39) uses assembly
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#25-27)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#31-33)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) uses a
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#62-66)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#85-92)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#99-108)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
2 different versions of Solidity are used:
 - Version constraint ^0.8.28 is used by:
  -^0.8.28 (contracts/access/RoleManager.sol#2)
  -^0.8.28 (contracts/security/SecurityManager.sol#2)
 - Version constraint ^0.8.0 is used by:
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/IERC20.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
INFO:Detectors:
AccessControl._setRoleAdmin(bytes32,bytes32) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#2
AccessControl._setupRole(bytes32,address) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#206-
Context._contextSuffixLength() (node_modules/@openzeppelin/contracts/utils/Context.sol#25-27) is never used a
Context._msgData() (node_modules/@openzeppelin/contracts/utils/Context.sol#21-23) is never used and should be
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Version constraint ^0.8.0 contains known severe issues (https://solidity.readthedocs.io/en/latest/bugs.html)
 - FullInlinerNonExpressionSplitArgumentEvaluationOrder
 - MissingSideEffectsOnSelectorAccess
 - AbiReencodingHeadOverflowWithStaticArrayCleanup
 - DirtyBytesArrayToStorage
 - DataLocationChangeInInternalOverride
 - NestedCalldataArrayAbiReencodingSizeValidation
 - SignedImmutables
 - ABIDecodeTwoDimensionalArrayMemory
 - KeccakCaching.
It is used by:
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/IERC20.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
RoleManager.tokenContract (contracts/access/RoleManager.sol#7) should be immutable
SecurityManager.roleManager (contracts/security/SecurityManager.sol#40) should be immutable
SecurityManager.tokenContract (contracts/security/SecurityManager.sol#11) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declar
INFO:Slither:contracts/security/SecurityManager.sol analyzed (11 contracts with 100 detectors), 24 result(s)
```

Mythril

```
/Users/irfangedik/Desktop/sozlesme_deneme/USDTg_UltraSecureToken/.venv/lib/python3.9/site-packages/urllib3/__
  warnings.warn(
mythril.interfaces.cli [ERROR]: Input file not found [Errno 2] No such file or directory: '@openzeppelin/cont
```

Surya Analysis Summary

```
Total functions: 11
Public: 1, External: 10
Protected by 'onlyMultisigOrTimelock': 0
Protected by 'onlyRole': 8
Unprotected (no critical modifier) public/external functions: 1

Unprotected functions:
- [34m[Ext][39m updateTransferStats[31m #[39m
```

Surya Function Map

```
 +  SecurityManager [90m(AccessControl)[39m
    - [32m[Pub][39m [90m[39m[31m #[39m
    - [34m[Ext][39m setSecurityBlacklistStatus[31m #[39m
    - [34m[Ext][39m setBotStatus[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setTransferLimit[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setDailyTransferLimit[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setExemptFromLimits[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m lockTokens[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m unlockTokens[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m lockWallet[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m checkTransferRestrictions
       - modifiers: onlyTokenContract
    - [34m[Ext][39m updateTransferStats[31m #[39m
       - modifiers: onlyTokenContract
    - [34m[Ext][39m resetDailyUsage[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m getTransferStats
    - [34m[Ext][39m getSecurityInfo
    - [34m[Ext][39m isSecurityBlacklisted


[33m ($)[39m = payable function
[31m #[39m = non-constant function
```

Contract: FeeManager.sol

Slither

```
'forge config --json' running
Could not detect solc version from Foundry config. Falling back to system version...
'solc --version' running
'solc @openzeppelin 2/=node_modules/@openzeppelin 2/ @openzeppelin/=node_modules/@openzeppelin/ eth-gas-repor
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) has bi
  - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-exponentiation
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#120)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#121)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#122)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#123)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#124)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#125)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - prod0 = prod0 / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#104)
 - result = prod0 * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#131)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
FeeManager.constructor(address)._tokenContract (contracts/fees/FeeManager.sol#21) lacks a zero-check on :
  - tokenContract = _tokenContract (contracts/fees/FeeManager.sol#22)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
Strings.toString(uint256) (node_modules/@openzeppelin/contracts/utils/Strings.sol#19-39) uses assembly
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#25-27)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#31-33)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) uses a
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#62-66)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#85-92)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#99-108)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
```

```
INFO:Detectors:
2 different versions of Solidity are used:
 - Version constraint ^0.8.28 is used by:
  -^0.8.28 (contracts/fees/FeeManager.sol#2)
 - Version constraint ^0.8.0 is used by:
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/IERC20.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
INFO:Detectors:
AccessControl._setRoleAdmin(bytes32,bytes32) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#2
AccessControl._setupRole(bytes32,address) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#206-
Context._contextSuffixLength() (node_modules/@openzeppelin/contracts/utils/Context.sol#25-27) is never used a
Context._msgData() (node_modules/@openzeppelin/contracts/utils/Context.sol#21-23) is never used and should be
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Version constraint ^0.8.0 contains known severe issues (https://solidity.readthedocs.io/en/latest/bugs.html)
 - FullInlinerNonExpressionSplitArgumentEvaluationOrder
 - MissingSideEffectsOnSelectorAccess
 - AbiReencodingHeadOverflowWithStaticArrayCleanup
 - DirtyBytesArrayToStorage
 - DataLocationChangeInInternalOverride
 - NestedCalldataArrayAbiReencodingSizeValidation
 - SignedImmutables
 - ABIDecodeTwoDimensionalArrayMemory
 - KeccakCaching.
It is used by:
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/IERC20.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Parameter FeeManager.setFee(uint256)._feePercent (contracts/fees/FeeManager.sol#34) is not in mixedCase
Parameter FeeManager.setFeeRecipient(address)._feeRecipient (contracts/fees/FeeManager.sol#40) is not in mixe
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conve
INFO:Detectors:
FeeManager.tokenContract (contracts/fees/FeeManager.sol#10) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declar
INFO:Slither:contracts/fees/FeeManager.sol analyzed (10 contracts with 100 detectors), 21 result(s) found
```

Mythril

```
/Users/irfangedik/Desktop/sozlesme_deneme/USDTg_UltraSecureToken/.venv/lib/python3.9/site-packages/urllib3/__
  warnings.warn(
mythril.interfaces.cli [ERROR]: Input file not found [Errno 2] No such file or directory: '@openzeppelin/cont
```

Surya Analysis Summary

```
Total functions: 5
Public: 1, External: 4
Protected by 'onlyMultisigOrTimelock': 0
Protected by 'onlyRole': 3
Unprotected (no critical modifier) public/external functions: 1

Unprotected functions:
- [34m[Ext][39m collectFee[31m #[39m
```

Surya Function Map

```
 +  FeeManager [90m(AccessControl)[39m
    - [32m[Pub][39m [90m[39m[31m #[39m
    - [34m[Ext][39m setFee[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setFeeRecipient[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setFeeExemption[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m calculateFee
    - [34m[Ext][39m collectFee[31m #[39m
       - modifiers: onlyTokenContract
    - [34m[Ext][39m getFeeInfo
    - [34m[Ext][39m isExempt


[33m ($)[39m = payable function
[31m #[39m = non-constant function
```

Contract: MetadataManager.sol

Slither

```
'forge config --json' running
Could not detect solc version from Foundry config. Falling back to system version...
'solc --version' running
'solc @openzeppelin 2/=node_modules/@openzeppelin 2/ @openzeppelin/=node_modules/@openzeppelin/ eth-gas-repor
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) has bi
  - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-exponentiation
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#120)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#121)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#122)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#123)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#124)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#125)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - prod0 = prod0 / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#104)
 - result = prod0 * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#131)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
MetadataManager.constructor(address)._tokenContract (contracts/metadata/MetadataManager.sol#24) lacks a zero-
  - tokenContract = _tokenContract (contracts/metadata/MetadataManager.sol#25)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
Strings.toString(uint256) (node_modules/@openzeppelin/contracts/utils/Strings.sol#19-39) uses assembly
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#25-27)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#31-33)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) uses a
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#62-66)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#85-92)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#99-108)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
2 different versions of Solidity are used:
 - Version constraint ^0.8.28 is used by:
  -^0.8.28 (contracts/metadata/MetadataManager.sol#2)
 - Version constraint ^0.8.0 is used by:
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
```

