1. Proxy.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/Proxy.sol

profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/Proxy.sol
/home/profganeshteam/Tools/FlattenedContracts/Proxy.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_LOCKED_MONEY
patternId: 30281d
severity: 3
line: 6
column: 0
content:
contractProxy{constructor(bytesmemoryconstructData,addresscontractLogic)public{assembly{sstore(0xc5f16f0fcc639fa48a6947836d9850f504798523bf8c9a3a87d5876cf622bcf7,contractLogic)}(boolsuccess,)=contractLogic.delegatecall(constructData);require(success,"Construction
failed");}function()externalpayable{assembly{letcontractLogic:=sload(0xc5f16f0fcc639fa48a6947836d9850f504798523bf8c9a3a87d5876cf622bcf7)calldatacopy(0x0,0x0,calldatasize)letsuccess:=delegatecall(sub(gas,10000),contractLogic,0x0,calldatasize,0,0)letretSz:=returndatasizereturndatacopy(0,0,retSz)switchsuccesscase0{revert(0,retSz)}default{return(0,retSz)}}}}

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: ^

ruleId: SOLIDITY_UNCHECKED_CALL
patternId: f39eed
severity: 3
line: 14
column: 61
content: delegatecall(constructData)

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 10
column: 8
content:
assembly{sstore(0xc5f16f0fcc639fa48a6947836d9850f504798523bf8c9a3a87d5876cf622bcf7,contractLogic)}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5

severity: 1

line: 19

column: 8

content:

assembly{letcontractLogic:=sload(0xc5f16f0fcc639fa48a6947836d9850f504798523bf8c9a3a87d5876cf622bcf7)calldatacopy(0x0,0x0,calldatasize)letsuccess:=delegatecall(sub(gas,10000),contractLogic,0x0,calldatasize,0,0)letretSz:=returndatasizereturndatacopy(0,0,retSz)switchsuccesscase0{revert(0,retSz)}default{return(0,retSz)}}

SOLIDITY_PRAGMAS_VERSION :1

SOLIDITY_LOCKED_MONEY :1

SOLIDITY_USING_INLINE_ASSEMBLY :2

SOLIDITY_UNCHECKED_CALL :1

2. RToken.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/RToken.sol

profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/RToken.sol

/home/profganeshteam/Tools/FlattenedContracts/RToken.sol

jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlline 249:27 extraneous input 'recipients' expecting {',', ')'}

line 249:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 250:26 mismatched input 'proportions' expecting {';', '='}

line 251:4 extraneous input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 251:15 extraneous input 'returns' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 251:29 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 306:27 extraneous input 'recipients' expecting {',', ')'}

line 307:26 extraneous input 'proportions' expecting {',', ')'}

line 307:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 309:4 mismatched input ')' expecting {';', '='}

line 309:32 extraneous input 'hatID' expecting ')'

line 309:38 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 984:24 extraneous input 'name_' expecting {',', ')'}

line 984:29 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 985:24 mismatched input 'symbol_' expecting {';', '='}
line 985:31 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 986:25 mismatched input ')' expecting {';', '='}
line 987:15 mismatched input '(' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 987:16 extraneous input '!' expecting {'solidity', 'experimental', 'from', '(', 'function', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'mapping', 'length', 'balance', 'string', 'bytes', 'emit', '_', 'revert', 'var', 'address', 'byte', 'bool', 'int', 'int8', 'int16', 'int24', 'int32', 'int40', 'int48', 'int56', 'int64', 'int72', 'int80', 'int88', 'int96', 'int104', 'int112', 'int120', 'int128', 'int136', 'int144', 'int152', 'int160', 'int168', 'int176', 'int184', 'int192', 'int200', 'int208', 'int216', 'int224', 'int232', 'int240', 'int248', 'int256', 'uint', 'uint8', 'uint16', 'uint24', 'uint32', 'uint40', 'uint48', 'uint56', 'uint64', 'uint72', 'uint80', 'uint88', 'uint96', 'uint104', 'uint112', 'uint120', 'uint128', 'uint136', 'uint144', 'uint152', 'uint160', 'uint168', 'uint176', 'uint184', 'uint192', 'uint200', 'uint208', 'uint216', 'uint224', 'uint232', 'uint240', 'uint248', 'uint256', 'bytes1', 'bytes2', 'bytes3', 'bytes4', 'bytes5', 'bytes6', 'bytes7', 'bytes8', 'bytes9', 'bytes10', 'bytes11', 'bytes12', 'bytes13', 'bytes14', 'bytes15', 'bytes16', 'bytes17', 'bytes18', 'bytes19', 'bytes20', 'bytes21', 'bytes22', 'bytes23', 'bytes24', 'bytes25', 'bytes26', 'bytes27', 'bytes28', 'bytes29', 'bytes30', 'bytes31', 'bytes32', 'fixed', 'fixed0x8', 'fixed0x16', 'fixed0x24', 'fixed0x32', 'fixed0x40', 'fixed0x48', 'fixed0x56', 'fixed0x64', 'fixed0x72', 'fixed0x80', 'fixed0x88', 'fixed0x96', 'fixed0x104', 'fixed0x112', 'fixed0x120', 'fixed0x128', 'fixed0x136', 'fixed0x144', 'fixed0x152', 'fixed0x160', 'fixed0x168', 'fixed0x176', 'fixed0x184', 'fixed0x192', 'fixed0x200', 'fixed0x208', 'fixed0x216', 'fixed0x224', 'fixed0x232', 'fixed0x240', 'fixed0x248', 'fixed0x256', 'fixed8x8', 'fixed8x16', 'fixed8x24', 'fixed8x32', 'fixed8x40', 'fixed8x48', 'fixed8x56', 'fixed8x64', 'fixed8x72', 'fixed8x80', 'fixed8x88', 'fixed8x96', 'fixed8x104', 'fixed8x112', 'fixed8x120', 'fixed8x128', 'fixed8x136', 'fixed8x144', 'fixed8x152', 'fixed8x160', 'fixed8x168', 'fixed8x176', 'fixed8x184', 'fixed8x192', 'fixed8x200', 'fixed8x208', 'fixed8x216', 'fixed8x224', 'fixed8x232', 'fixed8x240', 'fixed8x248', 'fixed16x8', 'fixed16x16', 'fixed16x24', 'fixed16x32', 'fixed16x40', 'fixed16x48', 'fixed16x56', 'fixed16x64', 'fixed16x72', 'fixed16x80', 'fixed16x88', 'fixed16x96', 'fixed16x104', 'fixed16x112', 'fixed16x120', 'fixed16x128', 'fixed16x136', 'fixed16x144', 'fixed16x152', 'fixed16x160', 'fixed16x168', 'fixed16x176', 'fixed16x184', 'fixed16x192', 'fixed16x200', 'fixed16x208', 'fixed16x216', 'fixed16x224', 'fixed16x232', 'fixed16x240', 'fixed24x8', 'fixed24x16', 'fixed24x24', 'fixed24x32', 'fixed24x40', 'fixed24x48', 'fixed24x56', 'fixed24x64', 'fixed24x72', 'fixed24x80', 'fixed24x88', 'fixed24x96', 'fixed24x104', 'fixed24x112', 'fixed24x120', 'fixed24x128', 'fixed24x136', 'fixed24x144', 'fixed24x152', 'fixed24x160', 'fixed24x168', 'fixed24x176', 'fixed24x184', 'fixed24x192', 'fixed24x200', 'fixed24x208', 'fixed24x216', 'fixed24x224', 'fixed24x232', 'fixed32x8', 'fixed32x16', 'fixed32x24', 'fixed32x32', 'fixed32x40', 'fixed32x48', 'fixed32x56', 'fixed32x64', 'fixed32x72', 'fixed32x80', 'fixed32x88', 'fixed32x96', 'fixed32x104', 'fixed32x112', 'fixed32x120', 'fixed32x128', 'fixed32x136', 'fixed32x144', 'fixed32x152', 'fixed32x160', 'fixed32x168', 'fixed32x176', 'fixed32x184', 'fixed32x192', 'fixed32x200', 'fixed32x208', 'fixed32x216', 'fixed32x224', 'fixed40x8', 'fixed40x16', 'fixed40x24', 'fixed40x32', 'fixed40x40', 'fixed40x48', 'fixed40x56', 'fixed40x64', 'fixed40x72', 'fixed40x80', 'fixed40x88', 'fixed40x96', 'fixed40x104', 'fixed40x112', 'fixed40x120', 'fixed40x128', 'fixed40x136', 'fixed40x144', 'fixed40x152', 'fixed40x160', 'fixed40x168',

