SKELETON ECOSYSTEM

SMART CONTRACT AUDIT

DVPN Network
DVPN
ERC20

0xc8cc4bBD33264dB465E4c9ea011F895D02505

Table of Contents

Global Disclaimer

This document serves as a disclaimer for the crypto smart contract audit conducted by Skeleton Ecosystem. The purpose of the audit was to review the codebase of the smart contracts for potential vulnerabilities and issues. It is important to note the following:

Limited Scope: The audit is based on the code and information available up to the audit completion date. It does not cover external factors, system interactions, or changes made after the audit. The audit itself can not guarantee 100% safaty and can not detect common scam methods like farming and developer sell-out.

No Guarantee of Security: While we have taken reasonable steps to identify vulnerabilities, it is impossible to guarantee the complete absence of security risks or issues. The audit report provides an assessment of the contract's security as of the audit date.

Continued Development: Smart contracts and blockchain technology are evolving fields. Updates, forks, or changes to the contract post-audit may introduce new risks that were not present during the audit.

Third-party Code: If the smart contract relies on third-party libraries or code, those components were not thoroughly audited unless explicitly stated. Security of these dependencies is the responsibility of their respective developers.

Non-Exhaustive Testing: The audit involved automated analysis, manual review, and testing under controlled conditions. It is possible that certain vulnerabilities or issues may not have been identified.

Risk Evaluation: The audit report includes a risk assessment for identified vulnerabilities. It is recommended that the development team carefully reviews and addresses these risks to mitigate potential exploits.

Not Financial Advice: This audit report is not intended as financial or investment advice. Decisions regarding the use, deployment, or investment in the smart contract should be made based on a comprehensive assessment of the associated risks.

By accessing and using this audit report, you acknowledge and agree to the limitations outlined above. Skeleton Ecosystem and its auditors shall not be held liable for any direct or indirect damages resulting from the use of the audit report or the smart contract itself.

Please consult with legal, technical, and financial professionals before making any decisions related to the smart contract.

Overview

Contract Name	DVPN
Ticker/Simbol	DVPN
Blockchain	Ethereum ERC20
Contract Address	0x22994fdB3f8509cf6a729BBfA93F939Db0B50D06
Creator Address	0x79B10f7A443D4050F5f12354d95D925bF747845d
Current Owner Address	0x0000000000000000000000000000000000000000
Contract Explorer	https://etherscan.io/address/0x22994fdB3f8509cf6a729BBfA93F939Db0B50D06#code
Compiler Version	v0.8.21+commit.d9974bed
License	MIT
Optimisation	No with 200 Runs
Total Supply	100,000,000DVPN
Decimals	18

Creation/Audit

Contract Deployed	22.05.2024
Audit Created	23.05.2023
Audit Update	V 1.0

Verified Socials

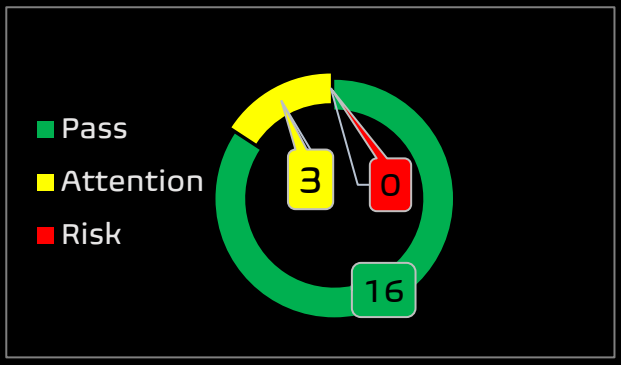
Website	https://devpn-erc.com/
Telegram	https://t.me/dvpnnetwork
Twitter (X)	https://x.com/dvpnnetworkerc