```
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
INFO:Detectors:
AccessControl._setRoleAdmin(bytes32,bytes32) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#2
AccessControl._setupRole(bytes32,address) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#206-
Context._contextSuffixLength() (node_modules/@openzeppelin/contracts/utils/Context.sol#25-27) is never used a
Context._msgData() (node_modules/@openzeppelin/contracts/utils/Context.sol#21-23) is never used and should be
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Version constraint ^0.8.0 contains known severe issues (https://solidity.readthedocs.io/en/latest/bugs.html)
 - FullInlinerNonExpressionSplitArgumentEvaluationOrder
 - MissingSideEffectsOnSelectorAccess
 - AbiReencodingHeadOverflowWithStaticArrayCleanup
 - DirtyBytesArrayToStorage
 - DataLocationChangeInInternalOverride
 - NestedCalldataArrayAbiReencodingSizeValidation
 - SignedImmutables
 - ABIDecodeTwoDimensionalArrayMemory
 - KeccakCaching.
It is used by:
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Parameter MetadataManager.updateSocialLinks(string,string,string,string)._telegram (contracts/metadata/Metada
Parameter MetadataManager.updateSocialLinks(string,string,string,string)._twitter (contracts/metadata/Metadat
Parameter MetadataManager.updateSocialLinks(string,string,string,string)._discord (contracts/metadata/Metadat
Parameter MetadataManager.updateSocialLinks(string,string,string,string)._github (contracts/metadata/Metadata
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conve
INFO:Detectors:
MetadataManager.tokenContract (contracts/metadata/MetadataManager.sol#9) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declar
INFO:Slither:contracts/metadata/MetadataManager.sol analyzed (9 contracts with 100 detectors), 23 result(s) f
```

Mythril

```
/Users/irfangedik/Desktop/sozlesme_deneme/USDTg_UltraSecureToken/.venv/lib/python3.9/site-packages/urllib3/__
  warnings.warn(
mythril.interfaces.cli [ERROR]: Input file not found [Errno 2] No such file or directory: '@openzeppelin/cont
```

Surya Analysis Summary

```
Total functions: 4
Public: 1, External: 3
Protected by 'onlyMultisigOrTimelock': 0
Protected by 'onlyRole': 3
Unprotected (no critical modifier) public/external functions: 0
```

Surya Function Map

```
 +  MetadataManager [90m(AccessControl)[39m
    - [32m[Pub][39m [90m[39m[31m #[39m
    - [34m[Ext][39m updateMetadata[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m updateSocialLinks[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m updateLogoURI[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m getFullMetadata
    - [34m[Ext][39m getWalletMetadata


[33m ($)[39m = payable function
[31m #[39m = non-constant function
```

Contract: GovernanceManager.sol

Slither

```
'forge config --json' running
Could not detect solc version from Foundry config. Falling back to system version...
'solc --version' running
'solc @openzeppelin 2/=node_modules/@openzeppelin 2/ @openzeppelin/=node_modules/@openzeppelin/ eth-gas-repor
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) has bi
  - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-exponentiation
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#120)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#121)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#122)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#123)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#124)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#125)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - prod0 = prod0 / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#104)
 - result = prod0 * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#131)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
GovernanceManager.constructor(address)._tokenContract (contracts/governance/GovernanceManager.sol#41) lacks a
  - tokenContract = _tokenContract (contracts/governance/GovernanceManager.sol#42)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
GovernanceManager.vote(uint256,bool) (contracts/governance/GovernanceManager.sol#96-116) uses timestamp for c
 Dangerous comparisons:
 - require(bool,string)(proposal.id == proposalId,Proposal does not exist) (contracts/governance/GovernanceMa
 - require(bool,string)(block.timestamp <= proposal.endTime,Voting period ended) (contracts/governance/Govern
 - require(bool,string)(! proposal.hasVoted[msg.sender],Already voted) (contracts/governance/GovernanceManage
 - require(bool,string)(! proposal.executed && ! proposal.canceled,Proposal not active) (contracts/governance
GovernanceManager.executeProposal(uint256) (contracts/governance/GovernanceManager.sol#118-128) uses timestam
 Dangerous comparisons:
 - require(bool,string)(proposal.id == proposalId,Proposal does not exist) (contracts/governance/GovernanceMa
 - require(bool,string)(block.timestamp > proposal.endTime,Voting period not ended) (contracts/governance/Gov
 - require(bool,string)(! proposal.executed,Already executed) (contracts/governance/GovernanceManager.sol#122
 - require(bool,string)(! proposal.canceled,Proposal canceled) (contracts/governance/GovernanceManager.sol#12
 - require(bool,string)(proposal.forVotes > proposal.againstVotes,Proposal not passed) (contracts/governance/
GovernanceManager.cancelProposal(uint256) (contracts/governance/GovernanceManager.sol#130-138) uses timestamp
 Dangerous comparisons:
 - require(bool,string)(proposal.id == proposalId,Proposal does not exist) (contracts/governance/GovernanceMa
 - require(bool,string)(! proposal.executed,Already executed) (contracts/governance/GovernanceManager.sol#133
 - require(bool,string)(! proposal.canceled,Already canceled) (contracts/governance/GovernanceManager.sol#134
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Strings.toString(uint256) (node_modules/@openzeppelin/contracts/utils/Strings.sol#19-39) uses assembly
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#25-27)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#31-33)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) uses a
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#62-66)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#85-92)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#99-108)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
2 different versions of Solidity are used:
 - Version constraint ^0.8.28 is used by:
  -^0.8.28 (contracts/governance/GovernanceManager.sol#2)
 - Version constraint ^0.8.0 is used by:
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
INFO:Detectors:
AccessControl._setRoleAdmin(bytes32,bytes32) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#2
AccessControl._setupRole(bytes32,address) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#206-
Context._contextSuffixLength() (node_modules/@openzeppelin/contracts/utils/Context.sol#25-27) is never used a
Context._msgData() (node_modules/@openzeppelin/contracts/utils/Context.sol#21-23) is never used and should be
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Version constraint ^0.8.0 contains known severe issues (https://solidity.readthedocs.io/en/latest/bugs.html)
 - FullInlinerNonExpressionSplitArgumentEvaluationOrder
 - MissingSideEffectsOnSelectorAccess
 - AbiReencodingHeadOverflowWithStaticArrayCleanup
 - DirtyBytesArrayToSt
 - DirtyBytesArrayToStorage
 - DataLocationChangeInInternalOverride
 - NestedCalldataArrayAbiReencodingSizeValidation
 - SignedImmutables
 - ABIDecodeTwoDimensionalArrayMemory
 - KeccakCaching.
It is used by:
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Parameter GovernanceManager.setMultisig(address)._multisig (contracts/governance/GovernanceManager.sol#63) is
Parameter GovernanceManager.setTimelock(address)._timelock (contracts/governance/GovernanceManager.sol#69) is
Parameter GovernanceManager.setMinDelay(uint256)._minDelay (contracts/governance/GovernanceManager.sol#75) is
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conve
INFO:Detectors:
GovernanceManager.tokenContract (contracts/governance/GovernanceManager.sol#10) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declar
INFO:Slither:contracts/governance/GovernanceManager.sol analyzed (9 contracts with 100 detectors), 25 result(
```

Mythril

```
/Users/irfangedik/Desktop/sozlesme_deneme/USDTg_UltraSecureToken/.venv/lib/python3.9/site-packages/urllib3/__
  warnings.warn(
mythril.interfaces.cli [ERROR]: Input file not found [Errno 2] No such file or directory: '@openzeppelin/cont
```

Surya Analysis Summary

```
Total functions: 9
Public: 1, External: 8
Protected by 'onlyMultisigOrTimelock': 0
Protected by 'onlyRole': 6
Unprotected (no critical modifier) public/external functions: 0
```

Surya Function Map

```
 +  GovernanceManager [90m(AccessControl)[39m
    - [32m[Pub][39m [90m[39m[31m #[39m
    - [34m[Ext][39m setGovernanceExecutor[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setMultisig[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setTimelock[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setMinDelay[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m createProposal[31m #[39m
    - [34m[Ext][39m vote[31m #[39m
    - [34m[Ext][39m executeProposal[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m cancelProposal[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m getProposal
    - [34m[Ext][39m hasVoted
    - [34m[Ext][39m getVote


