Smart-Contract Auditing

Members: Nick Carnevale, David Cueva, Kaushik Duvur, Jack Mishkin

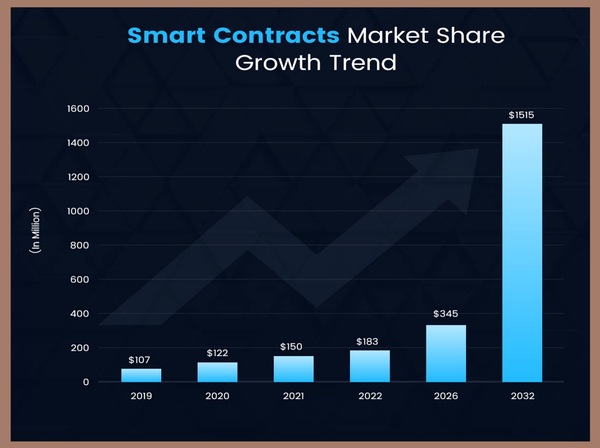
CSB/CSE Capstone Project 2024
Advisor: Thomas Reynolds
Sponsor: MacguyverTech

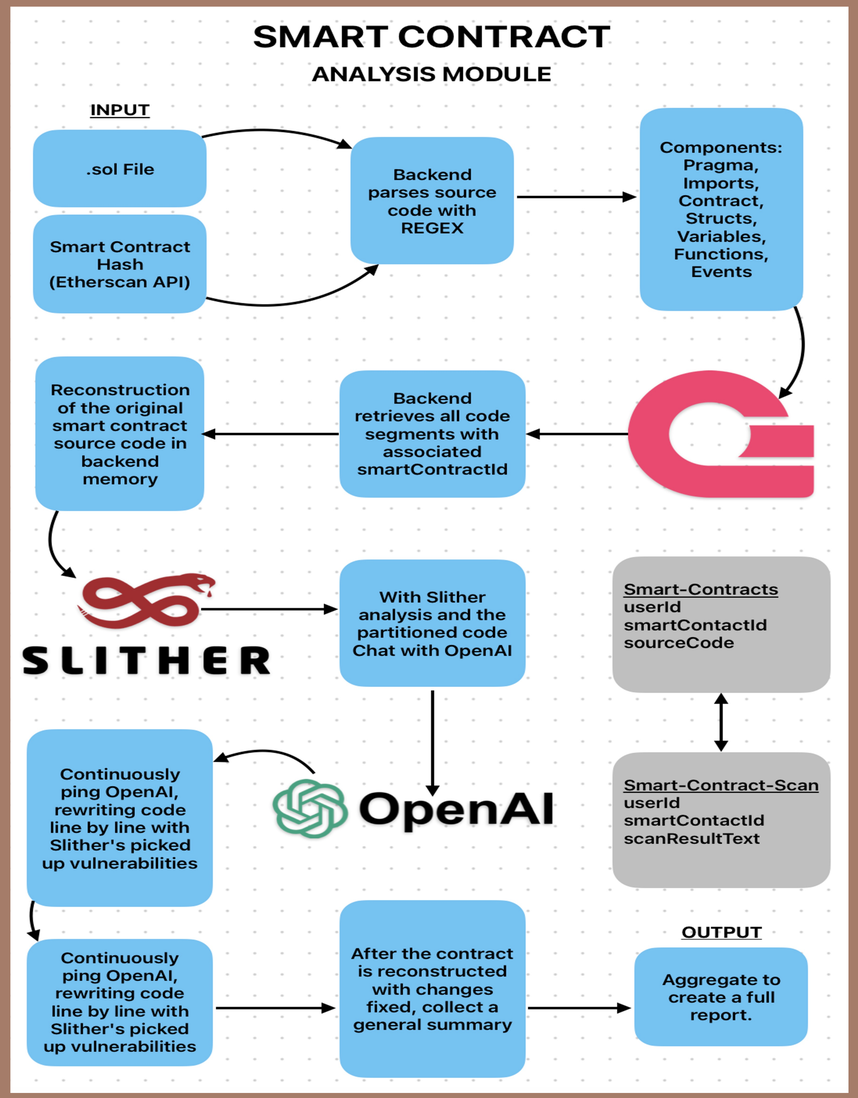
Abstract

Using OpenAI models, we designed a Python backend module to diagnose issues and rewrite smart-contracts.