SKELETON ECOSYSTEM
SMART CONTRACT AUDIT REPORT

DVPN NETWORK ERC20

Contract Function Analysis

Pass Attention Item Risky Item

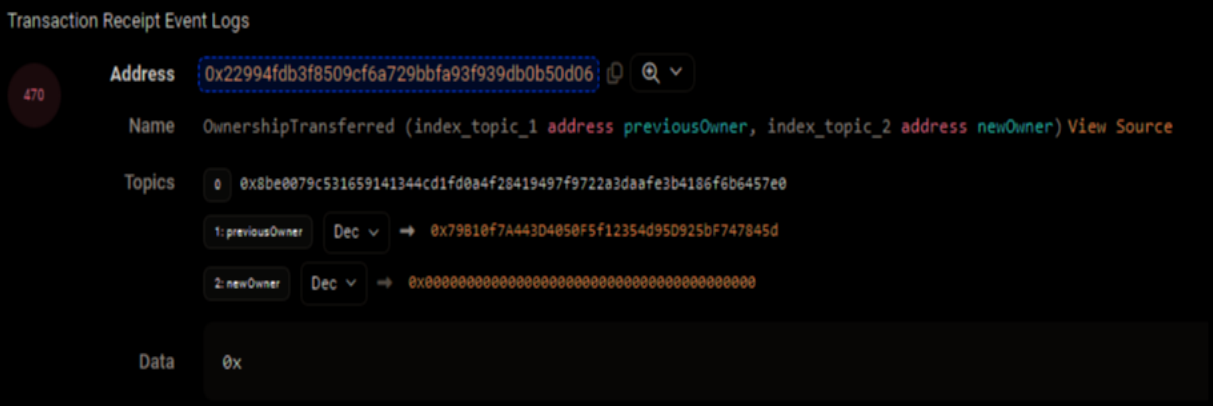


Contract Verified	✓	The contract source code is uploaded to blockchain explorer and is open source, so everybody can read it.
Contract Ownership		0x0000000000000000000000000000000000000000 Deployer
Buy Tax	5 %	Shows the taxes for purchase transactions. Above 10% may be considered a high tax rate. More than 50% tax rate means may not be tradable. Fee can be set!
Sell Tax	5 %	Shows the taxes for sell transactions. Above 10% may be considered a high tax rate. More than 50% tax rate means may not be tradable. Fee can be set!
Honeypot Analyse	✓	Holder is able to buy and sell. If honeypot: The contract blocks sell transfer from holder wallet. Multiple events may cause honeypot. Trading disabled, extremely high tax
Liqudity Status	✓	Liqudity status on 22.05.2024 Locked 99.00% on Unicrypt locker for *364 days.* https://etherscan.io/tx/0x2bb79fb5f7b2b5e44464c6e7a3acfbc3208fa425ff638d47025436311fb42bc9
Trading Disable Functions	✓	No Trading suspendable function found. If a suspendable code is included, the token maybe neither be bought or sold (honeypot risk). If contract is renounced this function can't be used
Set Fees function	⚠ max 5%	Fee Setting function found. Contract renounced, function can not be triggered by owner. The contract owner may contain the authority to modify the transaction tax. If the transaction tax is increased to more than 49%, the tokens may not be able to be traded (honeypot risk).
Proxy Contract	✓	Not a Proxy contract
Mint Function	✓	No Mint Function detected Mint function is transparent or non-existent. Hidden mint functions may increase the amount of tokens in circulation and effect the price of the token. Owner can mint new tokens and sell.

Balance Modifier Function	✅	No Balance Modifier function found. If there is a function for this, the contract owner can have the authority to modify the balance of tokens at other addresses. For example revoke the bought tokens from the holders wallet. Common form of scam: You buy the token, but it's disappearing from your wallet.
Blacklist Function	✅	No Blacklist Setting function found. If there is a blacklist, some addresses may not be able to trade normally. Example: you buy the token and right after your Wallet getting blacklisted. Like so you will be unable to sell. Honeypot Risk.
Whitelist Function	⚠️	Whitelist Setting function found. Contract renounced, function can not be triggered by owner. If there is a function for this Developer can set zero fee or no max wallet size for adresses (for example team wallets can trade without fee. Can cause farming)
Hidden Owner Analysis	✅	No Hidden or multi owner with authorisation For contract with a hidden owner, developer can still manipulate the contract even if the ownership has been abandoned.
Retrieve Ownership Function	✅	No Functions found which can retrieve ownership of the contract. If this function exists, it is possible for the project owner to regain ownership even after relinquishing it. Also known as fake renounce.
Self Destruct Function	✅	No Self Destruct function found. If this function exists and is triggered, the contract will be destroyed, all functions will be unavailable, and all related assets will be erased.
Specific Tax Changing Function	✅	No Specific Tax Changing Functions found. If it exists, the contract owner may set a very outrageous tax rate for assigned address to block it from trading. Can assign all wallets at once!
Trading Cooldown Function	✅	No Trading Cooldown Function found. If there is a trading cooldown function, the user will not be able to sell the token within a certain time or block after buying. Like a temporary honeypot.
Max Transaction and Holding Modify Function	⚠️	Max Transaction and Holding Modify function found. Contract renounced, function can not be triggered by owner. If there is a function for this, the maximum trading amount or maximum position can be modified. Can cause honeypot
Transaction Limiting Function	✅	No Transaction Limiter Function Found. The number of overall token transactions may be limited (honeypot risk)

Details of Risk - Attention Items

Removing Risk of contract function based on renounced ownership



Following detected contract functions serve as informational purposes about the contract. The owner has no more authorisation to trigger the following functions.