[33m ($)[39m = payable function
[31m #[39m = non-constant function
```

Contract: VestingManager.sol

Slither

```
'forge config --json' running
Could not detect solc version from Foundry config. Falling back to system version...
```

```
'solc --version' running
'solc @openzeppelin 2/=node_modules/@openzeppelin 2/ @openzeppelin/=node_modules/@openzeppelin/ eth-gas-repor
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) has bi
  - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-exponentiation
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#120)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#121)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#122)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#123)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#124)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#125)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - prod0 = prod0 / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#104)
 - result = prod0 * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#131)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
VestingManager.constructor(address)._tokenContract (contracts/vesting/VestingManager.sol#15) lacks a zero-che
  - tokenContract = _tokenContract (contracts/vesting/VestingManager.sol#16)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
VestingManager.getVestingWallet(address) (contracts/vesting/VestingManager.sol#33-38) uses timestamp for comp
 Dangerous comparisons:
 - require(bool,string)(walletAddr != address(0),No vesting contract) (contracts/vesting/VestingManager.sol#3
VestingWallet._vestingSchedule(uint256,uint64) (node_modules/@openzeppelin/contracts/finance/VestingWallet.so
 Dangerous comparisons:
 - timestamp < start() (node_modules/@openzeppelin/contracts/finance/VestingWallet.sol#137)
 - timestamp > start() + duration() (node_modules/@openzeppelin/contracts/finance/VestingWallet.sol#139)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Address._revert(bytes,string) (node_modules/@openzeppelin/contracts/utils/Address.sol#231-243) uses assembly
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Address.sol#236-239)
Strings.toString(uint256) (node_modules/@openzeppelin/contracts/utils/Strings.sol#19-39) uses assembly
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#25-27)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#31-33)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) uses a
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#62-66)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#85-92)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#99-108)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
3 different versions of Solidity are used:
 - Version constraint ^0.8.28 is used by:
  -^0.8.28 (contracts/vesting/VestingManager.sol#2)
 - Version constraint ^0.8.0 is used by:
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/finance/VestingWallet.sol#3)
  -^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/IERC20.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/extensions/IERC20Permit.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
 - Version constraint ^0.8.1 is used by:
  -^0.8.1 (node_modules/@openzeppelin/contracts/utils/Address.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
INFO:Detectors:
AccessControl._setRoleAdmin(bytes32,bytes32) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#2
AccessControl._setupRole(bytes32,address) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#206-
Context._contextSuffixLength() (node_modules/@openzeppelin/contracts/utils/Context.sol#25-27) is never used a
Context._msgData() (node_modules/@openzeppelin/contracts/utils/Context.sol#21-23) is never used and should be
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Version constraint ^0.8.0 contains known severe issues (https://solidity.readthedocs.io/en/latest/bugs.html)
 - FullInlinerNonExpressionSplitArgumentEvaluationOrder
 - MissingSideEffectsOnSelectorAccess
 - AbiReencodingHeadOverflowWithStaticArrayCleanup
 - DirtyBytesArrayToStorage
 - DataLocationChangeInInternalOverride
 - NestedCalldataArrayAbiReencodingSizeValidation
 - SignedImmutables
 - ABIDecodeTwoDimensionalArrayMemory
 - KeccakCaching.
It is used by:
```

```
It is used by:
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/finance/VestingWallet.sol#3)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/IERC20.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/extensions/IERC20Permit.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Version constraint ^0.8.1 contains known severe issues (https://solidity.readthedocs.io/en/latest/bugs.html)
 - FullInlinerNonExpressionSplitArgumentEvaluationOrder
 - MissingSideEffectsOnSelectorAccess
 - AbiReencodingHeadOverflowWithStaticArrayCleanup
 - DirtyBytesArrayToStorage
 - DataLocationChangeInInternalOverride
 - NestedCalldataArrayAbiReencodingSizeValidation
 - SignedImmutables
 - ABIDecodeTwoDimensionalArrayMemory
 - KeccakCaching.
It is used by:
 - ^0.8.1 (node_modules/@openzeppelin/contracts/utils/Address.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in SafeERC20._callOptionalReturnBool(IERC20,bytes) (node_modules/@openzeppelin/contracts/token
 - (success,returndata) = address(token).call(data) (node_modules/@openzeppelin/contracts/token/ERC20/utils/S
Low level call in Address.sendValue(address,uint256) (node_modules/@openzeppelin/contracts/utils/Address.sol#
 - (success,None) = recipient.call{value: amount}() (node_modules/@openzeppelin/contracts/utils/Address.sol#6
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (node_modules/@openzeppelin/con
 - (success,returndata) = target.call{value: value}(data) (node_modules/@openzeppelin/contracts/utils/Address
Low level call in Address.functionStaticCall(address,bytes,string) (node_modules/@openzeppelin/contracts/util
 - (success,returndata) = target.staticcall(data) (node_modules/@openzeppelin/contracts/utils/Address.sol#160
Low level call in Address.functionDelegateCall(address,bytes,string) (node_modules/@openzeppelin/contracts/ut
 - (success,returndata) = target.delegatecall(data) (node_modules/@openzeppelin/contracts/utils/Address.sol#1
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Function IERC20Permit.DOMAIN_SEPARATOR() (node_modules/@openzeppelin/contracts/token/ERC20/extensions/IERC20P
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conve
INFO:Detectors:
VestingManager.tokenContract (contracts/vesting/VestingManager.sol#11) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declar
INFO:Slither:contracts/vesting/VestingManager.sol analyzed (14 contracts with 100 detectors), 29 result(s) fo
```

Mythril

```
/Users/irfangedik/Desktop/sozlesme_deneme/USDTg_UltraSecureToken/.venv/lib/python3.9/site-packages/urllib3/__
  warnings.warn(
mythril.interfaces.cli [ERROR]: Input file not found [Errno 2] No such file or directory: '@openzeppelin/cont
```

Surya Analysis Summary

```
Total functions: 3
Public: 1, External: 2
Protected by 'onlyMultisigOrTimelock': 0
Protected by 'onlyRole': 1
Unprotected (no critical modifier) public/external functions: 1

Unprotected functions:
- [34m[Ext][39m transferToVesting[31m #[39m
```

Surya Function Map

```
 +  VestingManager [90m(AccessControl)[39m
    - [32m[Pub][39m [90m[39m[31m #[39m
    - [34m[Ext][39m createVestingWallet[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m getVestingWallet
    - [34m[Ext][39m transferToVesting[31m #[39m
       - modifiers: onlyTokenContract


[33m ($)[39m = payable function
[31m #[39m = non-constant function
```

Contract: StablecoinManager.sol

Slither

```
'forge config --json' running
Could not detect solc version from Foundry config. Falling back to system version...
'solc --version' running
'solc @openzeppelin 2/=node_modules/@openzeppelin 2/ @openzeppelin/=node_modules/@openzeppelin/ eth-gas-repor
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) has bi
  - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-exponentiation
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#120)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#121)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#122)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#123)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#124)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#125)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - prod0 = prod0 / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#104)
 - result = prod0 * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#131)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
StablecoinManager.constructor(address)._tokenContract (contracts/stablecoin/StablecoinManager.sol#19) lacks a
  - tokenContract = _tokenContract (contracts/stablecoin/StablecoinManager.sol#20)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
Reentrancy in StablecoinManager.buyTokenWithStable(address,uint256) (contracts/stablecoin/StablecoinManager.s
 External calls:
 - require(bool,string)(IERC20(stableToken).transferFrom(msg.sender,address(this),stableAmount),Transfer fail
 - ITokenMinter(tokenContract).mintForStablecoin(msg.sender,tokensToReceive) (contracts/stablecoin/Stablecoin
 Event emitted after the call(s):
 - TokenPurchased(msg.sender,stableAmount,tokensToReceive) (contracts/stablecoin/StablecoinManager.sol#52)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
Strings.toString(uint256) (node_modules/@openzeppelin/contracts/utils/Strings.sol#19-39) uses assembly
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#25-27)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#31-33)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) uses a
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#62-66)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#85-92)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#99-108)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
2 different versions of Solidity are used:
 - Version constraint ^0.8.28 is used by:
  -^0.8.28 (contracts/stablecoin/StablecoinManager.sol#2)
 - Version constraint ^0.8.0 is used by:
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/IERC20.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
INFO:Detectors:
AccessControl._setRoleAdmin(bytes32,bytes32) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#2
AccessControl._setupRole(bytes32,address) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#206-
Context._contextSuffixLength() (node_modules/@openzeppelin/contracts/utils/Context.sol#25-27) is never used a
Context._msgData() (node_modules/@openzeppelin/contracts/utils/Context.sol#21-23) is never used and should be
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Version constraint ^0.8.0 contains known severe issues (https://solidity.readthedocs.io/en/latest/bugs.html)
 - FullInlinerNonExpressionSplitArgumentEvaluationOrder
 - MissingSideEffectsOnSelectorAccess
 - AbiReencodingHeadOverflowWithStaticArrayCleanup
 - DirtyBytesArrayToStorage
 - DataLocationChangeInInternalOverride
 - NestedCalldataArrayAbiReencodingSizeValidation
 - SignedImmutables
 - ABIDecodeTwoDimensionalArrayMemory
 - KeccakCaching.
It is used by:
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/IERC20.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
StablecoinManager.tokenContract (contracts/stablecoin/StablecoinManager.sol#13) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declar
INFO:Slither:contracts/stablecoin/StablecoinManager.sol analyzed (12 contracts with 100 detectors), 20 result
```

Mythril

