Hans's Checklist

Summary

Author: Hans

The checklist is a collection of common issues that Hans has came across during audits. It is not a complete list of all possible issues. The checklist stands out from other checklists by the links to the references and the explanation of the issues.

Checklist

Category	Issue	Details	Reference
Version Issues	Solidity 0.8.13	Use of Solidity 0.8.13 with known issues in ABI encoding and memory side effects	https://github.com/code-423n4/2022-06-putty-findings/issues/348
	Solidity 0.8.17	abi.encodePacked allows hash collision in Solidity 0.8.17	https://github.com/sherlock-audit/2022-10-nftport-judging/issues/118
	OpenZeppelin < 4.7.3	OpenZeppelin has a vulnerability in versions lower than 4.7.3	https://github.com/sherlock-audit/2022-09-harpie-judging/blob/main/010-M/010-h.md
	selfdestruct()	After EIP-4758, selfdestruct won't work	https://github.com/code-423n4/2022-07-axelar-findings/issues/20
Inheritance	Upgradability	Make sure to inherit the correct branch of OpenZepplin library	https://solodit.xyz/issues/912
	Initializable inheritance	Inheritable/Upgradable contracts should use initializer modifier carefully	https://solodit.xyz/issues/1684
	Interface implementation	Check if all functions are implemented from the interface	https://solodit.xyz/issues/1322
	Ownable - ownership transfer	Use two-step process and make sure the protocol works while transfer	https://solodit.xyz/issues/3525
Initialization	State variables initialization	Check if important variables are initialized correctly	https://solodit.xyz/issues/2594

Category	Issue	Details	Reference
	Initialization arguments validation	Check if important variables are validated on initialization	https://solodit.xyz/issues/3537
	Domain Separator	Check if DOMAIN_SEPARATOR is set correctly	https://solodit.xyz/issues/2507
	Set critical params in constructor		https://github.com/code-423n4/2022-05-backd-findings/issues/99
Validation	Min/Max validation	Check if parameters are capped correctly	https://solodit.xyz/issues/3591
	Time validation		
	Zero input, double call validation		
	Calling multiple times	Calling a function X times with value Y == Calling it once with value XY	
	src==dst	Check what happens if an action is done to itself	
	don't check min threshold during withdrawal	Users wouldn't withdraw dust	https://solodit.xyz/issues/5912
	Don't use Address.isContract() for EOA checking		https://solodit.xyz/issues/5925
	OnlyEOA modifier using tx.origin		https://solodit.xyz/issues/6662
Admin Privilege	Rescue tokens from contract(2 addresses token)	Shouldn't allow to withdraw user's funds	
	Change active orders	Admin can change price/fee at any time for existing orders	https://github.com/code-423n4/2022-06-putty-findings/issues/422
Denial Of Service (DOS)	Withdraw check	Follow Withdraw-Pattern for best practice	https://solodit.xyz/issues/2939
	External contracts interaction	Make sure the protocol is not affected when the external dependencies do not work	https://solodit.xyz/issues/2967

Category	Issue	Details	Reference
	Minimum transaction amount	Disallow zero amount transactions to prevent attackers putting enormous requests	https://solodit.xyz/issues/1516
	Tokens with blacklisting	USDC	
	Forcing protocol to go through a list	e.g. queue of dust withdrawals	
	Possible DOS with low decimal tokens	The process wouldn't work because token amount is 0 when it should work	https://solodit.xyz/issues/6998
	Check overflow during multiply		https://solodit.xyz/issues/6854
	Use unchecked for TickMath, FullMath from uniswap	These libraries of uniswap use version 0.7.6	https://solodit.xyz/issues/6879
Gas limit	Active draining gas	An attacker can drains gas and leaves very little to prevent future processing	https://solodit.xyz/issues/3709
	Long loop	Loop without start index	https://github.com/sherlock-audit/2022-11-isomorph-judging/issues/69
Replay Attack	Failed TXs are open to replay attacks		https://github.com/code-423n4/2022-03-rolla-findings/issues/45
	Replay signature attack on another chain		https://github.com/sherlock-audit/2022-09-harpie-judging/blob/main/004-M/004-m.md
Pause/Unpause	Users can't cancel/withdraw when paused		
	Users can't avoid to pay penalty(interest) when paused		
Re-entrancy	CEI pattern check		https://solodit.xyz/issues/3560
	Complicated path exploit		https://solodit.xyz/issues/3383
Front-run	Get or Create	This kind of work is very likely to have vulnerability to frontrunning	