'fixed40x176', 'fixed40x184', 'fixed40x192', 'fixed40x200', 'fixed40x208', 'fixed40x216', 'fixed48x8', 'fixed48x16', 'fixed48x24', 'fixed48x32', 'fixed48x40', 'fixed48x48', 'fixed48x56', 'fixed48x64', 'fixed48x72', 'fixed48x80', 'fixed48x88', 'fixed48x96', 'fixed48x104', 'fixed48x112', 'fixed48x120', 'fixed48x128', 'fixed48x136', 'fixed48x144', 'fixed48x152', 'fixed48x160', 'fixed48x168', 'fixed48x176', 'fixed48x184', 'fixed48x192', 'fixed48x200', 'fixed48x208', 'fixed56x8', 'fixed56x16', 'fixed56x24', 'fixed56x32', 'fixed56x40', 'fixed56x48', 'fixed56x56', 'fixed56x64', 'fixed56x72', 'fixed56x80', 'fixed56x88', 'fixed56x96', 'fixed56x104', 'fixed56x112', 'fixed56x120', 'fixed56x128', 'fixed56x136', 'fixed56x144', 'fixed56x152', 'fixed56x160', 'fixed56x168', 'fixed56x176', 'fixed56x184', 'fixed56x192', 'fixed56x200', 'fixed64x8', 'fixed64x16', 'fixed64x24', 'fixed64x32', 'fixed64x40', 'fixed64x48', 'fixed64x56', 'fixed64x64', 'fixed64x72', 'fixed64x80', 'fixed64x88', 'fixed64x96', 'fixed64x104', 'fixed64x112', 'fixed64x120', 'fixed64x128', 'fixed64x136', 'fixed64x144', 'fixed64x152', 'fixed64x160', 'fixed64x168', 'fixed64x176', 'fixed64x184', 'fixed64x192', 'fixed72x8', 'fixed72x16', 'fixed72x24', 'fixed72x32', 'fixed72x40', 'fixed72x48', 'fixed72x56', 'fixed72x64', 'fixed72x72', 'fixed72x80', 'fixed72x88',.....
vate', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 1004:38 mismatched input '(' expecting {';', '='}
line 1004:46 mismatched input '(' expecting ')'
line 1004:51 extraneous input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 1004:78 extraneous input ')' expecting {';', '='}
line 1014:4 extraneous input 'function' expecting {<EOF>, 'pragma', 'import', 'contract', 'library', 'interface'}
ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: b140cd
severity: 1
line: 976
column: 45
content: 0xFFFFFFFF

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: a91b18
severity: 1
line: 646
column: 8
content: _owner=address(0)

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1

line: 33
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 33
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 125
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 209
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 209
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 476
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 535
column: 16

content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 535
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 598
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 672
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 693
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 852
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 880
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 945
column: 17
content: ^

ruleId: SOLIDITY_SAFEMATH
patternId: 837cac
severity: 1
line: 969
column: 4
content: usingSafeMathforuint256;

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 350
column: 16
content: (uint256hatID,address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 365
column: 16
content: (address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 416
column: 16
content: (uint256rAmount,uint256sOriginalAmount)

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 17
column: 8
content:
assembly{sstore(0xc5f16f0fcc639fa48a6947836d9850f504798523bf8c9a3a87d5876cf622bcf7,newAddress)}

ruleId: SOLIDITY_VISIBILITY

patternId: 910067
severity: 1
line: 247
column: 4
content: functionmintWithNewHat(uint256mintAmount,address[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 305
column: 4
content: functioncreateHat(address[]calldatarecipients,uint32[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 982
column: 4
content: functioninitialize(IAllocationStrategyallocationStrategy,stringcalldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 249
column: 27
content: recipients,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 250
column: 8
content: uint32[]calldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 251
column: 23
content: (bool);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1

line: 307
column: 26
content: proportions,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 308
column: 8
content: booldoChangeHat)externalreturns

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 309
column: 23
content: (uint256hatID);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 984
column: 24
content: name_,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 985
column: 8
content: stringcalldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 985
column: 24
content: symbol_,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 986
column: 8

content: uint256decimals_)external{

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 987
column: 8
content: require

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 987
column: 15
content: (!initialized,"The library has already been initialized.");LibraryLock.

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 988
column: 20
content: initialize

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 988
column: 30
content: ();_owner=msg.sender;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 990
column: 8
content: _guardCounter=1;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 991
column: 8
content: name=name_;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 992
column: 8
content: symbol=symbol_;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 993
column: 8
content: decimals=decimals_;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 994
column: 8
content: savingAssetConversionRate=INITIAL_SAVING_ASSET_CONVERSION_RATE;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 995
column: 8
content: ias=allocationStrategy;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 996
column: 8
content: token=IERC20

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 996
column: 22
content: (ias.underlying());

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0

severity: 1
line: 999
column: 8
content: hats.push(Hat

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 999
column: 21
content: (newaddress[]<missing ';'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 999
column: 35
content: (0),new

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 999
column: 44
content: uint32[]

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 999
column: 52
content: (0)));

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1002
column: 8
content: hatStats[0].useCount=MAX_UINT256;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1004

column: 8
content: emitAllocationStrategyChanged

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1004
column: 38
content: (address<missing ';'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1004
column: 46
content: (ias),savingAssetConversionRate);

SOLIDITY_VISIBILITY :34
SOLIDITY_SAFEMATH :1
SOLIDITY_PRAGMAS_VERSION :15
SOLIDITY_ADDRESS_HARDCODED :2
SOLIDITY_USING_INLINE_ASSEMBLY :1
SOLIDITY_SHOULD_RETURN_STRUCT :3

3. MainframeStake.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/MainframeStake.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/MainframeStake.sol
/home/profganeshteam/Tools/FlattenedContracts/MainframeStake.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlline 379:27 extraneous input 'recipients' expecting {',', ')'}
line 379:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 380:26 mismatched input 'proportions' expecting {';', '='}
line 381:4 extraneous input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 381:15 extraneous input 'returns' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length',

'balance', 'emit', '_', 'revert', Identifier}
line 381:29 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 436:27 extraneous input 'recipients' expecting {',', ')'}
line 437:26 extraneous input 'proportions' expecting {',', ')'}
line 437:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 439:4 mismatched input ')' expecting {';', '='}
line 439:32 extraneous input 'hatID' expecting ')'
line 439:38 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 820:57 extraneous input 'payable' expecting {',', ')'}
line 1083:10 extraneous input 'payable' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 1181:45 extraneous input 'addresses' expecting {',', ')'}
ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: a91b18
severity: 1
line: 776
column: 8
content: _owner=address(0)

ruleId: SOLIDITY_ERC20_APPROVE
patternId: af782c
severity: 2
line: 908
column: 4
content:
functionapprove(addressspender,uint256amount)publicreturns(bool){_approve(_msgSender(),spender,amount);returntrue;}

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: d3j11j
severity: 1
line: 1183
column: 4

content:
for(uint256i=0;i<addresses.length;i++){address_address=addresses[i];require(balances[_address]>0);token.transfer(_address,balances[_address]);totalDepositBalance=totalDepositBalance.sub(balances[_address]);emitRefundedBalance(_address,balances[_address]);balances[_address]=0;}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 1183
column: 4
content:
for(uint256i=0;i<addresses.length;i++){address_address=addresses[i];require(balances[_address]>0);token.transfer(_address,balances[_address]);totalDepositBalance=totalDepositBalance.sub(balances[_address]);emitRefundedBalance(_address,balances[_address]);balances[_address]=0;}

ruleId: SOLIDITY_OVERPOWERED_ROLE
patternId: j83hf7
severity: 2
line: 1173
column: 2
content: functionsetRequiredStake(uint256value)externalonlyOwner{requiredStake=value;}

ruleId: SOLIDITY_OVERPOWERED_ROLE
patternId: j83hf7
severity: 2
line: 1177
column: 2
content: functionsetArrayLimit(uint256newLimit)externalonlyOwner{arrayLimit=newLimit;}

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 163
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION

patternId: 23fc32
severity: 1
line: 163
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 255
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 339
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 339
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 606
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 665
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1

line: 665
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 728
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 802
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 832
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 1061
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 1069
column: 16
content: ^

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 861
column: 33

content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 863
column: 54
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 865
column: 12
content: private

ruleId: SOLIDITY_SAFEMATH
patternId: 837cac
severity: 1
line: 859
column: 4
content: usingSafeMathforuint256;

ruleId: SOLIDITY_SAFEMATH
patternId: 837cac
severity: 1
line: 1076
column: 2
content: usingSafeMathforuint256;

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 480
column: 16
content: (uint256hatID,address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 495
column: 16
content: (address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 546
column: 16
content: (uint256rAmount,uint256sOriginalAmount)

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 377
column: 4
content: functionmintWithNewHat(uint256mintAmount,address[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 435
column: 4
content: functioncreateHat(address[]calldatarecipients,uint32[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 379
column: 27
content: recipients,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 380
column: 8
content: uint32[]calldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 381
column: 23
content: (bool);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0

severity: 1
line: 437
column: 26
content: proportions,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 438
column: 8
content: booldoChangeHat)externalreturns

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 439
column: 23
content: (uint256hatID);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1078
column: 2
content: ERC20token;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1083
column: 2
content: addresspayable_owner;

SOLIDITY_VISIBILITY :10
SOLIDITY_SAFEMATH :2
SOLIDITY_OVERPOWERED_ROLE :2
SOLIDITY_PRAGMAS_VERSION :14
SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA :3
SOLIDITY_EXTRA_GAS_IN_LOOPS :1
SOLIDITY_ADDRESS_HARDCODED :1
SOLIDITY_GAS_LIMIT_IN_LOOPS :1
SOLIDITY_SHOULD_RETURN_STRUCT :3
SOLIDITY_ERC20_APPROVE :1

4. tokensalechallenge.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/tokensalechallenge.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/tokensalechallenge.sol
/home/profganeshteam/Tools/FlattenedContracts/tokensalechallenge.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 9
column: 16
content: ^

