LHOUSSAINE AIT AISSA

1. Initial Research and Context Gathering

- **Objective**: Understand the target contract and its potential vulnerabilities by analyzing similar contracts that have recently been exploited.
- **Approach**: Identify key vulnerability areas by studying the nature of previous hacks.
- **Tools**:
  - https://hacked.slowmist.io/
  - https://rekt.news/
  - https://immunefi.com/
  - https://defisafety.com/
  - https://blog.openzeppelin.com/
  - Relevant Twitter/X accounts for real-time updates

2. Reconnaissance

- **Objective**: Conduct an in-depth analysis of the contract's codebase, dependencies, and architecture.
- **Approach**: Compare the contract with others that have known vulnerabilities to identify potential weak spots.
- **Tools**:
  - Static Analysis Tools (e.g., Slither, MythX, Oyente)
  - Fuzz Testing (e.g., ityFuzz, Echidna, Etheno)
  - https://etherscan.io/ for contract exploration
  - AI tools for pattern recognition and code analysis

3. Manual Code Review

- **Objective**: Perform a thorough manual inspection of the smart contract.
- **Approach**: Focus on discovering logic errors, unsafe operations, and common vulnerability patterns such as reentrancy, unchecked calls, and integer overflows/underflows.

4. Exploit Simulation

- **Objective**: Test the contract's resilience by simulating potential attacks.
- **Approach**: Develop proof-of-concept exploits and test them in a controlled environment to evaluate the contract's behavior under attack scenarios.
- **Tools**:
  - Foundry Framework for testing and simulation
  - Testnet Networks (e.g., Sepolia) for deployment and testing

5. Reporting

- **Objective** : Deliver a detailed report on identified vulnerabilities.
- **Approach** : Document findings, proof of exploitation, and risk assessment.