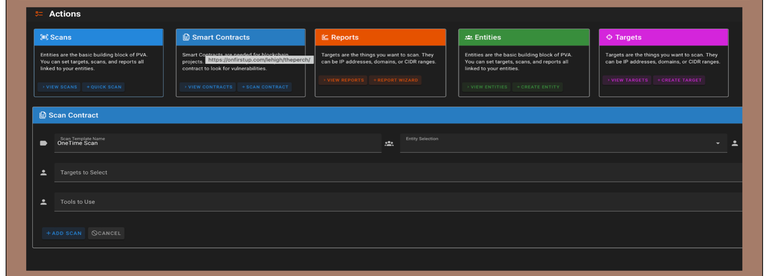
Motivation

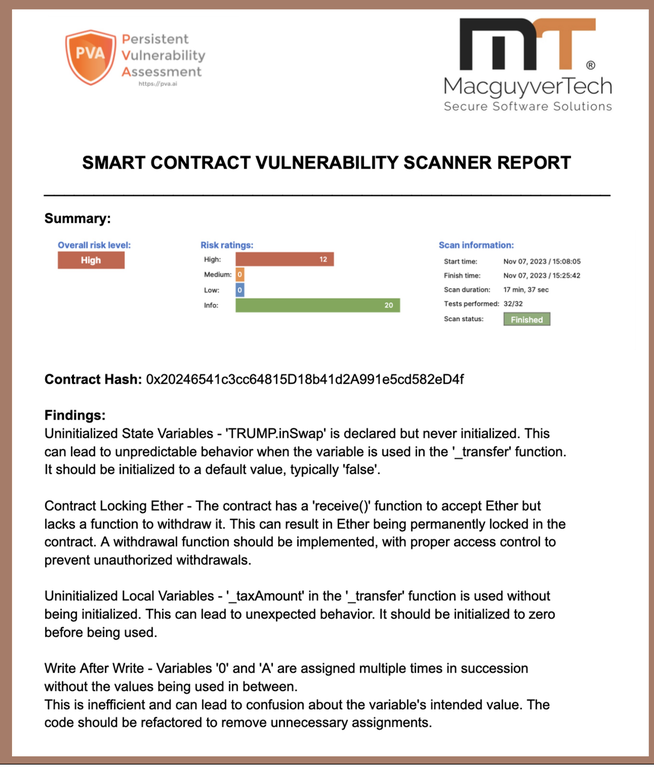
Smart Contracts are immutable digital contracts stored on Ethereum. Bugs / Vulnerabilities can lead to severe exploitation risks. Ensuring the reliability and resiliency of the smart contract on the decentralized blockchain is crucial.





Results & Conclusions





Persistent Vulnerability Assessment
https://pva.ai

MacguyverTech
Secure Software Solutions

SMART CONTRACT VULNERABILITY SCANNER REPORT

Summary:

Overall risk level: High

Risk ratings: High: 12; Medium: 0; Low: 0; Info: 20

Scan information:
Start time: Nov 07, 2023 / 15:08:05
Finish time: Nov 07, 2023 / 15:25:42
Scan duration: 17 min, 37 sec
Tests performed: 32/32
Scan status: Finished

Contract Hash: 0x20246541c3cc64815D18b41d2A991e5cd582eD4f

Findings:
Uninitialized State Variables - 'TRUMP.inSwap' is declared but never initialized. This can lead to unpredictable behavior when the variable is used in the '_transfer' function. It should be initialized to a default value, typically 'false'.

Contract Locking Ether - The contract has a 'receive()' function to accept Ether but lacks a function to withdraw it. This can result in Ether being permanently locked in the contract. A withdrawal function should be implemented, with proper access control to prevent unauthorized withdrawals.

Uninitialized Local Variables - '_taxAmount' in the '_transfer' function is used without being initialized. This can lead to unexpected behavior. It should be initialized to zero before being used.

Write After Write - Variables '0' and 'A' are assigned multiple times in succession without the values being used in between.
This is inefficient and can lead to confusion about the variable's intended value. The code should be refactored to remove unnecessary assignments.

LEHIGH UNIVERSITY

MacguyverTech