Homework 11 Answers

Audit contract

Answer

Problems

- 1. Floating Pragma: pragma solidity ^0.8.13;
- 2. Initialising variables to default values: lines 8,10,24,25,42
- 3. No security for function addInvestor
- 4. No security for function claimTokens
- 5. Repeat calculation of length property: line 27
- 6. No break in loop: line 29
- 7. Shadowing of blockReward variable: line 43
- 8. Block reward calculation is incorrect
- 9. Block reward calculation should have multiplication first
- 10. Public functions could be external
- 11. Investors array could grow too large for loop to complete
- 12. Initial amount could be immutable
- 13. A mapping may be more suitable to store investors (or a merkle tree)

Underhand Solidity Contest

Answer

See the description here