```
/Users/irfangedik/Desktop/sozlesme_deneme/USDTg_UltraSecureToken/.venv/lib/python3.9/site-packages/urllib3/__
  warnings.warn(
mythril.interfaces.cli [ERROR]: Input file not found [Errno 2] No such file or directory: '@openzeppelin/cont
```

Surya Analysis Summary

```
Total functions: 5
Public: 1, External: 4
Protected by 'onlyMultisigOrTimelock': 0
Protected by 'onlyRole': 2
Unprotected (no critical modifier) public/external functions: 0
```

Surya Function Map

```
 +  StablecoinManager [90m(AccessControl)[39m
    - [32m[Pub][39m [90m[39m[31m #[39m
    - [34m[Ext][39m setStableTokenWhitelist[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setUSDPrice[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m buyTokenWithStable[31m #[39m
    - [34m[Ext][39m getUsdPricePerToken
    - [34m[Ext][39m isStableTokenWhitelisted

 + [34m[Int][39m ITokenMinter
    - [34m[Ext][39m mintForStablecoin[31m #[39m


[33m ($)[39m = payable function
[31m #[39m = non-constant function
```

Contract: RoleManager.sol

Slither

```
'forge config --json' running
Could not detect solc version from Foundry config. Falling back to system version...
'solc --version' running
'solc @openzeppelin 2/=node_modules/@openzeppelin 2/ @openzeppelin/=node_modules/@openzeppelin/ eth-gas-repor
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) has bi
  - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-exponentiation
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#120)
```

```
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#121)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#122)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#123)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#124)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#125)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - prod0 = prod0 / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#104)
 - result = prod0 * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#131)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
RoleManager.constructor(address)._tokenContract (contracts/access/RoleManager.sol#28) lacks a zero-check on :
  - tokenContract = _tokenContract (contracts/access/RoleManager.sol#29)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
Strings.toString(uint256) (node_modules/@openzeppelin/contracts/utils/Strings.sol#19-39) uses assembly
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#25-27)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#31-33)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) uses a
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#62-66)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#85-92)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#99-108)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
2 different versions of Solidity are used:
 - Version constraint ^0.8.28 is used by:
  -^0.8.28 (contracts/access/RoleManager.sol#2)
 - Version constraint ^0.8.0 is used by:
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
INFO:Detectors:
AccessControl._setRoleAdmin(bytes32,bytes32) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#2
AccessControl._setupRole(bytes32,address) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#206-
Context._contextSuffixLength() (node_modules/@openzeppelin/contracts/utils/Context.sol#25-27) is never used a
Context._msgData() (node_modules/@openzeppelin/contracts/utils/Context.sol#21-23) is never used and should be
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Version constraint ^0.8.0 contains known severe issues (https://solidity.readthedocs.io/en/latest/bugs.html)
 - FullInlinerNonExpressionSplitArgumentEvaluationOrder
 - MissingSideEffectsOnSelectorAccess
 - AbiReencodingHeadOverflowWithStaticArrayCleanup
 - DirtyBytesArrayToStorage
 - DataLocationChangeInInternalOverride
 - NestedCalldataArrayAbiReencodingSizeValidation
 - SignedImmutables
 - ABIDecodeTwoDimensionalArrayMemory
 - KeccakCaching.
It is used by:
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
RoleManager.tokenContract (contracts/access/RoleManager.sol#7) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declar
INFO:Slither:contracts/access/RoleManager.sol analyzed (9 contracts with 100 detectors), 19 result(s) found
```

Mythril

```
/Users/irfangedik/Desktop/sozlesme_deneme/USDTg_UltraSecureToken/.venv/lib/python3.9/site-packages/urllib3/__
  warnings.warn(
mythril.interfaces.cli [ERROR]: Input file not found [Errno 2] No such file or directory: '@openzeppelin/cont
```

Surya Analysis Summary

```
Total functions: 5
Public: 3, External: 2
Protected by 'onlyMultisigOrTimelock': 0
Protected by 'onlyRole': 4
Unprotected (no critical modifier) public/external functions: 0
```

Surya Function Map

```
 +  RoleManager [90m(AccessControl)[39m
    - [32m[Pub][39m [90m[39m[31m #[39m
    - [90m[Int][39m _setupRoleHierarchy[31m #[39m
    - [32m[Pub][39m grantRole[31m #[39m
       - modifiers: onlyRole
    - [32m[Pub][39m revokeRole[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m grantMultipleRoles[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m revokeMultipleRoles[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m hasAnyRole
    - [34m[Ext][39m hasAllRoles
    - [34m[Ext][39m getRoleMembers
    - [34m[Ext][39m getAccountRoles
    - [34m[Ext][39m isOwner
    - [34m[Ext][39m isMinter
    - [34m[Ext][39m isBurner
    - [34m[Ext][39m isPauser
    - [34m[Ext][39m isBlacklistManager
    - [34m[Ext][39m isEmergencyRole


[33m ($)[39m = payable function
[31m #[39m = non-constant function
```

Contract: AccessManager.sol

Slither

```
'forge config --json' running
Could not detect solc version from Foundry config. Falling back to system version...
'solc --version' running
'solc @openzeppelin 2/=node_modules/@openzeppelin 2/ @openzeppelin/=node_modules/@openzeppelin/ eth-gas-repor
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) has bi
  - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-exponentiation
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#120)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#121)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#122)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#123)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#124)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#125)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - prod0 = prod0 / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#104)
 - result = prod0 * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#131)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
Strings.toString(uint256) (node_modules/@openzeppelin/contracts/utils/Strings.sol#19-39) uses assembly
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#25-27)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#31-33)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) uses a
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#62-66)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#85-92)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#99-108)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
2 different versions of Solidity are used:
 - Version constraint ^0.8.28 is used by:
  -^0.8.28 (contracts/access/AccessManager.sol#2)
 - Version constraint ^0.8.0 is used by:
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
INFO:Detectors:
AccessControl._setRoleAdmin(bytes32,bytes32) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#2
AccessControl._setupRole(bytes32,address) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#206-
Context._contextSuffixLength() (node_modules/@openzeppelin/contracts/utils/Context.sol#25-27) is never used a
Context._msgData() (node_modules/@openzeppelin/contracts/utils/Context.sol#21-23) is never used and should be
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Version constraint ^0.8.0 contains known severe issues (https://solidity.readthedocs.io/en/latest/bugs.html)
 - FullInlinerNonExpressionSplitArgumentEvaluationOrder
 - MissingSideEffectsOnSelectorAccess
 - AbiReencodingHeadOverflowWithStaticArrayCleanup
 - DirtyBytesArrayToStorage
 - DataLocationChangeInInternalOverride
 - NestedCalldataArrayAbiReencodingSizeValidation
 - SignedImmutables
 - ABIDecodeTwoDimensionalArrayMemory
 - KeccakCaching.
It is used by:
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Parameter AccessManager.setMultisig(address)._multi (contracts/access/AccessManager.sol#41) is not in mixedCa
Parameter AccessManager.setTimelock(address)._timelock (contracts/access/AccessManager.sol#48) is not in mixe
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conve
INFO:Slither:contracts/access/AccessManager.sol analyzed (9 contracts with 100 detectors), 19 result(s) found
```

Mythril