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 13
column: 4
content: uint256constantPRICE_PER_TOKEN=1ether;

SOLIDITY_VISIBILITY :1
SOLIDITY_PRAGMAS_VERSION :1

5. StakeInterface.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/StakeInterface.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/StakeInterface.sol
/home/profganeshteam/Tools/FlattenedContracts/StakeInterface.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: ^

SOLIDITY_PRAGMAS_VERSION :1

6. RTokenStructs.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/RTokenStructs.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/RTokenStructs.sol

/home/profganeshteam/Tools/FlattenedContracts/RTokenStructs.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 25
content: <

SOLIDITY_PRAGMAS_VERSION :2

7. RTokenStorage.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/RTokenStorage.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/RTokenStorage.sol
/home/profganeshteam/Tools/FlattenedContracts/RTokenStorage.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlline 220:27 extraneous input 'recipients' expecting {',', ')'}
line 220:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 221:26 mismatched input 'proportions' expecting {';', '='}
line 222:4 extraneous input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 222:15 extraneous input 'returns' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 222:29 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 277:27 extraneous input 'recipients' expecting {',', ')'}

line 278:26 extraneous input 'proportions' expecting {',', ')'}
line 278:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 280:4 mismatched input ')' expecting {';', '='}
line 280:32 extraneous input 'hatID' expecting ')'
line 280:38 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 96
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 180
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 180
column: 25

content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 447
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 506
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 506
column: 25
content: <

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 321
column: 16
content: (uint256hatID,address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 336
column: 16
content: (address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 387
column: 16
content: (uint256rAmount,uint256sOriginalAmount)

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 218
column: 4
content: functionmintWithNewHat(uint256mintAmount,address[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 276
column: 4
content: functioncreateHat(address[]calldatarecipients,uint32[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 220
column: 27
content: recipients,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 221
column: 8
content: uint32[]calldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 222
column: 23
content: (bool);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 278
column: 26
content: proportions,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0

severity: 1
line: 279
column: 8
content: booldoChangeHat)externalreturns

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 280
column: 23
content: (uint256hatID);

SOLIDITY_VISIBILITY :8
SOLIDITY_PRAGMAS_VERSION :8
SOLIDITY_SHOULD_RETURN_STRUCT :3

8. ReentrancyGuard.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/ReentrancyGuard.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/ReentrancyGuard.sol
/home/profganeshteam/Tools/FlattenedContracts/ReentrancyGuard.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlline 220:27 extraneous input 'recipients' expecting {',', ')'}
line 220:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 221:26 mismatched input 'proportions' expecting {';', '='}
line 222:4 extraneous input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 222:15 extraneous input 'returns' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 222:29 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 277:27 extraneous input 'recipients' expecting {',', ')'}
line 278:26 extraneous input 'proportions' expecting {',', ')'}
line 278:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block',

'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 280:4 mismatched input ')' expecting {';', '='}
line 280:32 extraneous input 'hatID' expecting ')'
line 280:38 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 96
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 180
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 180
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 447
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 506
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 506
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 569
column: 16
content: ^

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 321
column: 16
content: (uint256hatID,address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 336
column: 16
content: (address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l

severity: 1
line: 387
column: 16
content: (uint256rAmount,uint256sOriginalAmount)

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 218
column: 4
content: functionmintWithNewHat(uint256mintAmount,address[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 276
column: 4
content: functioncreateHat(address[]calldatarecipients,uint32[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 220
column: 27
content: recipients,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 221
column: 8
content: uint32[]calldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 222
column: 23
content: (bool);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 278

column: 26
content: proportions,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 279
column: 8
content: booldoChangeHat)externalreturns

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 280
column: 23
content: (uint256hatID);

SOLIDITY_VISIBILITY :8
SOLIDITY_PRAGMAS_VERSION :9
SOLIDITY_SHOULD_RETURN_STRUCT :3

9. Proxiable.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/Proxiable.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/Proxiable.sol /home/profganeshteam/Tools/FlattenedContracts/Proxiable.sol jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: ^

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 17
column: 8
content:
assembly{sstore(0xc5f16f0fcc639fa48a6947836d9850f504798523bf8c9a3a87d5876cf622bcf7,newAddress)}

SOLIDITY_PRAGMAS_VERSION :1
SOLIDITY_USING_INLINE_ASSEMBLY :1

10. Ownable.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/Ownable.sol

profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/Ownable.sol

/home/profganeshteam/Tools/FlattenedContracts/Ownable.sol

jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlline 220:27 extraneous input 'recipients' expecting {',', ')'}

line 220:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 221:26 mismatched input 'proportions' expecting {';', '='}

line 222:4 extraneous input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 222:15 extraneous input 'returns' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 222:29 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 277:27 extraneous input 'recipients' expecting {',', ')'}

line 278:26 extraneous input 'proportions' expecting {',', ')'}

line 278:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 280:4 mismatched input ')' expecting {';', '='}

line 280:32 extraneous input 'hatID' expecting ')'

line 280:38 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

ruleId: SOLIDITY_ADDRESS_HARDCODED

patternId: a91b18

severity: 1

line: 617

column: 8

content: _owner=address(0)

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 96
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 180
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 180
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 447
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 506
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 506
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 569
column: 16
content: ^

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 321
column: 16
content: (uint256hatID,address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 336
column: 16
content: (address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 387
column: 16
content: (uint256rAmount,uint256sOriginalAmount)

ruleId: SOLIDITY_VISIBILITY
patternId: 910067

severity: 1
line: 218
column: 4
content: functionmintWithNewHat(uint256mintAmount,address[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 276
column: 4
content: functioncreateHat(address[]calldatarecipients,uint32[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 220
column: 27
content: recipients,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 221
column: 8
content: uint32[]calldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 222
column: 23
content: (bool);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 278
column: 26
content: proportions,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 279

column: 8
content: booldoChangeHat)externalreturns

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 280
column: 23
content: (uint256hatID);

SOLIDITY_VISIBILITY :8
SOLIDITY_PRAGMAS_VERSION :9
SOLIDITY_ADDRESS_HARDCODED :1
SOLIDITY_SHOULD_RETURN_STRUCT :3

11. modifier_reentrancy.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/modifier_reentrancy.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/modifier_reentrancy.sol
/home/profganeshteam/Tools/FlattenedContracts/modifier_reentrancy.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: ^

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 8
column: 2
content: stringconstantname="Nu Token";

SOLIDITY_VISIBILITY :1
SOLIDITY_PRAGMAS_VERSION :1

12. MainframeTokenDistribution.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/MainframeTokenDistribution.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/MainframeTokenDistribution.sol

/home/profganeshteam/Tools/FlattenedContracts/MainframeTokenDistribution.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlline 220:27 extraneous input 'recipients' expecting {',', ')'}
line 220:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 221:26 mismatched input 'proportions' expecting {';', '='}
line 222:4 extraneous input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 222:15 extraneous input 'returns' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 222:29 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 277:27 extraneous input 'recipients' expecting {',', ')'}
line 278:26 extraneous input 'proportions' expecting {',', ')'}
line 278:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 280:4 mismatched input ')' expecting {';', '='}
line 280:32 extraneous input 'hatID' expecting ')'
line 280:38 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 661:57 extraneous input 'payable' expecting {',', ')'}
ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: a91b18
severity: 1
line: 617
column: 8
content: _owner=address(0)

ruleId: SOLIDITY_ERC20_APPROVE
patternId: af782c
severity: 2
line: 908
column: 4
content:
functionapprove(addressspender,uint256amount)publicreturns(bool){_approve(_msgSender(),spender,amount);returntrue;}

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS

patternId: d3j11j
severity: 1
line: 1078
column: 4
content:
for(uinti=0;i<recipients.length;i++){if(values[i]>0){require(mainframeToken.transferFrom(tokenOwner,recipients[i],values[i]));emitTokensDistributed(recipients[i],values[i]);totalDistributed+=values[i];}}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 1078
column: 4
content:
for(uinti=0;i<recipients.length;i++){if(values[i]>0){require(mainframeToken.transferFrom(tokenOwner,recipients[i],values[i]));emitTokensDistributed(recipients[i],values[i]);totalDistributed+=values[i];}}

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 96
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 180
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 180
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 447
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 506
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 506
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 569
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 643
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION

patternId: 23fc32
severity: 1
line: 673
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 832
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 1061
column: 16
content: ^

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 861
column: 33
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 863
column: 54
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 865
column: 12
content: private

ruleId: SOLIDITY_SAFEMATH
patternId: 837cac
severity: 1

line: 859
column: 4
content: usingSafeMathforuint256;

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 321
column: 16
content: (uint256hatID,address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 336
column: 16
content: (address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 387
column: 16
content: (uint256rAmount,uint256sOriginalAmount)

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 218
column: 4
content: functionmintWithNewHat(uint256mintAmount,address[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 276
column: 4
content: functioncreateHat(address[]calldatarecipients,uint32[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 220
column: 27

content: recipients,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 221
column: 8
content: uint32[]calldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 222
column: 23
content: (bool);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 278
column: 26
content: proportions,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 279
column: 8
content: booldoChangeHat)externalreturns

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 280
column: 23
content: (uint256hatID);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1068
column: 2
content: ERC20mainframeToken;