⚠ Set Fee (Max 5% limit found)

Contract renounced, function can not be triggered by owner.

The contract owner may contain the authority to modify the transaction tax. If the transaction tax is increased to more than 49%, the tokens may not be able to be traded (honeypot risk).

```
ftrace | funcSig
564    function updateFees(uint256 _buy↑, uint256 _sell↑) external onlyOwner {
565        require(_buy↑ <= 5, "Exceed the limit");
566        require(_sell↑ <= 5, "Exceed the limit");
567        buyTotalFees = _buy↑;
568        sellTotalFees = _sell↑;
569    }
570
```

⚠ Whitelist

Contract renounced, function can not be triggered by owner.

If there is a function for this Developer can set zero fee or no max wallet size for adresses (for example team wallets can trade without fee. Can cause farming)

```
ftrace | funcSig
513  function whitelistContract(address _whitelist, bool isWL) public onlyOwner {
514      _isExcludedMaxTransactionAmount[_whitelist] = isWL;
515
516      _isExcludedFromFees[_whitelist] = isWL;
517  }
518
ftrace | funcSig
519  function excludeFromMaxTransaction(address updAds, bool isEx) public onlyOwner {
520      _isExcludedMaxTransactionAmount[updAds] = isEx;
521  }
522
523  // only use to disable contract sales if absolutely necessary (emergency use only)
ftrace | funcSig
524  function updateSwapEnabled(bool enabled) external onlyOwner {
525      swapEnabled = enabled;
526  }
527
ftrace | funcSig
528  function excludeFromFees(address account, bool excluded) public onlyOwner {
529      _isExcludedFromFees[account] = excluded;
530      emit ExcludeFromFees(account, excluded);
531  }
532
```

⚠ Max Transaction and Holding Modify function

If there is a function for this, the maximum trading amount or maximum position can be modified. Can cause honeypot

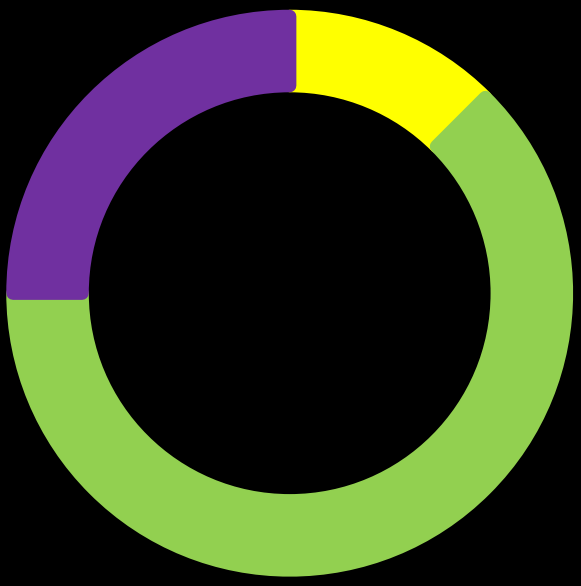
Contract renounced, function can not be triggered by owner.

```
ftrace | funcSig
499  function updateMaxSwap(uint256 newAmount) external onlyOwner {
500      maxSwapAmount = newAmount * (10 ** 18);
501  }
502
ftrace | funcSig
503  function updateMaxTxnAmount(uint256 newNum) external onlyOwner {
504      require(newNum >= ((totalSupply() * 1) / 1000) / 1e18, "Cannot set maxTransactionAmount lower than 0.1%");
505      maxTransactionAmount = newNum * (10 ** 18);
506  }
507
ftrace | funcSig
508  function updateMaxWalletAmount(uint256 newNum) external onlyOwner {
509      require(newNum >= ((totalSupply() * 5) / 1000) / 1e18, "Cannot set maxWallet lower than 0.5%");
510      maxWallet = newNum * (10 ** 18);
511  }
512
```

Contract Security

Total Findings: 8

- High 0
- Medium 1
- Low 5
- Info 2



High Severity Issues: High possibility to cause problems, need to be resolved.