```
/Users/irfangedik/Desktop/sozlesme_deneme/USDTg_UltraSecureToken/.venv/lib/python3.9/site-packages/urllib3/__
  warnings.warn(
mythril.interfaces.cli [ERROR]: input files do not contain any valid contracts
```

Surya Analysis Summary

```
Total functions: 3
Public: 0, External: 3
Protected by 'onlyMultisigOrTimelock': 0
Protected by 'onlyRole': 3
Unprotected (no critical modifier) public/external functions: 0
```

Surya Function Map

```
 +  AccessManager [90m(AccessControl)[39m
    - [34m[Ext][39m setGovernanceExecutor[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setMultisig[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m setTimelock[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m getAccessInfo


[33m ($)[39m = payable function
[31m #[39m = non-constant function
```

Contract: MultisigWallet.sol

Slither

```
'forge config --json' running
Could not detect solc version from Foundry config. Falling back to system version...
'solc --version' running
'solc @openzeppelin 2/=node_modules/@openzeppelin 2/ @openzeppelin/=node_modules/@openzeppelin/ eth-gas-repor
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) has bi
  - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-exponentiation
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse = (3 * denominator) ^ 2 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#116)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#120)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#121)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#122)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#123)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#124)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - denominator = denominator / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#101)
 - inverse *= 2 - denominator * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#125)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) perfor
 - prod0 = prod0 / twos (node_modules/@openzeppelin/contracts/utils/math/Math.sol#104)
 - result = prod0 * inverse (node_modules/@openzeppelin/contracts/utils/math/Math.sol#131)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
MultisigWallet.constructor(address,address[],uint256)._tokenContract (contracts/multisig/MultisigWallet.sol#4
  - tokenContract = _tokenContract (contracts/multisig/MultisigWallet.sol#41)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
MultisigWallet.executeTransaction(uint256) (contracts/multisig/MultisigWallet.sol#142-157) uses timestamp for
 Dangerous comparisons:
  - require(bool,string)(transaction.confirmations >= requiredSignatures,Insufficient confirmations) (contract
 - require(bool,string)(transaction.confirmations >= requiredSignatures,Insufficient confirmations) (contract
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Strings.toString(uint256) (node_modules/@openzeppelin/contracts/utils/Strings.sol#19-39) uses assembly
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#25-27)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/Strings.sol#31-33)
Math.mulDiv(uint256,uint256,uint256) (node_modules/@openzeppelin/contracts/utils/math/Math.sol#55-134) uses a
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#62-66)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#85-92)
 - INLINE ASM (node_modules/@openzeppelin/contracts/utils/math/Math.sol#99-108)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
2 different versions of Solidity are used:
 - Version constraint ^0.8.28 is used by:
  -^0.8.28 (contracts/multisig/MultisigWallet.sol#2)
 - Version constraint ^0.8.0 is used by:
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/security/ReentrancyGuard.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
INFO:Detectors:
MultisigWallet.removeSigner(address) (contracts/multisig/MultisigWallet.sol#170-187) has costly operations in
 - signers.pop() (contracts/multisig/MultisigWallet.sol#181)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#costly-operations-inside-a-loop
INFO:Detectors:
AccessControl._setRoleAdmin(bytes32,bytes32) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#2
AccessControl._setupRole(bytes32,address) (node_modules/@openzeppelin/contracts/access/AccessControl.sol#206-
Context._contextSuffixLength() (node_modules/@openzeppelin/contracts/utils/Context.sol#25-27) is never used a
Context._msgData() (node_modules/@openzeppelin/contracts/utils/Context.sol#21-23) is never used and should be
ReentrancyGuard._reentrancyGuardEntered() (node_modules/@openzeppelin/contracts/security/ReentrancyGuard.sol#
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Version constraint ^0.8.0 contains known severe issues (https://solidity.readthedocs.io/en/latest/bugs.html)
 - FullInlinerNonExpressionSplitArgumentEvaluationOrder
 - MissingSideEffectsOnSelectorAccess
 - AbiReencodingHeadOverflowWithStaticArrayCleanup
 - DirtyBytesArrayToStorage
 - DataLocationChangeInInternalOverride
 - NestedCalldataArrayAbiReencodingSizeValidation
 - SignedImmutables
 - ABIDecodeTwoDimensionalArrayMemory
 - KeccakCaching.
It is used by:
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/AccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/access/IAccessControl.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/security/ReentrancyGuard.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Strings.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/ERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/introspection/IERC165.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/Math.sol#4)
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SignedMath.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in MultisigWallet.executeTransaction(uint256) (contracts/multisig/MultisigWallet.sol#142-157):
 - (success,None) = transaction.target.call{value: transaction.value}(transaction.data) (contracts/multisig/M
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Loop condition i < signers.length (contracts/multisig/MultisigWallet.sol#228) should use cached array length
 Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#cache-array-length
INFO:Detectors:
MultisigWallet.tokenContract (contracts/multisig/MultisigWallet.sol#8) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declar
INFO:Slither:contracts/multisig/MultisigWallet.sol analyzed (10 contracts with 100 detectors), 24 result(s) f
```

Mythril

```
/Users/irfangedik/Desktop/sozlesme_deneme/USDTg_UltraSecureToken/.venv/lib/python3.9/site-packages/urllib3/__
  warnings.warn(
mythril.interfaces.cli [ERROR]: Input file not found [Errno 2] No such file or directory: '@openzeppelin/cont
```

Surya Analysis Summary

```
Total functions: 10
Public: 2, External: 8
Protected by 'onlyMultisigOrTimelock': 0
Protected by 'onlyRole': 3
Unprotected (no critical modifier) public/external functions: 6

Unprotected functions:
- [34m[Ext][39m submitTransaction[31m #[39m
- [34m[Ext][39m confirmTransaction[31m #[39m
- [34m[Ext][39m revokeConfirmation[31m #[39m
- [32m[Pub][39m executeTransaction[31m #[39m
- [34m[Ext][39m emergencyPause[31m #[39m
- [34m[Ext][39m emergencyUnpause[31m #[39m
```

Surya Function Map

```
 +  MultisigWallet [90m(AccessControl, ReentrancyGuard)[39m
    - [32m[Pub][39m [90m[39m[31m #[39m
    - [34m[Ext][39m submitTransaction[31m #[39m
       - modifiers: onlySigner
    - [34m[Ext][39m confirmTransaction[31m #[39m
       - modifiers: onlySigner,transactionExists,notExecuted,notConfirmed
    - [34m[Ext][39m revokeConfirmation[31m #[39m
       - modifiers: onlySigner,transactionExists,notExecuted
    - [32m[Pub][39m executeTransaction[31m #[39m
       - modifiers: onlySigner,transactionExists,notExecuted,nonReentrant
    - [34m[Ext][39m addSigner[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m removeSigner[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m updateRequiredSignatures[31m #[39m
       - modifiers: onlyRole
    - [34m[Ext][39m getTransaction
    - [34m[Ext][39m getSigners
    - [34m[Ext][39m isConfirmed
    - [34m[Ext][39m getTransactionConfirmations
    - [34m[Ext][39m getPendingTransactions
    - [34m[Ext][39m emergencyPause[31m #[39m
       - modifiers: onlySigner
    - [34m[Ext][39m emergencyUnpause[31m #[39m
       - modifiers: onlySigner
    - [34m[Ext][39m [90m[39m[33m ($)[39m


[33m ($)[39m = payable function
[31m #[39m = non-constant function
```

Contract: CounterManager.sol

Slither