SOLIDITY_VISIBILITY :9
SOLIDITY_SAFEMATH :1
SOLIDITY_PRAGMAS_VERSION :13
SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA :3
SOLIDITY_EXTRA_GAS_IN_LOOPS :1
SOLIDITY_ADDRESS_HARDCODED :1
SOLIDITY_GAS_LIMIT_IN_LOOPS :1
SOLIDITY_SHOULD_RETURN_STRUCT :3
SOLIDITY_ERC20_APPROVE :1

13. MainframeToken.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/MainframeToken.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/MainframeToken.sol
/home/profganeshteam/Tools/FlattenedContracts/MainframeToken.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlline 22:57 extraneous input 'payable' expecting {',', ')'}
line 943:27 extraneous input 'recipients' expecting {',', ')'}
line 943:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 944:26 mismatched input 'proportions' expecting {';', '='}
line 945:4 extraneous input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 945:15 extraneous input 'returns' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 945:29 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 1000:27 extraneous input 'recipients' expecting {',', ')'}
line 1001:26 extraneous input 'proportions' expecting {',', ')'}
line 1001:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 1003:4 mismatched input ')' expecting {';', '='}
line 1003:32 extraneous input 'hatID' expecting ')'

line 1003:38 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: a91b18
severity: 1
line: 1340
column: 8
content: _owner=address(0)

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: c67a09
severity: 1
line: 1388
column: 19
content: 0x0

ruleId: SOLIDITY_DEPRECATED_CONSTRUCTIONS
patternId: 28fa69
severity: 1
line: 578
column: 2
content:
functionbalanceOf(TokenStoragestorageself,address_owner)constantreturns(uintbalance){returnself.balances[_owner];}

ruleId: SOLIDITY_DEPRECATED_CONSTRUCTIONS
patternId: 28fa69
severity: 1
line: 588
column: 2
content:
functionallowance(TokenStoragestorageself,address_owner,address_spender)constantreturns(uintremaining){returnself.allowed[_owner][_spender];}

ruleId: SOLIDITY_DEPRECATED_CONSTRUCTIONS
patternId: 28fa69
severity: 1
line: 619
column: 3
content: functiontotalSupply()constantreturns(uint){returntoken.totalSupply;}

ruleId: SOLIDITY_DEPRECATED_CONSTRUCTIONS

patternId: 28fa69
severity: 1
line: 623
column: 3
content: functionbalanceOf(addresswho)constantreturns(uint){returntoken.balanceOf(who);}

ruleId: SOLIDITY_DEPRECATED_CONSTRUCTIONS
patternId: 28fa69
severity: 1
line: 627
column: 3
content:
functionallowance(addressowner,addressspender)constantreturns(uint){returntoken.allowance(owner,sp
ender);}

ruleId: SOLIDITY_ERC20_APPROVE
patternId: af782c
severity: 2
line: 348
column: 4
content:
functionapprove(addressspender,uint256amount)publicreturns(bool){_approve(_msgSender(),spender,a
mount);returntrue;}

ruleId: SOLIDITY_ERC20_APPROVE
patternId: af782c
severity: 2
line: 639
column: 3
content:
functionapprove(addressspender,uintvalue)returns(boolok){returntoken.approve(spender,value);}

ruleId: SOLIDITY_ERC20_APPROVE
patternId: af782c
severity: 2
line: 1439
column: 2
content:
functionapprove(addressspender,uint256value)publicisTradeablereturns(bool){returnsuper.approve(spe
nder,value);}

ruleId: SOLIDITY_OVERPOWERED_ROLE
patternId: j83hf7
severity: 2

line: 1453
column: 2
content:
functionsetDistributor(addressnewDistributor)externalonlyOwner{distributor=newDistributor;}

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 34
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 113
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 272
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 507
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 542

column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 595
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 649
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 688
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 732
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 806
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 806
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 903
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 903
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 1170
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 1229
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 1229
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 1292
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION

patternId: 23fc32
severity: 1
line: 1366
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 1395
column: 16
content: ^

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 301
column: 33
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 303
column: 54
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 305
column: 12
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 696
column: 15
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1

line: 754
column: 9
content: private

ruleId: SOLIDITY_SAFEMATH
patternId: 837cac
severity: 1
line: 299
column: 4
content: usingSafeMathforuint256;

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 1044
column: 16
content: (uint256hatID,address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 1059
column: 16
content: (address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 1110
column: 16
content: (uint256rAmount,uint256sOriginalAmount)

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 521
column: 2
content: functiontimes(uinta,uintb)returns(uint){uintc=a*b;assert(a==0||c/a==b);returnc;}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 527
column: 2

content: functionminus(uinta,uintb)returns(uint){assert(b<=a);returna-b;}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 532
column: 2
content: functionplus(uinta,uintb)returns(uint){uintc=a+b;assert(c>=a);returnc;}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 556
column: 2
content:
functioninit(TokenStoragestorageself,uint_initial_supply){self.totalSupply=_initial_supply;self.balance
s[msg.sender]=_initial_supply;}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 561
column: 2
content:
functiontransfer(TokenStoragestorageself,address_to,uint_value)returns(boolsuccess){self.balances[ms
g.sender]=self.balances[msg.sender].minus(_value);self.balances[_to]=self.balances[_to].plus(_value);
Transfer(msg.sender,_to,_value);returntrue;}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 568
column: 2
content:
functiontransferFrom(TokenStoragestorageself,address_from,address_to,uint_value)returns(boolsucces
s){var_allowance=self.allowed[_from][msg.sender];self.balances[_to]=self.balances[_to].plus(_value);
self.balances[_from]=self.balances[_from].minus(_value);self.allowed[_from][msg.sender]=_allowanc
e.minus(_value);Transfer(_from,_to,_value);returntrue;}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 578
column: 2

content:
functionbalanceOf(TokenStoragestorageself,address_owner)constantreturns(uintbalance){returnself.balances[_owner];}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 582
column: 2
content:
functionapprove(TokenStoragestorageself,address_spender,uint_value)returns(boolsuccess){self.allowed[msg.sender][_spender]=_value;Approval(msg.sender,_spender,_value);returntrue;}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 588
column: 2
content:
functionallowance(TokenStoragestorageself,address_owner,address_spender)constantreturns(uintremaining){returnself.allowed[_owner][_spender];}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 615
column: 3
content: functionStandardToken(){token.init(INITIAL_SUPPLY);}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 619
column: 3
content: functiontotalSupply()constantreturns(uint){returntoken.totalSupply;}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 623
column: 3
content: functionbalanceOf(addresswho)constantreturns(uint){returntoken.balanceOf(who);}

ruleId: SOLIDITY_VISIBILITY

patternId: 910067
severity: 1
line: 627
column: 3
content:
functionallowance(addressowner,addressspender)constantreturns(uint){returntoken.allowance(owner,sp
ender);}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 631
column: 3
content: functiontransfer(addressto,uintvalue)returns(boolok){returntoken.transfer(to,value);}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 635
column: 3
content:
functiontransferFrom(addressfrom,addressto,uintvalue)returns(boolok){returntoken.transferFrom(from,
to,value);}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 639
column: 3
content:
functionapprove(addressspender,uintvalue)returns(boolok){returntoken.approve(spender,value);}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 941
column: 4
content: functionmintWithNewHat(uint256mintAmount,address[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 999
column: 4

content: functioncreateHat(address[]calldatarecipients,uint32[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 1382
column: 2
content: functiontransferOwnership(addressnewOwner)onlyOwner{pendingOwner=newOwner;}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 1386
column: 2
content: functionclaimOwnership()onlyPendingOwner{owner=pendingOwner;pendingOwner=0x0;}

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 608
column: 3
content: ERC20Lib.TokenStoragetoken;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 943
column: 27
content: recipients,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 944
column: 8
content: uint32[]calldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 945
column: 23
content: (bool);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1001
column: 26
content: proportions,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1002
column: 8
content: booldoChangeHat)externalreturns

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1003
column: 23
content: (uint256hatID);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1406
column: 2
content: uinttotalSupply_;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1407
column: 2
content: mapping(address=>uint256)balances;

SOLIDITY_VISIBILITY :29
SOLIDITY_SAFEMATH :1
SOLIDITY_OVERPOWERED_ROLE :1
SOLIDITY_DEPRECATED_CONSTRUCTIONS :5
SOLIDITY_PRAGMAS_VERSION :20
SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA :5
SOLIDITY_ADDRESS_HARDCODED :2
SOLIDITY_SHOULD_RETURN_STRUCT :3
SOLIDITY_ERC20_APPROVE :3

14. Lockdrop.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/Lockdrop.sol

profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/Lockdrop.sol

/home/profganeshteam/Tools/FlattenedContracts/Lockdrop.sol

jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlline 56:44 extraneous input 'edgewareAddr' expecting {',', ')'}

line 56:56 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 56:74 mismatched input ')' expecting {';', '='}

line 61:4 mismatched input '{' expecting {';', '='}

line 68:14 mismatched input '(' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 68:22 mismatched input '(' expecting ')'

line 68:32 extraneous input '.' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 68:41 mismatched input '==' expecting {';', '='}

line 68:53 mismatched input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 69:19 mismatched input '(' expecting {';', '='}

line 69:25 mismatched input ',' expecting ')'

line 69:30 mismatched input ',' expecting {';', '='}

line 69:40 extraneous input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 69:46 mismatched input ',' expecting {';', '='}

line 69:60 extraneous input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 69:73 mismatched input ',' expecting {';', '='}

line 69:78 mismatched input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig',