Medium Severity Issue: Will likely cause problems, recommended to resolve.

Low Severity Issues: Won't cause problems, but for improvement purposes could be adjusted.

Informational Severity Issues: Not harmful in any way, information for the developer team.

Contract Security

List of Found Issues

High severity Issues: (0)

Medium severity issues: (1)

- Incorrect Access Control

Low severity issues: (5)

- Missing Events
- Long number literals
- Outdated compiler Version
- Approve of Front Running Attack
- Unchecked Array Lenght

Informational severity issues: (2)

- Public Functions Should be Declared External
- Costly Loop Operations

Contract Weakness Classisication

THE SMART CONTRACT WEAKNESS CLASSIFICATION REGISTRY (SWC REGISTRY) IS AN IMPLEMENTATION OF THE WEAKNESS CLASSIFICATION SCHEME PROPOSED IN EIP-1470. IT IS LOOSELY ALIGNED TO THE TERMINOLOGIES AND STRUCTURE USED IN THE COMMON WEAKNESS ENUMERATION (CWE) WHILE OVERLAYING A WIDE RANGE OF WEAKNESS VARIANTS THAT ARE

ID	Description	AI	Manual	Result
SWC-100	Function Default Visibility	Passed	Passed	Passed
SWC-101	Integer Overflow and Underflow	Passed	Passed	Passed
SWC-102	Outdated Compiler Version	low	low	low
SWC-103	Floating Pragma	Passed	Passed	Passed
SWC-104	Unchecked Call Return Value	Passed	Passed	Passed
SWC-105	Unprotected Ether Withdrawal	Passed	Passed	Passed
SWC-106	Unprotected SELFDESTRUCT Instruction	Passed	Passed	Passed
SWC-107	Reentrancy	Passed	Passed	Passed
SWC-108	State Variable Default Visibility	Passed	Passed	Passed
SWC-109	Uninitialized Storage Pointer	Passed	Passed	Passed
SWC-110	Assert Violation	Passed	Passed	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed	Passed	Passed
SWC-112	Delegatecall to Untrusted Callee	Passed	Passed	Passed
SWC-113	DoS with Failed Call	Passed	Passed	Passed
SWC-114	Transaction Order Dependence	Passed	Passed	Passed
SWC-115	Authorization through tx.origin	Passed	Passed	Passed
SWC-116	Block values as a proxy for time	Passed	Passed	Passed
SWC-117	Signature Malleability	Passed	Passed	Passed
SWC-118	Incorrect Constructor Name	Passed	Passed	Passed

SWC-119	Shadowing State Variables	Passed	Passed	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed	Passed	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed	Passed	Passed
SWC-122	Lack of Proper Signature Verification	Passed	Passed	Passed
SWC-123	Requirement Violation	Passed	Passed	Passed
SWC-124	Write to Arbitrary Storage Location	Passed	Passed	Passed
SWC-125	Incorrect Inheritance Order	Passed	Passed	Passed
SWC-126	Insufficient Gas Griefing	Passed	Passed	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed	Passed	Passed
SWC-128	DoS With Block Gas Limit	Passed	Passed	Passed
SWC-129	Typographical Error	low	Passed	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed	Passed	Passed
SWC-131	Presence of unused variables	Passed	Passed	Passed
SWC-132	Unexpected Ether balance	Passed	Passed	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed	Passed	Passed
SWC-134	Message call with hardcoded gas amount	Passed	Passed	Passed
SWC-135	Code With No Effects	Passed	Passed	Passed
SWC-136	Unencrypted Private Data On-Chain	Passed	Passed	Passed

Detected High and Medium Severity Vulnerability Description.

