Homework 12

Audit

Imagine you have been given the following code to audit

Contract

with the following note from the team

"DogCoinGame is a game where players are added to the contract via the addPlayer function, they need to send 1 ETH to play.
Once 200 players have entered, the UI will be notified by the startPayout event, and will pick 100 winners which will be added to the winners array, the UI will then call the payout function to pay each of the winners.
The remaining balance will be kept as profit for the developers."

Write out the main points that you would include in an audit report.

Underhanded Solidity

This contract is the winner of this years underhanded solidity contest, it mimics the OpenSea application.
Can you spot the flaws in it

⛽🏌️ This is a gas-golfed version of Zora v3's Offers module!
🤩 A bidder can call createBid to bid on the NFT of their dreams.
💰 The NFT owner can call acceptBid to accept one of these on-chain bids.
🤝 Assets exchange hands.
😤 What could possibly go wrong?

Hints
Look at the Solmate contracts used, and the way transferFrom is implemented.