Category	Description of Category	Finding type	Example
Business Logic	Reviewing the logic to ensure that the code implements the expected functionality as specified in the documents.	Differences between Morpho and Compound borrow validation logic (missing logic)	https://solodit.xyz/issues/differences-between-morpho-and-compound-borrow-validation-logic-spearbit-morpho-pdf
Numerics	Handling and processing numerical values and calculations accurately and efficiently, considering potential limitations, precision issues, and rounding errors associated with different data types and arithmetic operations.	Precision is lost in depositAuction and withdrawAuction user amount due calculations	https://solodit.xyz/issues/m-1-precision-is-lost-in-depositauction-and-withdrawauction-user-amount-due-calculations-sherlock-opyn-opyn-crab-netting-git
		Compare two or more tokens with different value without appropriate handling	https://solodit.xyz/issues/h-06-discrepency-in-the-uniswap-v3-position-price-calculation-because-of-decimals-code4rena-paraspace-paraspace-contest-git#
		Wrong calculations with low-decimals t	https://solodit.xyz/issues/m-04-interest-accrued-could-be-zero-for-small-decimal-tokens-code4rena-sublime-sublime-contest-git
Access Control	Assessing and managing the mechanisms in place to regulate and restrict user access to resources, systems, or information based on predefined permissions and privileges.		
Data Validation	Evaluating the mechanisms of the smart contract for validating and verifying the integrity and correctness of the data it relies on.	Unchecked external calls in NFTXLPStaking	https://solodit.xyz/issues/l-06-unchecked-external-calls-in-nftxlpstaking-code4rena-nftx-nftx-contest-git
		Price deviations between stETH and ETH may cause Tellor oracle to return an incorrect price	https://solodit.xyz/issues/price-deviations-between-steth-and-eth-may-cause-tellor-oracle-to-return-an-incorrect-price-trailofbits-tempus-raft-pdf
Cryptography	Implementing secure cryptographic algorithms and protocols to protect sensitive data, ensuring confidentiality, integrity, and authentication in various applications and systems.	setGlobalKey is susceptible to signature replay	https://solodit.xyz/issues/setglobalkey-is-susceptible-to-signature-replay-trailofbits-dharma-labs-smart-wallet-pdf
Gas Griefing	Insufficient gas griefing attacks can be performed on contracts which accept data and use it in a sub-call on another contract. If the sub-call fails, either the whole transaction is reverted, or execution is continued. In the case of a relayer contract, the user who executes the transaction, the 'forwarder', can effectively censor transactions by using just enough gas to execute the transaction, but not enough for the sub-call to succeed.		https://swcregistry.io/docs/SWC-126
Denial of Service	Identifying and mitigating vulnerabilities that could lead to a Denial of Service attack, which aims to disrupt or incapacitate a system, network, or service, rendering it unavailable to legitimate users.	Unbounded loop can cause denial of service	https://solodit.xyz/issues/unbounded-loop-can-cause-denial-of-service-trailofbits-growth-labs-gsquared-pdf
		Incorrect fee calculation on withdrawal can lead to DoS of withdrawals or loss of assets	https://solodit.xyz/issues/incorrect-fee-calculation-on-withdrawal-can-lead-to-dos-of-withdrawals-or-loss-of-assets-trailofbits-atlendis-labs-loan-products-pdf
	Assessing and improving the overall quality, readability, maintainability, and efficiency of the software codebase through practices like code reviews, adherence to coding standards, and the use of automated analysis tools.		
Reentrancy	Addressing vulnerabilities that could allow an attacker to reenter a function or contract before the previous execution has completed, potentially leading to unintended consequences or malicious actions.		
Inconsistency	This category focuses on identifying and resolving inconsistencies, disparities, or discrepancies between documented specifications, guidelines, or instructions and the actual implementation of a system, software, or process.		
Redundancy	Eliminating unnecessary or redundancies in smart contracts or code, minimizing potential attack surfaces or unintended behavior.		
Centralization	Assessing and mitigating risks associated with centralization of data, control, or authority in systems or organizations, considering potential single points of failure or vulnerabilities.	Owner can extract all wrapped token from WrapTokenGateway	https://solodit.xyz/issues/owner-can-extract-all-wrapped-token-from-wraptokengateway-halborn-savvy-defi-pdf
Configuration	Managing and maintaining the configuration settings and parameters of a system or application, including customization options, environmental variables, and external dependencies, to ensure optimal performance and functionality.	Floating pragma	https://solodit.xyz/issues/floating-pragma-halborn-easyfi-staking-contracts-pdf
		Configuration is crucial (both Nomad and Connext)	https://solodit.xyz/issues/configuration-is-crucial-both-nomad-and-connext-spearbit-connext-pdf
Compiler	Identifying and addressing vulnerabilities that depend on compiler version.		https://docs.soliditylang.org/en/latest/bugs.html

Category	Description of Category	Finding type	Example
Logging	Implementing a system that captures and records relevant events, actions, and errors occurring within an application or system, facilitating troubleshooting, auditing, and analysis of system behavior.	Emit pool information on the add pool function	https://solodit.xyz/issues/emit-pool-information-on-the-add-pool-function-halborn-savvy-defi-pdf
Selfdestruct	Considering the implications and risks associated with the self-destruct functionality in smart contracts, ensuring proper usage and safeguarding against unintended consequences.	Use of selfdestruct function	https://solodit.xyz/issues/use-of-selfdestruct-function-halborn-polkadex-pdf
Weak Randomness	Identifying and addressing vulnerabilities that depend on the randomness of deterministic variables.	Bad source of randomness	https://solodit.xyz/issues/m-06-bad-source-of-randomness-code4rena-holograph-holograph-contest-git
Front-running	Identifying and addressing vulnerabilities that allow malicious actors to exploit privileged information, typically in decentralized financial applications, to gain unfair advantages in transactions or trades.	Race condition in _startBridge of LIFuelFacet	https://solodit.xyz/issues/race-condition-in-_startbridge-oflifuelfacet-spearbit-lifi-pdf
		Front run of addBlackList() function	https://solodit.xyz/issues/m-3-front-run-of-addblacklist-function-sherlock-telcoin-telcoin-update-git
Gas Optimization	Suggestions for reducing gas costs.		