⚠ Approve of front running attack. Also known as Sandwich bot attack. (2 Items)

Item: 1	Location:	Line 298-301	Severity:	Low

Function	The approve() method overrides current allowance regardless of whether the spender already used it or not, so there is no way to increase or decrease allowance by a certain value atomically unless the token owner is a smart contract, not an account. This can be abused by a token receiver when they try to withdraw certain tokens from the sender's account. Meanwhile, if the sender decides to change the amount and sends another approve transaction, the receiver can notice this transaction before it's mined and can extract tokens from both the transactions, therefore, ending up with tokens from both the transactions. This is a front-running attack affecting the ERC20 Approve function. The function approve can be front-run by abusing the _approve function.
Remedation	1. Introduce mechanisms that limit the maximum acceptable gas price for transactions. This can help prevent front-runners from drastically increasing the gas fees to prioritize their transactions. 2. Use transaction taxes to prevent against front-run attack

```
ftrace | funcSig
298  function approve(address spender, uint256 amount) public virtual override returns (bool) {
299      _approve(_msgSender(), spender, amount);
300      return true;
301  }
302
```

Item: 2	Location:	Line 303-313	Severity:	Low

Function	The transferFrom() method overrides current allowance regardless of whether the spender already used it or not, so there is no way to increase or decrease allowance by a certain value atomically unless the token owner is a smart contract, not an account. This can be abused by a token receiver when they try to withdraw certain tokens from the sender's account. Meanwhile, if the sender decides to change the amount and sends another approve transaction, the receiver can notice this transaction before it's mined and can extract tokens from both the transactions, therefore, ending up with tokens from both the transactions. This is a front-running attack affecting the ERC20 Approve function. The function approve can be front-run by abusing the _approve function.
Remedation	1. Introduce mechanisms that limit the maximum acceptable gas price for transactions. This can help prevent front-runners from drastically increasing the gas fees to prioritize their transactions. 2. Use transaction taxes to prevent against front-run attack

```
ftrace | funcSig
303     function transferFrom(address sender, address recipient, uint256 amount) public virtual override returns (bool) {
304         _transfer(sender, recipient, amount);
305
306         uint256 currentAllowance = _allowances[sender][_msgSender()];
307         require(currentAllowance >= amount, "ERC20: transfer amount exceeds allowance");
308         unchecked {
309             _approve(sender, _msgSender(), currentAllowance - amount);
310         }
311
312         return true;
313     }
314
```

Outdated Compiler Version.

Item: 1	Location:	Line 15	Severity:	Low

Function	Using an outdated compiler version can be problematic especially if there are publicly disclosed bugs and issues that affect the current compiler version. The following outdated versions were detected: /dvpn.sol - ^0.8.21
Remedation	It is recommended to use a recent version of the Solidity compiler that should not be the most recent version, and it should not be an outdated version as well. Using very old versions of Solidity prevents the benefits of bug fixes and newer security checks. Consider using the solidity version v0.8.25, which patches most solidity vulnerabilities.

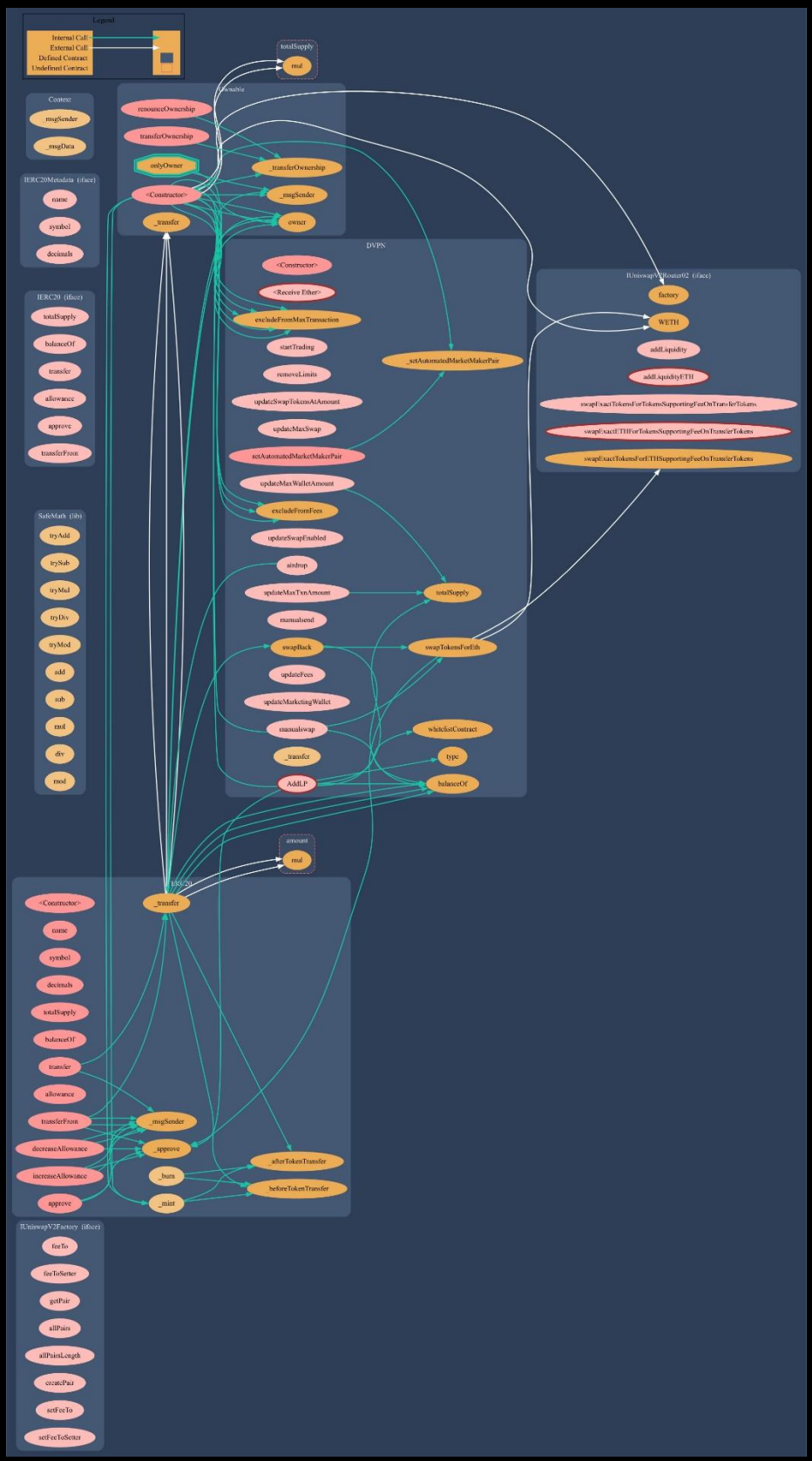
⚠ Incorrect Access Control (1 Item)