'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 78:4 extraneous input 'function' expecting {<EOF>, 'pragma', 'import', 'contract', 'library', 'interface'}
ruleId: SOLIDITY_LOCKED_MONEY
patternId: 30281d
severity: 3
line: 6
column: 0
content:
contractLock{constructor(addressowner,uint256unlockTime)publicpayable{assembly{sstore(0x00,owner)sstore(0x01,unlockTime)}}function()externalpayable{assembly{switchgt(timestamp,sload(0x01))case0{revert(0,0)}case1{switchcall(gas,sload(0x00),balance(address),0,0,0,0)case0{revert(0,0)}}}}}

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: ^

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 10
column: 8
content: assembly{sstore(0x00,owner)sstore(0x01,unlockTime)}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 20
column: 8
content:
assembly{switchgt(timestamp,sload(0x01))case0{revert(0,0)}case1{switchcall(gas,sload(0x00),balance(address),0,0,0,0)case0{revert(0,0)}}}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 56
column: 4
content: functionlock(Termterm,bytescalldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 56
column: 44
content: edgewareAddr,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 56
column: 58
content: boolisValidator)externalpayable

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 59
column: 8
content: didStartdidNotEnd{

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 62
column: 8
content: uint256eth=msg.value;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 63
column: 8
content: addressowner=msg.sender;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 64
column: 8
content: uint256unlockTime=unlockTimeForTerm(term);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0

severity: 1
line: 66
column: 8
content: LocklockAddr=(newLock).value(eth)(owner,unlockTime);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 68
column: 8
content: assert

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 68
column: 14
content: (address<missing ';'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 68
column: 22
content: (lockAddr).balance==

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 68
column: 44
content: msg.value);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 69
column: 8
content: emitLocked

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 69

column: 19
content: (owner,eth,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 69
column: 32
content: lockAddr,term,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 69
column: 48
content: edgewareAddr,isValidator,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 69
column: 75
content: now);

SOLIDITY_VISIBILITY :17
SOLIDITY_PRAGMAS_VERSION :1
SOLIDITY_LOCKED_MONEY :1
SOLIDITY_USING_INLINE_ASSEMBLY :2

15. LibraryLock.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/LibraryLock.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/LibraryLock.sol
/home/profganeshteam/Tools/FlattenedContracts/LibraryLock.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlline 220:27 extraneous input 'recipients' expecting {',', ')'}
line 220:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 221:26 mismatched input 'proportions' expecting {';', '='}
line 222:4 extraneous input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig',

'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 222:15 extraneous input 'returns' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 222:29 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 277:27 extraneous input 'recipients' expecting {',', ')'}
line 278:26 extraneous input 'proportions' expecting {',', ')'}
line 278:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 280:4 mismatched input ')' expecting {';', '='}
line 280:32 extraneous input 'hatID' expecting ')'
line 280:38 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 96
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION

patternId: 23fc32
severity: 1
line: 180
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 180
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 447
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 506
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 506
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 569
column: 16
content: ^

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1

line: 321
column: 16
content: (uint256hatID,address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 336
column: 16
content: (address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 387
column: 16
content: (uint256rAmount,uint256sOriginalAmount)

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 218
column: 4
content: functionmintWithNewHat(uint256mintAmount,address[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 276
column: 4
content: functioncreateHat(address[]calldatarecipients,uint32[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 220
column: 27
content: recipients,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 221
column: 8

content: uint32[]calldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 222
column: 23
content: (bool);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 278
column: 26
content: proportions,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 279
column: 8
content: booldoChangeHat)externalreturns

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 280
column: 23
content: (uint256hatID);

SOLIDITY_VISIBILITY :8
SOLIDITY_PRAGMAS_VERSION :9
SOLIDITY_SHOULD_RETURN_STRUCT :3

16. IRTokenAdmin.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/IRTokenAdmin.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/IRTokenAdmin.sol
/home/profganeshteam/Tools/FlattenedContracts/IRTokenAdmin.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1

line: 8
column: 16
content: >=

SOLIDITY_PRAGMAS_VERSION :1

17. IRToken.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/IRToken.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/IRTokenAdmin.sol /home/profganeshteam/Tools/FlattenedContracts/IRTokenAdmin.sol jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 8
column: 16
content: >=

SOLIDITY_PRAGMAS_VERSION :1
profganeshteam@SmartContract:~$ ^C
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/IRToken.sol /home/profganeshteam/Tools/FlattenedContracts/IRToken.sol jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlline 220:27 extraneous input 'recipients' expecting {',', ')'}
line 220:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 221:26 mismatched input 'proportions' expecting {';', '='}
line 222:4 extraneous input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 222:15 extraneous input 'returns' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 222:29 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}

line 277:27 extraneous input 'recipients' expecting {',', ')'}
line 278:26 extraneous input 'proportions' expecting {',', ')'}
line 278:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 280:4 mismatched input ')' expecting {';', '='}
line 280:32 extraneous input 'hatID' expecting ')'
line 280:38 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 96
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 180
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 180

column: 25
content: <

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 321
column: 16
content: (uint256hatID,address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 336
column: 16
content: (address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 387
column: 16
content: (uint256rAmount,uint256sOriginalAmount)

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 218
column: 4
content: functionmintWithNewHat(uint256mintAmount,address[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 276
column: 4
content: functioncreateHat(address[]calldatarecipients,uint32[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 220
column: 27
content: recipients,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 221
column: 8
content: uint32[]calldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 222
column: 23
content: (bool);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 278
column: 26
content: proportions,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 279
column: 8
content: booldoChangeHat)externalreturns

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 280
column: 23
content: (uint256hatID);

SOLIDITY_VISIBILITY :8
SOLIDITY_PRAGMAS_VERSION :5
SOLIDITY_SHOULD_RETURN_STRUCT :3

18. IAllocationStrategy.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/IAllocationStrategy.sol
profganeshteam@SmartContract:~$ smartcheck -p

/home/profganeshteam/Tools/FlattenedContracts/IAllocationStrategy.sol
/home/profganeshteam/Tools/FlattenedContracts/IAllocationStrategy.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: ^

SOLIDITY_PRAGMAS_VERSION :1

19. guess_the_random_number.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/guess_the_random_number.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/guess_the_random_number.sol
/home/profganeshteam/Tools/FlattenedContracts/guess_the_random_number.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_BALANCE_EQUALITY
patternId: 5094ad
severity: 1
line: 20
column: 15
content: address(this).balance==0

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 9
column: 16
content: ^

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 12
column: 4
content: uintanswer;

SOLIDITY_VISIBILITY :1
SOLIDITY_PRAGMAS_VERSION :1

SOLIDITY_BALANCE_EQUALITY :1

20. dos_simple.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/dos_simple.sol

profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/dos_simple.sol
/home/profganeshteam/Tools/FlattenedContracts/dos_simple.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: ^

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 8
column: 4
content: address[]listAddresses;

SOLIDITY_VISIBILITY :1
SOLIDITY_PRAGMAS_VERSION :1

21. dos_number.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/dos_number.sol

profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlatenedContracts/dos_number.sol
/home/profganeshteam/Tools/FlattenedContracts/dos_number.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartchec-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_ARRAY_LENTH_MANIPULATION
patternId: 872bdd
severity: 1
line: 16
column: 16
content: array.length+=1

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4

column: 16
content: ^

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 8
column: 4
content: uintnumElements=0;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 9
column: 4
content: uint[]array;

SOLIDITY_VISIBILITY :2
SOLIDITY_PRAGMAS_VERSION :1
SOLIDITY_ARRAY_LENGTH_MANIPULATION :1

22. dos_address.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/dos_address.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/dos_address.sol
/home/profganeshteam/Tools/FlattenedContracts/dos_address.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: ^

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 8
column: 4
content: address[]creditorAddresses;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0

severity: 1
line: 9
column: 4
content: boolwin=false;

SOLIDITY_VISIBILITY :2
SOLIDITY_PRAGMAS_VERSION :1

23. CompoundAllocationStrategy.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/CompoundAllocationStrategy.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/CompoundAllocationStrategy.sol /home/profganeshteam/Tools/FlattenedContracts/CompoundAllocationStrategy.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlline 274:27 extraneous input 'recipients' expecting {',', ')'}
line 274:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 275:26 mismatched input 'proportions' expecting {';', '='}
line 276:4 extraneous input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 276:15 extraneous input 'returns' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 276:29 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 331:27 extraneous input 'recipients' expecting {',', ')'}
line 332:26 extraneous input 'proportions' expecting {',', ')'}
line 332:37 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 334:4 mismatched input ')' expecting {';', '='}
line 334:32 extraneous input 'hatID' expecting ')'
line 334:38 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length',

'balance', 'emit', '_', 'revert', Identifier}
ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: a91b18
severity: 1
line: 617
column: 8
content: _owner=address(0)

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 58
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 58
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 150
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 234
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION

patternId: 23fc32
severity: 1
line: 234
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 506
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 506
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 569
column: 16
content: ^