```
'forge config --json' running
Could not detect solc version from Foundry config. Falling back to system version...
'solc --version' running
'solc @openzeppelin 2/=node_modules/@openzeppelin 2/ @openzeppelin/=node_modules/@openzeppelin/ eth-gas-repor
INFO:Detectors:
2 different versions of Solidity are used:
 - Version constraint ^0.8.28 is used by:
  -^0.8.28 (contracts/interfaces/ICounter.sol#2)
  -^0.8.28 (contracts/utils/CounterManager.sol#2)
 - Version constraint ^0.8.0 is used by:
  -^0.8.0 (node_modules/@openzeppelin/contracts/utils/Counters.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
INFO:Detectors:
CounterManager._decrement() (contracts/utils/CounterManager.sol#103-106) is never used and should be removed
CounterManager._getCounter() (contracts/utils/CounterManager.sol#86-88) is never used and should be removed
CounterManager._increment() (contracts/utils/CounterManager.sol#94-97) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Version constraint ^0.8.0 contains known severe issues (https://solidity.readthedocs.io/en/latest/bugs.html)
 - FullInlinerNonExpressionSplitArgumentEvaluationOrder
 - MissingSideEffectsOnSelectorAccess
 - AbiReencodingHeadOverflowWithStaticArrayCleanup
 - DirtyBytesArrayToStorage
 - DataLocationChangeInInternalOverride
 - NestedCalldataArrayAbiReencodingSizeValidation
 - SignedImmutables
 - ABIDecodeTwoDimensionalArrayMemory
 - KeccakCaching.
It is used by:
 - ^0.8.0 (node_modules/@openzeppelin/contracts/utils/Counters.sol#4)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Slither:contracts/utils/CounterManager.sol analyzed (3 contracts with 100 detectors), 5 result(s) found
```

Mythril

```
/Users/irfangedik/Desktop/sozlesme_deneme/USDTg_UltraSecureToken/.venv/lib/python3.9/site-packages/urllib3/__
  warnings.warn(
mythril.interfaces.cli [ERROR]: Input file not found [Errno 2] No such file or directory: '@openzeppelin/cont
```

Surya Analysis Summary

```
Total functions: 6
Public: 0, External: 6
Protected by 'onlyMultisigOrTimelock': 0
Protected by 'onlyRole': 0
Unprotected (no critical modifier) public/external functions: 0
```

Surya Function Map

```
 +  CounterManager [90m(ICounter)[39m
    - [34m[Ext][39m current
    - [34m[Ext][39m increment[31m #[39m
    - [34m[Ext][39m decrement[31m #[39m
    - [34m[Ext][39m reset[31m #[39m
    - [34m[Ext][39m set[31m #[39m
    - [34m[Ext][39m add[31m #[39m
    - [34m[Ext][39m subtract[31m #[39m
    - [90m[Int][39m _getCounter
    - [90m[Int][39m _increment[31m #[39m
    - [90m[Int][39m _decrement[31m #[39m


[33m ($)[39m = payable function
[31m #[39m = non-constant function
```

Echidna

```
[2025-06-16 23:49:51.27] Compiling contracts/USDExchangeToken.sol... Done! (3.265453s)
Multiple contracts found, only analyzing the first
Analyzing contract: /Users/irfangedik/Desktop/sozlesme_deneme/USDTg_UltraSecureToken/contracts/USDExchangeTok
[2025-06-16 23:49:54.57] Running slither on contracts/USDExchangeToken.sol... Done! (3.845582s)
[2025-06-16 23:49:58.49] [Worker 3] New coverage: 3797 instr, 1 contracts, 1 seqs in corpus
```

```
[2025-06-16 23:49:58.50] [Worker 1] New coverage: 3797 instr, 1 contracts, 2 seqs in corpus
[2025-06-16 23:49:58.50] [Worker 0] New coverage: 3797 instr, 1 contracts, 3 seqs in corpus
[2025-06-16 23:49:58.50] [Worker 2] New coverage: 3797 instr, 1 contracts, 4 seqs in corpus
[2025-06-16 23:49:58.55] [Worker 3] New coverage: 3809 instr, 1 contracts, 5 seqs in corpus
[2025-06-16 23:49:58.60] [Worker 3] New coverage: 3890 instr, 1 contracts, 6 seqs in corpus
[2025-06-16 23:49:58.65] [Worker 3] New coverage: 3930 instr, 1 contracts, 7 seqs in corpus
[2025-06-16 23:49:58.77] [Worker 2] New coverage: 4026 instr, 1 contracts, 8 seqs in corpus
[2025-06-16 23:49:58.77] [Worker 3] New coverage: 4026 instr, 1 contracts, 9 seqs in corpus
[2025-06-16 23:49:58.78] [Worker 1] New coverage: 4026 instr, 1 contracts, 10 seqs in corpus
[2025-06-16 23:49:59.05] [Worker 2] New coverage: 4056 instr, 1 contracts, 11 seqs in corpus
[2025-06-16 23:49:59.73] [Worker 0] New coverage: 4086 instr, 1 contracts, 12 seqs in corpus
[2025-06-16 23:50:00.04] [Worker 0] New coverage: 4117 instr, 1 contracts, 13 seqs in corpus
[2025-06-16 23:50:00.07] [Worker 2] New coverage: 4150 instr, 1 contracts, 14 seqs in corpus
[2025-06-16 23:50:00.29] [Worker 2] New coverage: 4319 instr, 1 contracts, 15 seqs in corpus
[2025-06-16 23:50:00.96] [Worker 1] New coverage: 4324 instr, 1 contracts, 16 seqs in corpus
[2025-06-16 23:50:01.20] [Worker 3] New coverage: 4420 instr, 1 contracts, 17 seqs in corpus
[2025-06-16 23:50:01.21] [Worker 0] New coverage: 4420 instr, 1 contracts, 18 seqs in corpus
[2025-06-16 23:50:01.43] [status] tests: 0/88, fuzzing: 23425/50000, values: [], cov: 4420, corpus: 18
[2025-06-16 23:50:01.82] [Worker 3] New coverage: 4455 instr, 1 contracts, 19 seqs in corpus
[2025-06-16 23:50:01.89] [Worker 1] New coverage: 4515 instr, 1 contracts, 20 seqs in corpus
[2025-06-16 23:50:02.52] [Worker 3] New coverage: 4537 instr, 1 contracts, 21 seqs in corpus
[2025-06-16 23:50:02.61] [Worker 1] New coverage: 4600 instr, 1 contracts, 22 seqs in corpus
[2025-06-16 23:50:02.62] [Worker 2] New coverage: 4635 instr, 1 contracts, 23 seqs in corpus
[2025-06-16 23:50:02.78] [Worker 0] New coverage: 4693 instr, 1 contracts, 24 seqs in corpus
[2025-06-16 23:50:03.01] [Worker 0] New coverage: 4724 instr, 1 contracts, 25 seqs in corpus
[2025-06-16 23:50:03.43] [Worker 3] Test limit reached. Stopping.
[2025-06-16 23:50:03.45] [Worker 0] Test limit reached. Stopping.
[2025-06-16 23:50:03.49] [Worker 1] Test limit reached. Stopping.
[2025-06-16 23:50:03.50] [Worker 2] Test limit reached. Stopping.
[2025-06-16 23:50:03.50] [status] tests: 0/88, fuzzing: 50249/50000, values: [], cov: 4724, corpus: 25
roleManager(): passing
name(): passing
approve(address,uint256): passing
executeProposal(uint256): passing
submitMultisigTransaction(address,uint256,bytes,string): passing
setMetadataManager(address): passing
setUSDPrice(uint256): passing
setVestingManager(address): passing
totalSupply(): passing
grantMultipleRoles(bytes32[],address): passing
transferFrom(address,address,uint256): passing
setDailyTransferLimit(address,uint256): passing
BURNER_ROLE(): passing
confirmMultisigTransaction(uint256): passing
isEmergencyRole(address): passing
getMultisigTransaction(uint256): passing
grantRole(bytes32,address): passing
isOwner(address): passing
decimals(): passing
increaseAllowance(address,uint256): passing
isBlacklistManager(address): passing
unpause(): passing
mint(address,uint256): passing
BLACKLIST_MANAGER_ROLE(): passing
transferToVesting(address,uint256): passing
burn(uint256): passing
isBurner(address): passing
isPauser(address): passing
setFeeManager(address): passing
createProposal(string): passing
setSecurityBlacklistStatus(address,bool): passing
getPendingMultisigTransactions(): passing
metadataManager(): passing
buyTokenWithStable(address,uint256): passing
setStablecoinManager(address): passing
isSecurityBlacklisted(address): passing
counterManager(): passing
getWalletMetadata(): passing
paused(): passing
updateLogoURI(string): passing
setMultisigWallet(address): passing
getMultisigSigners(): passing
setFee(uint256): passing
balanceOf(address): passing
setFeeExemption(address,bool): passing
burnFrom(address,uint256): passing
revokeMultisigConfirmation(uint256): passing
lockWallet(address,bool): passing
setStableTokenWhitelist(address,bool): passing
pause(): passing
changeAdmin(address): passing
multisigWallet(): passing
setCounterManager(address): passing
setSecurityManager(address): passing
symbol(): passing
updateSocialLinks(string,string,string,string): passing
DEFAULT_ADMIN_ROLE(): passing
lockTokens(address,uint256,uint256): passing
decreaseAllowance(address,uint256): passing
transfer(address,uint256): passing
isMinter(address): passing
setBotStatus(address,bool): passing
getFullMetadata(): passing
executeMultisigTransaction(uint256): passing
executeMultisigTransaction(uint256): passing
setTimelock(address): passing
getProposal(uint256): passing
stablecoinManager(): passing
vote(uint256,bool): passing
unlockTokens(address): passing
getVestingWallet(address): passing
feeManager(): passing
governanceManager(): passing
timelock(): passing
MINTER_ROLE(): passing
revokeRole(bytes32,address): passing
vestingManager(): passing
updateMetadata(string,string,string): passing
allowance(address,address): passing
securityManager(): passing
setGovernanceManager(address): passing
PAUSER_ROLE(): passing
setFeeRecipient(address): passing
setTransferLimit(address,uint256): passing
setRoleManager(address): passing
mintForStablecoin(address,uint256): passing
revokeMultipleRoles(bytes32[],address): passing
createVestingWallet(address,uint256): passing
AssertionFailed(..): passing