Item: 1	Location:	Line 539-542	Severity:	Medium

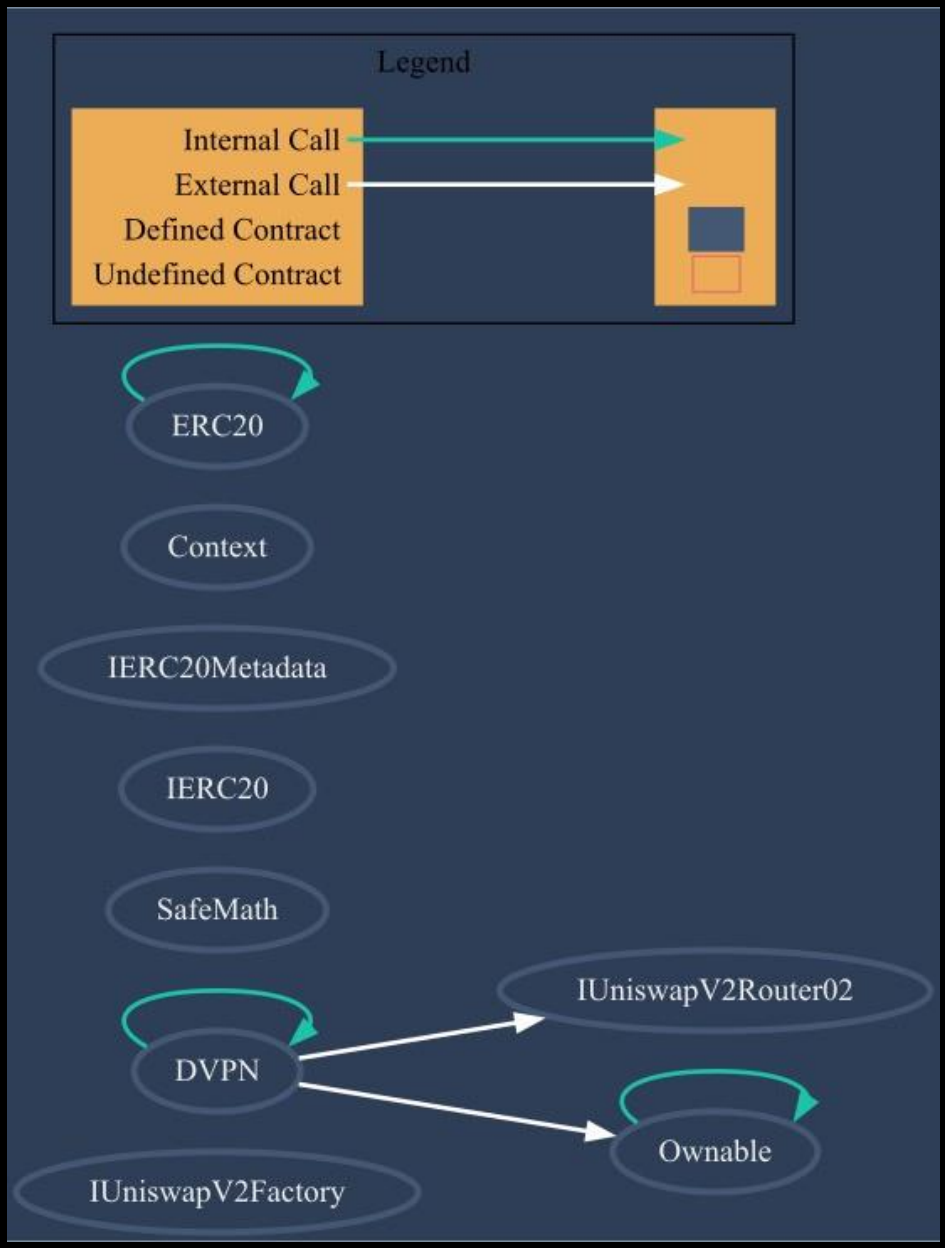
Function	Access control plays an important role in segregation of privileges in smart contracts and other applications. If this is misconfigured or not properly validated on sensitive functions, it may lead to loss of funds, tokens and in some cases compromise of the smart contract. The contract DVPN is importing an access control library @openzeppelin/contracts/access/Ownable.sol but the function manualsend is missing the modifier onlyOwner.
Remedation	1. Consider adding access control modifiers to the function to Ensure that initialization functions can only be called once and only by authorized entities. 2. Implement least-privilege roles using libraries like OpenZeppelin's Access Control. 3. Add proper access control modifiers to sensitive functions, such as onlyOwner or custom roles.

```
ftrace | funcSig
539     function manualsend() external {
540         bool success;
541         (success,) = address(marketingWallet).call{value: address(this).balance}("");
542     }
543
ftrace | funcSig
```