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 643
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 643
column: 25
content: <

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1

line: 995
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 995
column: 25
content: <

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 1003
column: 20
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 1004
column: 11
content: private

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 375
column: 16
content: (uint256hatID,address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 390
column: 16
content: (address[]memoryrecipients,uint32[]memoryproportions)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 441
column: 16

content: (uint256rAmount,uint256sOriginalAmount)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 823
column: 28
content: (uint256,uint256,uint256,uint256)

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 272
column: 4
content: functionmintWithNewHat(uint256mintAmount,address[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 330
column: 4
content: functioncreateHat(address[]calldatarecipients,uint32[]calldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 274
column: 27
content: recipients,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 275
column: 8
content: uint32[]calldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 276
column: 23
content: (bool);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 332
column: 26
content: proportions,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 333
column: 8
content: booldoChangeHat)externalreturns

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 334
column: 23
content: (uint256hatID);

SOLIDITY_VISIBILITY :8
SOLIDITY_PRAGMAS_VERSION :13
SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA :2
SOLIDITY_ADDRESS_HARDCODED :1
SOLIDITY_SHOULD_RETURN_STRUCT :4

24. Casino.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/Casino.sol
profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/Casino.sol
/home/profganeshteam/Tools/FlattenedContracts/Casino.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlline 28:136 extraneous input 'x' expecting {',', ')'}
line 41:52 extraneous input '_datasource' expecting {',', ')'}
line 41:63 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 41:81 mismatched input '_arg' expecting {';', '='}
line 41:85 extraneous input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length',

'balance', 'emit', '_', 'revert', Identifier}
line 41:96 extraneous input 'payable' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 41:121 extraneous input '_id' expecting ')'
line 41:125 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 43:65 extraneous input '_datasource' expecting {',', ')'}
line 43:76 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 43:94 mismatched input '_arg' expecting {';', '='}
line 43:98 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 43:114 mismatched input ')' expecting {';', '='}
line 43:150 extraneous input '_id' expecting ')'
line 43:154 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 44:66 extraneous input '_datasource' expecting {',', ')'}
line 44:77 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 44:94 mismatched input '_argN' expecting {';', '='}
line 44:99 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 44:115 mismatched input ')' expecting {';', '='}
line 44:151 extraneous input '_id' expecting ')'
line 44:155 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 45:66 extraneous input '_datasource' expecting {',', ')'}
line 45:77 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block',

'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 45:95 mismatched input '_arg1' expecting {';', '='}
line 45:100 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 45:118 mismatched input '_arg2' expecting {';', '='}
line 45:123 mismatched input ',' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 45:139 mismatched input ')' expecting {';', '='}
line 45:175 extraneous input '_id' expecting ')'
line 45:179 mismatched input ';' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
line 1344:27 mismatched input 'payable' expecting ')'
line 1344:37 extraneous input ')' expecting {'solidity', 'experimental', 'from', 'constructor', 'block', 'coinbase', 'difficulty', 'gaslimit', 'number', 'timestamp', 'blockhash', 'msg', 'data', 'gas', 'sender', 'sig', 'value', 'now', 'this', 'tx', 'origin', 'gasprice', 'public', 'internal', 'external', 'private', 'constant', 'length', 'balance', 'emit', '_', 'revert', Identifier}
ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: adc165
severity: 1
line: 319
column: 24
content: 0xC63A9D291B9496638bCa8550c34CBA82B3d94aE4

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: adc165
severity: 1
line: 320
column: 40
content: 0xC63A9D291B9496638bCa8550c34CBA82B3d94aE4

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: adc165
severity: 1
line: 324
column: 24
content: 0x77AF3146DaAa33e9F4610A7057d489DC27f025aD

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: adc165
severity: 1
line: 325
column: 40
content: 0x77AF3146DaAa33e9F4610A7057d489DC27f025aD

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: adc165
severity: 1
line: 329
column: 24
content: 0x6f485C8BF6fc43eA212E93BBF8ce046C7f1cb475

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: adc165
severity: 1
line: 330
column: 40
content: 0x6f485C8BF6fc43eA212E93BBF8ce046C7f1cb475

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: adc165
severity: 1
line: 333
column: 24
content: 0x51efaF4c8B3C9AfBD5aB9F4bbC82784Ab6ef8fAA

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: adc165
severity: 1
line: 334
column: 40
content: 0x51efaF4c8B3C9AfBD5aB9F4bbC82784Ab6ef8fAA

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: b140cd
severity: 1
line: 203
column: 29
content: 0xFF

ruleId: SOLIDITY_ADDRESS_HARDCODED

patternId: b140cd
severity: 1
line: 206
column: 29
content: 0xFFFF

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: b140cd
severity: 1
line: 209
column: 29
content: 0xFFFFFFFF

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: b140cd
severity: 1
line: 212
column: 29
content: 0xFFFFFFFFFFFFFFFF

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: b140cd
severity: 1
line: 270
column: 35
content: 0x00

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: b140cd
severity: 1
line: 271
column: 37
content: 0x30

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: b140cd
severity: 1
line: 272
column: 37
content: 0xF0

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: b140cd
severity: 1

line: 273
column: 38
content: 0x01

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: b140cd
severity: 1
line: 274
column: 38
content: 0x40

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: b140cd
severity: 1
line: 275
column: 40
content: 0x10

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: b140cd
severity: 1
line: 1105
column: 53
content: 0x20

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: b140cd
severity: 1
line: 1109
column: 80
content: 0x20

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: b140cd
severity: 1
line: 1142
column: 21
content: 0xFE

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: a91b18
severity: 1
line: 1262
column: 19

content: (false,address(0))

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: a91b18
severity: 1
line: 1295
column: 19
content: (false,address(0))

ruleId: SOLIDITY_ARRAY_LENGTH_MANIPULATION
patternId: 872bdd
severity: 1
line: 1446
column: 9
content: numberBetPlayers[j].length=0

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: d3j11j
severity: 1
line: 896
column: 12
content:
for(uinti=0;i<h.length;i++){if(h[i]==n[0]){subindex=1;while(subindex<n.length&&(i+subindex)<h.len
gth&&h[i+subindex]==n[subindex]){subindex++;}if(subindex==n.length){returnint(i);}}}

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: d3j11j
severity: 1
line: 933
column: 8
content: for(i=0;i<_ba.length;i++){babcde[k++]=_ba[i];}

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: d3j11j
severity: 1
line: 936
column: 8
content: for(i=0;i<_bb.length;i++){babcde[k++]=_bb[i];}

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: d3j11j
severity: 1
line: 939
column: 8

content: for(i=0;i<_bc.length;i++){babcde[k++]=_bc[i];}

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: d3j11j
severity: 1
line: 942
column: 8
content: for(i=0;i<_bd.length;i++){babcde[k++]=_bd[i];}

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: d3j11j
severity: 1
line: 945
column: 8
content: for(i=0;i<_be.length;i++){babcde[k++]=_be[i];}

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: d3j11j
severity: 1
line: 959
column: 8
content:
for(uinti=0;i<bresult.length;i++){if((uint(uint8(bresult[i]))>=48)&&(uint(uint8(bresult[i]))<=57)){if(decimals){if(_b==0)break;else_b--;}mint*=10;mint+=uint(uint8(bresult[i]))-48;}elseif(uint(uint8(bresult[i]))==46){require(!decimals,'More than one decimal encountered in string!');decimals=true;}else{revert("Non-numeral character encountered in string!");}}

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: d3j11j
severity: 1
line: 988
column: 8
content:
for(uinti=0;i<bresult.length;i++){if((uint(uint8(bresult[i]))>=48)&&(uint(uint8(bresult[i]))<=57)){if(decimals){if(_b==0){break;}else{_b--;}}mint*=10;mint+=uint(uint8(bresult[i]))-48;}elseif(uint(uint8(bresult[i]))==46){decimals=true;}}

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: d3j11j
severity: 1
line: 1033
column: 8
content: for(uinti=0;i<_arr.length;i++){buf.encodeString(_arr[i]);}

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: d3j11j
severity: 1
line: 1045
column: 8
content: for(uinti=0;i<_arr.length;i++){buf.encodeBytes(_arr[i]);}

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: d3j11j
severity: 1
line: 1440
column: 6
content:
for(uinti=0;i<numberBetPlayers[numberWinner].length;i++){numberBetPlayers[numberWinner][i].tra
nsfer(winnerEtherAmount);}

