Audit Report - e9878782-8e54-4020-aedb-4b7579a49537

HIGH - Line 132

Issue: Reentrancy vulnerability in fulfillRandomWords function

Recommendation: Use the Checks-Effects-Interactions pattern to prevent reentrancy attacks. In this case, move the external call to recentWinner after all state changes have been made.

MEDIUM - Line 84

Issue: Use of tx.origin is not present, but msg.sender is cast to payable without checking if it's a contract. If it's a contract, it might not be able to receive ether.

Recommendation: Check if msg.sender is a contract before casting it to payable and sending ether to it.

MEDIUM - Line 43

Issue: Use of immutable variables for configuration parameters

Recommendation: While not necessarily a security issue, using immutable variables for configuration parameters like i_interval and i_entranceFee can make the contract less flexible. Consider using a more dynamic configuration method if needed.

LOW - Line 104

Issue: checkUpkeep function does not check if the contract has enough LINK to fulfill the randomness request

Recommendation: Add a check in the checkUpkeep function to ensure that the contract has enough LINK to fulfill the randomness request.

LOW - Line 171

Issue: getPlayer function does not check if the index is within bounds

Recommendation: Add a check in the getPlayer function to ensure that the index is within the bounds of the s_players array.