Unique instructions: 4724
Unique codehashes: 1
Corpus size: 25
Seed: 2166347443694560111
Total calls: 50249
```

Scribble Tests

```
[2025-06-16 23:50:05.19] Compiling contracts/USDExchangeToken.sol... Done! (3.2169s)
Multiple contracts found, only analyzing the first
Analyzing contract: /Users/irfangedik/Desktop/sozlesme_deneme/USDTg_UltraSecureToken/contracts/USDExchangeTok
[2025-06-16 23:50:08.43] Running slither on contracts/USDExchangeToken.sol... Done! (3.976892s)
[2025-06-16 23:50:12.49] [Worker 0] New coverage: 3834 instr, 1 contracts, 1 seqs in corpus
[2025-06-16 23:50:12.49] [Worker 1] New coverage: 3834 instr, 1 contracts, 2 seqs in corpus
[2025-06-16 23:50:12.49] [Worker 3] New coverage: 3834 instr, 1 contracts, 3 seqs in corpus
[2025-06-16 23:50:12.50] [Worker 2] New coverage: 3834 instr, 1 contracts, 4 seqs in corpus
[2025-06-16 23:50:12.54] [Worker 3] New coverage: 3966 instr, 1 contracts, 5 seqs in corpus
[2025-06-16 23:50:12.54] [Worker 0] New coverage: 3966 instr, 1 contracts, 6 seqs in corpus
[2025-06-16 23:50:12.67] [Worker 3] New coverage: 3988 instr, 1 contracts, 7 seqs in corpus
[2025-06-16 23:50:12.69] [Worker 2] New coverage: 3988 instr, 1 contracts, 8 seqs in corpus
[2025-06-16 23:50:12.73] [Worker 2] New coverage: 3991 instr, 1 contracts, 9 seqs in corpus
[2025-06-16 23:50:12.85] [Worker 0] New coverage: 4026 instr, 1 contracts, 10 seqs in corpus
[2025-06-16 23:50:12.95] [Worker 1] New coverage: 4084 instr, 1 contracts, 11 seqs in corpus
[2025-06-16 23:50:13.05] [Worker 2] New coverage: 4148 instr, 1 contracts, 12 seqs in corpus
[2025-06-16 23:50:13.36] [Worker 2] New coverage: 4183 instr, 1 contracts, 13 seqs in corpus
[2025-06-16 23:50:13.70] [Worker 3] New coverage: 4214 instr, 1 contracts, 14 seqs in corpus
[2025-06-16 23:50:13.79] [Worker 3] New coverage: 4249 instr, 1 contracts, 15 seqs in corpus
[2025-06-16 23:50:13.88] [Worker 2] New coverage: 4279 instr, 1 contracts, 16 seqs in corpus
[2025-06-16 23:50:14.00] [Worker 2] New coverage: 4299 instr, 1 contracts, 17 seqs in corpus
[2025-06-16 23:50:14.35] [Worker 0] New coverage: 4365 instr, 1 contracts, 18 seqs in corpus
[2025-06-16 23:50:14.59] [Worker 1] New coverage: 4390 instr, 1 contracts, 19 seqs in corpus
[2025-06-16 23:50:15.02] [Worker 3] New coverage: 4394 instr, 1 contracts, 20 seqs in corpus
[2025-06-16 23:50:15.30] [Worker 1] New coverage: 4424 instr, 1 contracts, 21 seqs in corpus
[2025-06-16 23:50:15.41] [status] tests: 0/88, fuzzing: 29474/50000, values: [], cov: 4424, corpus: 21
[2025-06-16 23:50:15.43] [Worker 3] New coverage: 4454 instr, 1 contracts, 22 seqs in corpus
[2025-06-16 23:50:15.54] [Worker 0] New coverage: 4485 instr, 1 contracts, 23 seqs in corpus
[2025-06-16 23:50:16.33] [Worker 3] New coverage: 4520 instr, 1 contracts, 24 seqs in corpus
[2025-06-16 23:50:16.45] [Worker 0] New coverage: 4550 instr, 1 contracts, 25 seqs in corpus
[2025-06-16 23:50:16.51] [Worker 0] New coverage: 4580 instr, 1 contracts, 26 seqs in corpus
[2025-06-16 23:50:16.54] [Worker 0] New coverage: 4601 instr, 1 contracts, 27 seqs in corpus
[2025-06-16 23:50:16.76] [Worker 1] New coverage: 4776 instr, 1 contracts, 28 seqs in corpus
[2025-06-16 23:50:16.89] [Worker 3] Test limit reached. Stopping.
[2025-06-16 23:50:16.90] [Worker 1] Test limit reached. Stopping.
[2025-06-16 23:50:16.92] [Worker 0] Test limit reached. Stopping.
[2025-06-16 23:50:16.92] [Worker 2] Test limit reached. Stopping.
[2025-06-16 23:50:16.92] [status] tests: 0/88, fuzzing: 50058/50000, values: [], cov: 4776, corpus: 28
roleManager(): passing
name(): passing
approve(address,uint256): passing
executeProposal(uint256): passing
submitMultisigTransaction(address,uint256,bytes,string): passing
setMetadataManager(address): passing
setUSDPrice(uint256): passing
setVestingManager(address): passing
totalSupply(): passing
grantMultipleRoles(bytes32[],address): passing
transferFrom(address,address,uint256): passing
```