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: k4o1l4
severity: 1
line: 899
column: 20
content:
while(subindex<n.length&&(i+subindex)<h.length&&h[i+subindex]==n[subindex]){subindex++;}

ruleId: SOLIDITY_FUNCTIONS_RETURNS_TYPE_AND_NO_RETURN
patternId: 58bdd3
severity: 1
line: 822
column: 4
content:
functiongetCodeSize(address_addr)viewinternalreturns(uint_size){assembly{_size:=extcodesize(_addr)
}}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 871
column: 8
content: for(uinti=0;i<minLength;i++){if(a[i]<b[i]){return-1;}elseif(a[i]>b[i]){return1;}}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 896

column: 12
content:
for(uinti=0;i<h.length;i++){if(h[i]==n[0]){subindex=1;while(subindex<n.length&&(i+subindex)<h.len
gth&&h[i+subindex]==n[subindex]){subindex++;}if(subindex==n.length){returnint(i);}}}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 933
column: 8
content: for(i=0;i<_ba.length;i++){babcde[k++]=_ba[i];}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 936
column: 8
content: for(i=0;i<_bb.length;i++){babcde[k++]=_bb[i];}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 939
column: 8
content: for(i=0;i<_bc.length;i++){babcde[k++]=_bc[i];}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 942
column: 8
content: for(i=0;i<_bd.length;i++){babcde[k++]=_bd[i];}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 945
column: 8
content: for(i=0;i<_be.length;i++){babcde[k++]=_be[i];}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 959

column: 8
content:
for(uinti=0;i<bresult.length;i++){if((uint(uint8(bresult[i]))>=48)&&(uint(uint8(bresult[i]))<=57)){if(decimals){if(_b==0)break;else_b--;}mint*=10;mint+=uint(uint8(bresult[i]))-48;}elseif(uint(uint8(bresult[i]))==46){require(!decimals,'More than one decimal encountered in string!');decimals=true;}else{revert("Non-numeral character encountered in string!");}}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 988
column: 8
content:
for(uinti=0;i<bresult.length;i++){if((uint(uint8(bresult[i]))>=48)&&(uint(uint8(bresult[i]))<=57)){if(decimals){if(_b==0){break;}else{_b--;}}mint*=10;mint+=uint(uint8(bresult[i]))-48;}elseif(uint(uint8(bresult[i]))==46){decimals=true;}}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 1033
column: 8
content: for(uinti=0;i<_arr.length;i++){buf.encodeString(_arr[i]);}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 1045
column: 8
content: for(uinti=0;i<_arr.length;i++){buf.encodeBytes(_arr[i]);}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 1440
column: 6
content:
for(uinti=0;i<numberBetPlayers[numberWinner].length;i++){numberBetPlayers[numberWinner][i].transfer(winnerEtherAmount);}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: 17f23a
severity: 1
line: 899

column: 26
content: subindex<n.length&&(i+subindex)<h.length&&h[i+subindex]==n[subindex]

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: 17f23a
severity: 1
line: 1218
column: 15
content: i<(32+_fromOffset+_length)

ruleId: SOLIDITY_LOCKED_MONEY
patternId: 30281d
severity: 3
line: 31
column: 0
content:
contractOraclizeI{addresspubliccbAddress;functionsetProofType(byte_proofType)external;functionset
CustomGasPrice(uint_gasPrice)external;functiongetPrice(stringmemory_datasource)publicreturns(uint
_dsprice);functionrandomDS_getSessionPubKeyHash()externalviewreturns(bytes32_sessionKeyHash);
functiongetPrice(stringmemory_datasource,uint_gasLimit)publicreturns(uint_dsprice);functionqueryN(
uint_timestamp,stringmemory_datasource,bytesmemory_argN)publicpayablereturns(bytes32_id);functi
onquery(uint_timestamp,stringcalldata<missing
')'>_datasource,stringcalldata_arg)externalpayablereturns<missing
';'>(bytes32_id);functionquery2(uint_timestamp,stringmemory_datasource,stringmemory_arg1,stringm
emory_arg2)publicpayablereturns(bytes32_id);functionquery_withGasLimit(uint_timestamp,stringcall
data<missing
')'>_datasource,stringcalldata_arg,uint_gasLimit)externalpayablereturns(bytes32_id);functionqueryN_
withGasLimit(uint_timestamp,stringcalldata<missing
')'>_datasource,bytescalldata_argN,uint_gasLimit)externalpayablereturns(bytes32_id);functionquery2_
withGasLimit(uint_timestamp,stringcalldata<missing
')'>_datasource,stringcalldata_arg1,stringcalldata_arg2,uint_gasLimit)externalpayablereturns(bytes32_i
d);}

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 24
column: 16
content: >=

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 1313

column: 16
content: ^

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 192
column: 10
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 193
column: 10
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 194
column: 10
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 195
column: 10
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 196
column: 10
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 197
column: 10
content: private

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 198
column: 10
content: private

ruleId: SOLIDITY_REVERT_REQUIRE
patternId: c56b12
severity: 1
line: 967
column: 19
content: if(uint(uint8(bresult[i]))==46){require(!decimals,'More than one decimal encountered in string!');decimals=true;}else{revert("Non-numeral character encountered in string!");}

ruleId: SOLIDITY_SHOULD_NOT_BE_PURE
patternId: 11314f
severity: 1
line: 79
column: 4
content:
functioninit(buffermemory_buf,uint_capacity)internalpure{uintcapacity=_capacity;if(capacity%32!=0){capacity+=32-(capacity%32);}_buf.capacity=capacity;assembly{letptr:=mload(0x40)mstore(_buf,ptr)mstore(ptr,0)mstore(0x40,add(ptr,capacity))}}

ruleId: SOLIDITY_SHOULD_NOT_BE_PURE
patternId: 11314f
severity: 1
line: 113
column: 4
content:
functionappend(buffermemory_buf,bytesmemory_data)internalpurereturns(buffermemory_buffer){if(_data.length+_buf.buf.length>_buf.capacity){resize(_buf,max(_buf.capacity,_data.length)*2);}uintdest;uintsrc;uintlen=_data.length;assembly{letbufptr:=mload(_buf)letbuflen:=mload(bufptr)dest:=add(add(bufptr,buflen),32)mstore(bufptr,add(buflen,mload(_data)))src:=add(_data,32)}for(;len>=32;len-=32){assembly{mstore(dest,mload(src))}dest+=32;src+=32;}uintmask=256**(32-len)-1;assembly{letsrcpart:=and(mload(src),not(mask))letdestpart:=and(mload(dest),mask)mstore(dest,or(destpart,srcpart))}return_buf;}

ruleId: SOLIDITY_SHOULD_NOT_BE_PURE
patternId: 11314f
severity: 1
line: 151

column: 4
content:
functionappend(buffermemory_buf,uint8_data)internalpure{if(_buf.buf.length+1>_buf.capacity){resiz
e(_buf,_buf.capacity*2);}assembly{letbufptr:=mload(_buf)letbuflen:=mload(bufptr)letdest:=add(add(b
ufptr,buflen),32)mstore8(dest,_data)mstore(bufptr,add(buflen,1))}}

ruleId: SOLIDITY_SHOULD_NOT_BE_PURE
patternId: 11314f
severity: 1
line: 172
column: 4
content:
functionappendInt(buffermemory_buf,uint_data,uint_len)internalpurereturns(buffermemory_buffer){if(
_len+_buf.buf.length>_buf.capacity){resize(_buf,max(_buf.capacity,_len)*2);}uintmask=256**_len-1;
assembly{letbufptr:=mload(_buf)letbuflen:=mload(bufptr)letdest:=add(add(bufptr,buflen),_len)mstore(
dest,or(and(mload(dest),not(mask)),_data))mstore(bufptr,add(buflen,_len))}return_buf;}

ruleId: SOLIDITY_SHOULD_NOT_BE_PURE
patternId: 11314f
severity: 1
line: 1213
column: 4
content:
functioncopyBytes(bytesmemory_from,uint_fromOffset,uint_length,bytesmemory_to,uint_toOffset)int
ernalpurereturns(bytesmemory_copiedBytes){uintminLength=_length+_toOffset;require(_to.length>=
minLength);uinti=32+_fromOffset;uintj=32+_toOffset;while(i<(32+_fromOffset+_length)){assembly{
lettmp:=mload(add(_from,i))mstore(add(_to,j),tmp)}i+=32;j+=32;}return_to;}

ruleId: SOLIDITY_SHOULD_NOT_BE_PURE
patternId: 11314f
severity: 1
line: 1300
column: 4
content:
functionsafeMemoryCleaner()internalpure{assembly{letfmem:=mload(0x40)codecopy(fmem,codesize,
sub(msize,fmem))}}

ruleId: SOLIDITY_SHOULD_NOT_BE_VIEW
patternId: 189abf
severity: 1
line: 822
column: 4
content:
functiongetCodeSize(address_addr)viewinternalreturns(uint_size){assembly{_size:=extcodesize(_addr)

}}

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 1232
column: 95
content: (bool_success,address_recoveredAddress)

ruleId: SOLIDITY_SHOULD_RETURN_STRUCT
patternId: 83hf3l
severity: 1
line: 1257
column: 75
content: (bool_success,address_recoveredAddress)

ruleId: SOLIDITY_TRANSFER_IN_LOOP
patternId: 8jdj43
severity: 2
line: 1440
column: 6
content:
for(uinti=0;i<numberBetPlayers[numberWinner].length;i++){numberBetPlayers[numberWinner][i].tra
nsfer(winnerEtherAmount);}

ruleId: SOLIDITY_UNCHECKED_CALL
patternId: f39eed
severity: 3
line: 341
column: 8
content: __callback(_myid,_result,newbytes(0))