Category	Issue	Details	Reference
	Two-transaction actions should be safe from frontrunning	A good example is when the protocol depends on the user's approval to take the token	https://github.com/sherlock-audit/2022-11-isomorph-judging/issues/47
	Make other's call revert by calling first with dust		https://solodit.xyz/issues/5920
Array	Transaction while reassignment	Best practice - do not require index as a parameter	
	Summing vs separate calculation	Calculation against the sum is often more than the sum of each one calculated	https://github.com/sherlock-audit/2022-11-isomorph-judging/issues/174
Defi	Oracle: Usage of deprecated chainlink functions	latestRoundData() might return stale or incorrect results	https://github.com/code-423n4/2022-04-backd-findings/issues/17
	Oracle: twap period	Oracle's period is very low allowing the twap price to be manipulated	https://github.com/code-423n4/2022-06-canto-v2-findings/issues/124
	Hard-coded slippage	Hard-coded slippage may freeze user funds during market turbulence	https://github.com/code-423n4/2022-05-sturdy-findings/issues/133
	Validate reserve	Protocol reserve can be lent out	https://github.com/sherlock-audit/2022-08-sentiment-judging/blob/main/122-M/1-report.md
	ETH 2.0 reward slashing		https://solodit.xyz/issues/5924
	Check flashloan attack during stake/unstake	Attackers can steal staking rewards using via flashloan	
	Check deadline during trading	Recommend checking deadline	https://solodit.xyz/issues/6297
	Should add an interest during LTV calculation		https://solodit.xyz/issues/6644
	Use twap instead of raw value		https://solodit.xyz/issues/6647
	Liquidation/repaying should be enabled/disabled together		https://solodit.xyz/issues/6649
	Liquidation should work after frontrunning by borrower	liqAmount might be decreased by borrower using frontrunning	https://solodit.xyz/issues/7364

Category	Issue	Details	Reference
	Defi functions should have deadline like uniswap		https://solodit.xyz/issues/6687
	0x requires ETH as fee	https://0x.org/docs/0x-swap-api/guides/use-0x-api-liquidity-in-your-smart-contracts	https://solodit.xyz/issues/8722
	Chainlink price in L2 chains	https://docs.chain.link/data-feeds/l2-sequencer-feeds#example-code	https://solodit.xyz/issues/6689
	Dangerous reward distribution	A user can prevent other's reward distribution by reverting himself	https://solodit.xyz/issues/7263
	Constant ratio is dangerous during depegging	Should use oracle to get price	https://solodit.xyz/issues/9793
Flashloan	Checkpoint faking	OpenZepplin checkpoint works with block number that can be faked with flashloan	
	Disable withdraw in the same block		
	ERC4626 flashloan manipulation		https://github.com/code-423n4/2022-01-behodler-findings/issues/304
ERC20	Fee-on-transfer token	Best practice - check before/after balance	https://solodit.xyz/issues/3630
	ERC777 - tokens with hooks	Best practice - Check Effect Interaction pattern	https://solodit.xyz/issues/3627
	Multi-addresses token	Best practice - check before/after balance of that address, no compare address	
	Return value of transfer/approve	Best practice - safeERC20 of OpenZepplin	
	Revert on zero transfer		https://github.com/code-423n4/2022-05-sturdy-findings/issues/79
	Revert to address(0)		https://github.com/code-423n4/2022-07-yield-findings/issues/116

Category	Issue	Details	Reference
	solmate's SafeTransferLib	solmate's SafeTransferLib doesn't check if the token is a contract	https://github.com/code-423n4/2022-05-cally-findings/issues/225
	safeapprove()	safeapprove() must first be approved by zero	https://github.com/code-423n4/2022-04-backd-findings/issues/180
	should approve before swap		
	Revert on Approve Max		https://solodit.xyz/issues/3521
	transferfrom() shouldn't decrease allowance if from = caller		https://solodit.xyz/issues/6704
ERC721/1155	Make sure supportsInterface succeeds	Contract should return true for supportsInterface call	https://solodit.xyz/issues/703
	Support both ERC721 and ERC1155	Use supportsInterface in order of 1155/721 to support both	https://solodit.xyz/issues/2772
	Free NFT ownership is dangerous for airdrop		https://solodit.xyz/issues/6102
	Allowance logic for CryptoPunks are frontrunable	Should check the owner for CryptoPunks	https://solodit.xyz/issues/6289
ERC4626	Initial Deposit Issue	Mint some initial tokens and save the initial shares as a permanent reserve	https://solodit.xyz/issues/3474
	First Depositor Issue	First depositor can break minting of shares	https://github.com/code-423n4/2022-04-jpegd-findings/issues/12
	EIP4626 decimals	EIP4626 can have different decimals from the underlying token	https://github.com/sherlock-audit/2022-08-sentiment-judging/blob/main/025-H/025-h.md
Misc.	block.number is inconsistent in Ethereum/Optimism/Arbitrum		https://solodit.xyz/issues/6345
	There should be some delay to activate proposal		https://solodit.xyz/issues/3213
	Check code asymmetries	Check create/delete, deposit/withdraw patterns	

Category	Issue	Details	Reference
	LibClone's clone function generates ETH receive() automatically		
	There should be a removal logic for bad controllers		https://solodit.xyz/issues/7157
	The contract should be able to withdraw airdrops if any		https://solodit.xyz/issues/9624