```
setDailyTransferLimit(address,uint256): passing
BURNER_ROLE(): passing
confirmMultisigTransaction(uint256): passing
isEmergencyRole(address): passing
getMultisigTransaction(uint256): passing
grantRole(bytes32,address): passing
isOwner(address): passing
decimals(): passing
increaseAllowance(address,uint256): passing
isBlacklistManager(address): passing
unpause(): passing
mint(address,uint256): passing
BLACKLIST_MANAGER_ROLE(): passing
transferToVesting(address,uint256): passing
burn(uint256): passing
isBurner(address): passing
isPauser(address): passing
setFeeManager(address): passing
createProposal(string): passing
setSecurityBlacklistStatus(address,bool): passing
getPendingMultisigTransactions(): passing
metadataManager(): passing
buyTokenWithStable(address,uint256): passing
setStablecoinManager(address): passing
isSecurityBlacklisted(address): passing
counterManager(): passing
getWalletMetadata(): passing
paused(): passing
updateLogoURI(string): passing
setMultisigWallet(address): passing
getMultisigSigners(): passing
setFee(uint256): passing
balanceOf(address): passing
setFeeExemption(address,bool): passing
burnFrom(address,uint256): passing
revokeMultisigConfirmation(uint256): passing
lockWallet(address,bool): passing
setStableTokenWhitelist(address,bool): passing
pause(): passing
changeAdmin(address): passing
multisigWallet(): passing
setCounterManager(address): passing
setSecurityManager(address): passing
symbol(): passing
updateSocialLinks(string,string,string,string): passing
DEFAULT_ADMIN_ROLE(): passing
lockTokens(address,uint256,uint256): passing
decreaseAllowance(address,uint256): passing
transfer(address,uint256): passing
isMinter(address): passing
setBotStatus(address,bool): passing
getFullMetadata(): passing
executeMultisigTransaction(uint256): passing
setTimelock(address): passing
getProposal(uint256): passing
stablecoinManager(): passing
vote(uint256,bool): passing
unlockTokens(address): passing
getVestingWallet(address): passing
feeManager(): passing
governanceManager(): passing
timelock(): passing
MINTER_ROLE(): passing
revokeRole(bytes32,address): passing
vestingManager(): passing
updateMetadata(string,string,string): passing
allowance(address,address): passing
securityManager(): passing
setGovernanceManager(address): passing
PAUSER_ROLE(): passing
setFeeRecipient(address): passing
setTransferLimit(address,uint256): passing
setRoleManager(address): passing
mintForStablecoin(address,uint256): passing
revokeMultipleRoles(bytes32[],address): passing
createVestingWallet(address,uint256): passing
AssertionFailed(..): passing


Unique instructions: 4776
Unique codehashes: 1
Corpus size: 28
Seed: 8633611792248724317
Total calls: 50058
```

Foundry

```
Compiler run failed:
Error (6160): Wrong argument count for function call: 0 arguments given but expected 1.
  --> test/AccessControlTest.t.sol:16:23:
   |
16 |         roleManager = new RoleManager();
   |                       ^^^^^^^^^^^^^^^^^

Error (6160): Wrong argument count for function call: 7 arguments given but expected 0.
  --> test/AccessControlTest.t.sol:17:17:
   |
17 |         token = new USDeXchangeToken(
   |                 ^ (Relevant source part starts here and spans across multiple lines).

Error (6160): Wrong argument count for function call: 0 arguments given but expected 1.
  --> test/ReentrancyTest.t.sol:38:23:
   |
38 |         roleManager = new RoleManager();
   |                       ^^^^^^^^^^^^^^^^^

Error (6160): Wrong argument count for function call: 7 arguments given but expected 0.
  --> test/ReentrancyTest.t.sol:39:17:
   |
39 |         token = new USDeXchangeToken(
   |                 ^ (Relevant source part starts here and spans across multiple lines).
```

Hardhat

```
Compiled 1 Solidity file successfully (evm target: paris).

Error HH702: Invalid artifact path contracts/USDExchangeToken.sol:USDeXchangeToken, its correct case-sensitiv
For more info go to https://hardhat.org/HH702 or run Hardhat with --show-stack-traces
```

Emergency Tests

```
Compiler run failed:
Error (6160): Wrong argument count for function call: 0 arguments given but expected 1.
  --> test/AccessControlTest.t.sol:16:23:
   |
16 |         roleManager = new RoleManager();
   |                       ^^^^^^^^^^^^^^^^^

Error (6160): Wrong argument count for function call: 7 arguments given but expected 0.
  --> test/AccessControlTest.t.sol:17:17:
   |
17 |         token = new USDeXchangeToken(
   |                 ^ (Relevant source part starts here and spans across multiple lines).

Error (6160): Wrong argument count for function call: 0 arguments given but expected 1.
  --> test/EmergencyTest.t.sol:16:23:
   |
16 |         roleManager = new RoleManager();
   |                       ^^^^^^^^^^^^^^^^^

Error (6160): Wrong argument count for function call: 7 arguments given but expected 0.
  --> test/EmergencyTest.t.sol:17:17:
   |
17 |         token = new USDeXchangeToken(
   |                 ^ (Relevant source part starts here and spans across multiple lines).

Error (9582): Member "emergencyPause" not found or not visible after argument-dependent lookup in contract US
  --> test/EmergencyTest.t.sol:34:9:
   |
34 |         token.emergencyPause();
   |         ^^^^^^^^^^^^^^^^^^^^

Error: Compilation failed
```

Reentrancy Tests

```
Compiler run failed:
Error (6160): Wrong argument count for function call: 0 arguments given but expected 1.
  --> test/AccessControlTest.t.sol:16:23:
   |
16 |         roleManager = new RoleManager();
   |                       ^^^^^^^^^^^^^^^^^

Error (6160): Wrong argument count for function call: 7 arguments given but expected 0.
  --> test/AccessControlTest.t.sol:17:17:
   |
17 |         token = new USDeXchangeToken(
   |                 ^ (Relevant source part starts here and spans across multiple lines).

Error (6160): Wrong argument count for function call: 0 arguments given but expected 1.
  --> test/EmergencyTest.t.sol:16:23:
   |
16 |         roleManager = new RoleManager();
   |                       ^^^^^^^^^^^^^^^^^

Error (6160): Wrong argument count for function call: 7 arguments given but expected 0.
  --> test/EmergencyTest.t.sol:17:17:
   |
17 |         token = new USDeXchangeToken(
   |                 ^ (Relevant source part starts here and spans across multiple lines).

Error (9582): Member "emergencyPause" not found or not visible after argument-dependent lookup in contract US
  --> test/EmergencyTest.t.sol:34:9:
   |
34 |         token.emergencyPause();
   |         ^^^^^^^^^^^^^^^^^^^^

Error: Compilation failed
```

Access Control Tests

```
Compiler run failed:
Error (6160): Wrong argument count for function call: 0 arguments given but expected 1.
  --> test/AccessControlTest.t.sol:16:23:
   |
16 |         roleManager = new RoleManager();
   |                       ^^^^^^^^^^^^^^^^^

Error (6160): Wrong argument count for function call: 7 arguments given but expected 0.
  --> test/AccessControlTest.t.sol:17:17:
   |
17 |         token = new USDeXchangeToken(
   |                 ^ (Relevant source part starts here and spans across multiple lines).

Error (6160): Wrong argument count for function call: 0 arguments given but expected 1.
  --> test/EmergencyTest.t.sol:16:23:
   |
16 |         roleManager = new RoleManager();
   |                       ^^^^^^^^^^^^^^^^^

Error (6160): Wrong argument count for function call: 7 arguments given but expected 0.
  --> test/EmergencyTest.t.sol:17:17:
   |
17 |         token = new USDeXchangeToken(
   |                 ^ (Relevant source part starts here and spans across multiple lines).

Error (9582): Member "emergencyPause" not found or not visible after argument-dependent lookup in contract US
  --> test/EmergencyTest.t.sol:34:9:
   |
34 |         token.emergencyPause();
   |         ^^^^^^^^^^^^^^^^^^^^

Error: Compilation failed
```

Counter Tests

```
Compiler run failed:
Error (6160): Wrong argument count for function call: 0 arguments given but expected 1.
  --> test/AccessControlTest.t.sol:16:23:
   |
16 |         roleManager = new RoleManager();
   |                       ^^^^^^^^^^^^^^^^^

Error (6160): Wrong argument count for function call: 7 arguments given but expected 0.
  --> test/AccessControlTest.t.sol:17:17:
   |
17 |         token = new USDeXchangeToken(
   |                 ^ (Relevant source part starts here and spans across multiple lines).

Error (6160): Wrong argument count for function call: 0 arguments given but expected 1.
  --> test/EmergencyTest.t.sol:16:23:
   |
16 |         roleManager = new RoleManager();
   |                       ^^^^^^^^^^^^^^^^^

Error (6160): Wrong argument count for function call: 7 arguments given but expected 0.
  --> test/EmergencyTest.t.sol:17:17:
   |
17 |         token = new USDeXchangeToken(
   |                 ^ (Relevant source part starts here and spans across multiple lines).

Error (9582): Member "emergencyPause" not found or not visible after argument-dependent lookup in contract US
  --> test/EmergencyTest.t.sol:34:9:
   |
34 |         token.emergencyPause();
   |         ^^^^^^^^^^^^^^^^^^^^

Error: Compilation failed
```