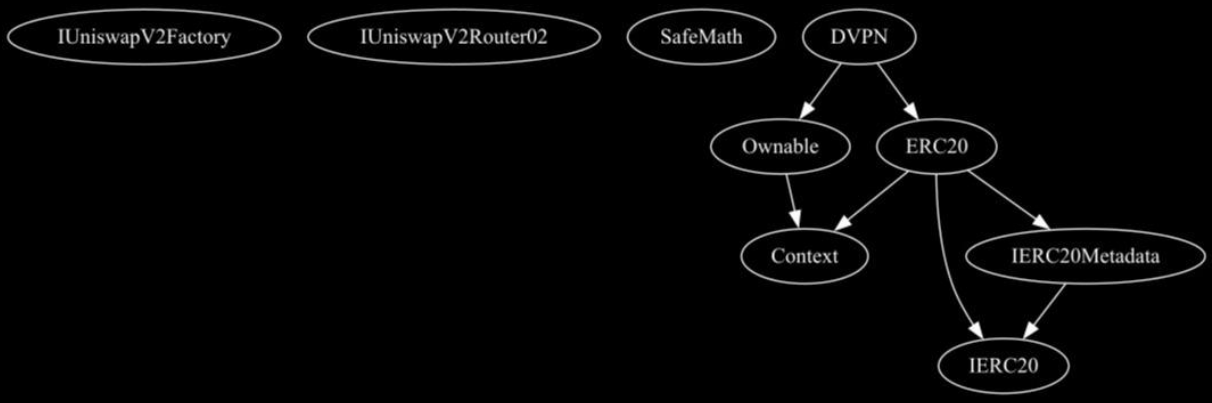
Contract Flow Graph



Contract Interaction Graph



Inheritance Graph



Contract Functions

Contract	Type	Bases		
L	Function Name	Visibility	Mutability	Modifiers
IUniswapV2Factory	Interface			
L	feeTo	External ❗		NO❗
L	feeToSetter	External ❗		NO❗
L	getPair	External ❗		NO❗
L	allPairs	External ❗		NO❗
L	allPairsLength	External ❗		NO❗
L	createPair	External ❗	🛑	NO❗
L	setFeeTo	External ❗	🛑	NO❗
L	setFeeToSetter	External ❗	🛑	NO❗
IUniswapV2Router02	Interface			
L	factory	External ❗		NO❗
L	WETH	External ❗		NO❗
L	addLiquidity	External ❗	🛑	NO❗
L	addLiquidityETH	External ❗	💵	NO❗
L	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
L	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗	💵	NO❗
L	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗

SafeMath	Library			
└	tryAdd	Internal 🔒		
└	trySub	Internal 🔒		
└	tryMul	Internal 🔒		
└	tryDiv	Internal 🔒		
└	tryMod	Internal 🔒		
└	add	Internal 🔒		
└	sub	Internal 🔒		
└	mul	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
└	sub	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
IERC20	Interface			
└	totalSupply	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	transfer	External ❗	🛑	NO❗
└	allowance	External ❗		NO❗
└	approve	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
IERC20Metadata	Interface	IERC20		
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗
└	decimals	External ❗		NO❗

Context	Implementation			
L	_msgSender	Internal 🔒		
L	_msgData	Internal 🔒		
Ownable	Implementation	Context		
L		Public ❗	🛑	NO❗
L	owner	Public ❗		NO❗
L	renounceOwnership	Public ❗	🛑	onlyOwner
L	transferOwnership	Public ❗	🛑	onlyOwner
L	_transferOwnership	Internal 🔒	🛑	
ERC20	Implementation	Context, IERC20, IERC20Metadata		
L		Public ❗	🛑	NO❗
L	name	Public ❗		NO❗
L	symbol	Public ❗		NO❗
L	decimals	Public ❗		NO❗
L	totalSupply	Public ❗		NO❗
L	balanceOf	Public ❗		NO❗
L	transfer	Public ❗	🛑	NO❗
L	allowance	Public ❗		NO❗
L	approve	Public ❗	🛑	NO❗
L	transferFrom	Public ❗	🛑	NO❗
L	increaseAllowance	Public ❗	🛑	NO❗
L	decreaseAllowance	Public ❗	🛑	NO❗
L	_transfer	Internal 🔒	🛑	

L	_mint	Internal 🔒	🛑	
L	_burn	Internal 🔒	🛑	
L	_approve	Internal 🔒	🛑	
L	_beforeTokenTransfer	Internal 🔒	🛑	
L	_afterTokenTransfer	Internal 🔒	🛑	
DVPN	Implementation	ERC20, Ownable		
L		Public ❗	🛑	ERC20
L		External ❗	💸	NO❗
L	AddLP	External ❗	💸	onlyOwner
L	startTrading	External ❗	🛑	onlyOwner
L	removeLimits	External ❗	🛑	onlyOwner
L	updateSwapTokensAtAmount	External ❗	🛑	onlyOwner
L	updateMaxSwap	External ❗	🛑	onlyOwner
L	updateMaxTxnAmount	External ❗	🛑	onlyOwner
L	updateMaxWalletAmount	External ❗	🛑	onlyOwner
L	whitelistContract	Public ❗	🛑	onlyOwner
L	excludeFromMaxTransaction	Public ❗	🛑	onlyOwner
L	updateSwapEnabled	External ❗	🛑	onlyOwner
L	excludeFromFees	Public ❗	🛑	onlyOwner
L	manualswap	External ❗	🛑	NO❗
L	manualsend	External ❗	🛑	NO❗
L	setAutomatedMarketMakerPair	Public ❗	🛑	onlyOwner

L	_setAutomatedMarketMakerPair	Private		
L	updateFees	External		onlyOwner
L	updateMarketingWallet	External		onlyOwner
L	airdrop	External		NO!
L	_transfer	Internal		
L	swapTokensForEth	Private		
L	swapBack	Private		

Function can modify state

Function is payable

Audit Scope

Audit Method.

Our smart contract audit is an extensive methodical examination and analysis of the smart contract's code that is used to interact with the blockchain. Goal: discover errors, issues and security vulnaribilities in the code. Findings getting reported and improvements getting suggested.

Automatic and Manual Review
We are using automated tools to scan functions and weeknesses of the contract. Transfers, integer over-undeflow checks such as all CWE events.

Tools we use:
Visual Studio Code
CWE
SWC
Solidity Scan
SVD

In manual code review our auditor looking at source code and performing line by line examination. This method helps to clarify developer's coding decisions and business logic.

Skeleton Ecosystem

https://skeletonecosystem.com

https://github.com/SkeletonEcosystem/Audits