HOMEWORK 6

Part 1 - Very Safu Proxy

1. Do not use code that you do not understand - simply put, if you are not sure about how delegatecall works, do NOT use it - ask people, read articles and docs!
2. Never trust unstructured storage that does not give the formulas to how the slots are calculated!
3. Even if the formulas are given, do not trust that the coded values are the right ones!
4. Just because the comment above some random values says "EIP" do NOT trust it - especially if it's not a finalized proposal.
5. Do not be lazy, verify everything !

Part 2 - Contract

FINDINGS

CRITICAL SEVERITY

1. There is no require statement to ensure that the payment is received, without verifying if payment is received, the function allows for state changes.

2. Instead of specifying 1 ether, it is specified as just 1, which translates to 1 wei instead of 1 ether.

3. Winner function is public. Anyone can be added to winner list, without any criteria, even the ones who are not players.

4. The payOut Function logic checks if balance of contract is 100 wei instead of 100 ether.

5. The amountToPay calculation also seems faulty.

6. The payWinners function is public, so anyone can add themself to winners list and call payWinners function to drain the balance of contract.

MAJOR SEVERITY

1. Compiler warns against usage of send function. It is not recommended for sending Ether.

INFORMATION

1. **currentPrize** is unused.