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 85
column: 8
content: assembly{letptr:=mload(0x40)mstore(_buf,ptr)mstore(ptr,0)mstore(0x40,add(ptr,capacity))}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 120
column: 8

content:
assembly{letbufptr:=mload(_buf)letbuflen:=mload(bufptr)dest:=add(add(bufptr,buflen),32)mstore(bufptr,add(buflen,mload(_data)))src:=add(_data,32)}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 128
column: 12
content: assembly{mstore(dest,mload(src))}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 135
column: 8
content:
assembly{letsrcpart:=and(mload(src),not(mask))letdestpart:=and(mload(dest),mask)mstore(dest,or(destpart,srcpart))}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 155
column: 8
content:
assembly{letbufptr:=mload(_buf)letbuflen:=mload(bufptr)letdest:=add(add(bufptr,buflen),32)mstore8(dest,_data)mstore(bufptr,add(buflen,1))}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 177
column: 8
content:
assembly{letbufptr:=mload(_buf)letbuflen:=mload(bufptr)letdest:=add(add(bufptr,buflen),_len)mstore(dest,or(and(mload(dest),not(mask)),_data))mstore(bufptr,add(buflen,_len))}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 1060
column: 8
content:

assembly{mstore(unonce,0x20)mstore(add(unonce,0x20),xor(blockhash(sub(number,1)),xor(coinbase,timestamp)))mstore(sessionKeyHash,0x20)mstore(add(sessionKeyHash,0x20),sessionKeyHash_bytes32)}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 1072
column: 8
content: assembly{mstore(add(delay,0x20),_delay)}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 1080
column: 8
content:
assembly{letx:=mload(add(delay_bytes8,0x20))mstore8(add(delay_bytes8_left,0x27),div(x,0x1000000000000000000000000000000000000000000000000000000000))mstore8(add(delay_bytes8_left,0x26),div(x,0x10000000000000000000000000000000000000000000000000000000000000))mstore8(add(delay_bytes8_left,0x25),div(x,0x100000000000000000000000000000000000000000000000000000000000))mstore8(add(delay_bytes8_left,0x24),div(x,0x1000000000000000000000000000000000000000000000000))mstore8(add(delay_bytes8_left,0x23),div(x,0x10000000000000000000000000000000000000000000000000))mstore8(add(delay_bytes8_left,0x22),div(x,0x100000000000000000000000000000000000000000000))mstore8(add(delay_bytes8_left,0x21),div(x,0x1000000000000000000000000000000000000000000000))mstore8(add(delay_bytes8_left,0x20),div(x,0x10000000000000000000000000000000000000000000000000))}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 1110
column: 8
content: assembly{sigr:=mload(add(sigr_,32))sigs:=mload(add(sigs_,32))}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 1219
column: 12
content: assembly{lettmp:=mload(add(_from,i))mstore(add(_to,j),tmp)}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5

severity: 1
line: 1243
column: 8
content:
assembly{letsize:=mload(0x40)mstore(size,_hash)mstore(add(size,32),_v)mstore(add(size,64),_r)mstor
e(add(size,96),_s)ret:=call(3000,1,0,size,128,size,32)addr:=mload(size)}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 1269
column: 8
content: assembly{r:=mload(add(_sig,32))s:=mload(add(_sig,64))v:=byte(0,mload(add(_sig,96)))}

ruleId: SOLIDITY_USING_INLINE_ASSEMBLY
patternId: 109cd5
severity: 1
line: 1301
column: 8
content: assembly{letfmem:=mload(0x40)codecopy(fmem,codesize,sub(msize,fmem))}

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 41
column: 4
content: functionquery(uint_timestamp,stringcalldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 43
column: 4
content: functionquery_withGasLimit(uint_timestamp,stringcalldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067
severity: 1
line: 44
column: 4
content: functionqueryN_withGasLimit(uint_timestamp,stringcalldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: 910067

severity: 1
line: 45
column: 4
content: functionquery2_withGasLimit(uint_timestamp,stringcalldata<missing ')'>

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 41
column: 52
content: _datasource,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 41
column: 65
content: stringcalldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 41
column: 112
content: (bytes32_id);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 43
column: 65
content: _datasource,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 43
column: 78
content: stringcalldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 43

column: 94
content: _arg,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 43
column: 100
content: uint_gasLimit)externalpayablereturns

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 43
column: 141
content: (bytes32_id);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 44
column: 66
content: _datasource,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 44
column: 79
content: bytescalldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 44
column: 94
content: _argN,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 44
column: 101
content: uint_gasLimit)externalpayablereturns

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 44
column: 142
content: (bytes32_id);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 45
column: 66
content: _datasource,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 45
column: 79
content: stringcalldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 45
column: 95
content: _arg1,

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 45
column: 102
content: stringcalldata

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 45
column: 118
content: _arg2,

ruleId: SOLIDITY_VISIBILITY

patternId: b51ce0
severity: 1
line: 45
column: 125
content: uint_gasLimit)externalpayablereturns

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 45
column: 166
content: (bytes32_id);

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 263
column: 4
content: OraclizeIoraclize;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 264
column: 4
content: OraclizeAddrResolverIOAR;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 266
column: 4
content: uintconstantday=60*60*24;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 267
column: 4
content: uintconstantweek=60*60*24*7;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1

line: 268
column: 4
content: uintconstantmonth=60*60*24*30;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 270
column: 4
content: byteconstantproofType_NONE=0x00;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 271
column: 4
content: byteconstantproofType_Ledger=0x30;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 272
column: 4
content: byteconstantproofType_Native=0xF0;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 273
column: 4
content: byteconstantproofStorage_IPFS=0x01;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 274
column: 4
content: byteconstantproofType_Android=0x40;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 275
column: 4

content: byteconstantproofType_TLSNotary=0x10;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 277
column: 4
content: stringoraclize_network_name;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 278
column: 4
content: uint8constantnetworkID_auto=0;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 279
column: 4
content: uint8constantnetworkID_morden=2;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 280
column: 4
content: uint8constantnetworkID_mainnet=1;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 281
column: 4
content: uint8constantnetworkID_testnet=2;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 282
column: 4
content: uint8constantnetworkID_consensys=161;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 284
column: 4
content: mapping(bytes32=>bytes32)oraclize_randomDS_args;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 285
column: 4
content: mapping(bytes32=>bool)oraclize_randomDS_sessionKeysHashVerified;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1319
column: 3
content: addressowner;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1344
column: 3
content: mapping(uint=>addresspayable[])numberBetPlayers;

ruleId: SOLIDITY_VISIBILITY
patternId: b51ce0
severity: 1
line: 1347
column: 3
content: mapping(address=>uint)playerBetsNumber;

SOLIDITY_VISIBILITY :46
SOLIDITY_PRAGMAS_VERSION :2
SOLIDITY_ARRAY_LENGTH_MANIPULATION :1
SOLIDITY_FUNCTIONS_RETURNS_TYPE_AND_NO_RETURN :1
SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA :7
SOLIDITY_EXTRA_GAS_IN_LOOPS :12
SOLIDITY_ADDRESS_HARDCODED :23
SOLIDITY_GAS_LIMIT_IN_LOOPS :14
SOLIDITY_UNCHECKED_CALL :1

SOLIDITY_SHOULD_RETURN_STRUCT :2
SOLIDITY_SHOULD_NOT_BE_PURE :6
SOLIDITY_REVERT_REQUIRE :1
SOLIDITY_LOCKED_MONEY :1
SOLIDITY_USING_INLINE_ASSEMBLY :14
SOLIDITY_TRANSFER_IN_LOOP :1
SOLIDITY_SHOULD_NOT_BE_VIEW :1

25. send_loop.sol

smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/send_loop.sol

profganeshteam@SmartContract:~$ smartcheck -p /home/profganeshteam/Tools/FlattenedContracts/send_loop.sol
/home/profganeshteam/Tools/FlattenedContracts/send_loop.sol
jar:file:/usr/lib/node_modules/@smartdec/smartcheck/jdeploy-bundle/smartcheck-2.0-jar-with-dependencies.jar!/solidity-rules.xmlruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: adc165
severity: 1
line: 12
column: 29
content: 0x79B483371E87d664cd39491b5F06250165e4b184

ruleId: SOLIDITY_ADDRESS_HARDCODED
patternId: adc165
severity: 1
line: 13
column: 29
content: 0x79B483371E87d664cd39491b5F06250165e4b185

ruleId: SOLIDITY_EXTRA_GAS_IN_LOOPS
patternId: d3j11j
severity: 1
line: 18
column: 8
content:
for(uintx;x<refundAddresses.length;x++){require(refundAddresses[x].send(refunds[refundAddresses[x]]));}

ruleId: SOLIDITY_GAS_LIMIT_IN_LOOPS
patternId: f6f853
severity: 2
line: 18
column: 8
content:
for(uintx;x<refundAddresses.length;x++){require(refundAddresses[x].send(refunds[refundAddresses[x]]));}

ruleId: SOLIDITY_PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 4
column: 16
content: ^

ruleId: SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA
patternId: 5616b2
severity: 1
line: 8
column: 10
content: private

ruleId: SOLIDITY_SEND
patternId: 430636
severity: 1
line: 19
column: 39
content: send(refunds[refundAddresses[x]])

SOLIDITY_PRAGMAS_VERSION :1
SOLIDITY_PRIVATE_MODIFIER_DONT_HIDE_DATA :1
SOLIDITY_SEND :1
SOLIDITY_EXTRA_GAS_IN_LOOPS :1
SOLIDITY_ADDRESS_HARDCODED :2
SOLIDITY_GAS_LIMIT_IN_LOOPS :1