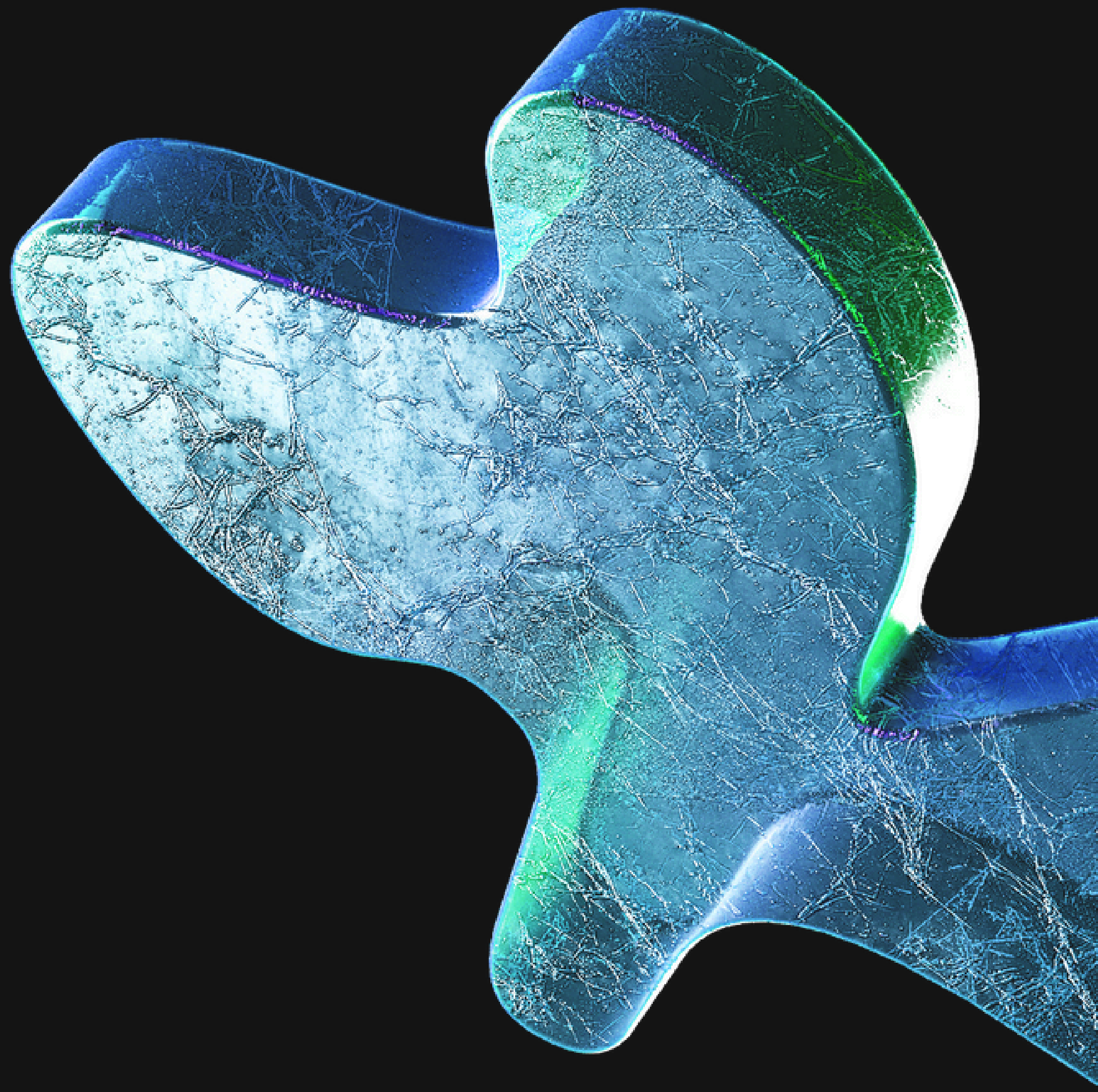


MEV Sentinel: Real-time MEV Bot Detection and Protection Dashboard

Detecting and mitigating front-running, sandwich, and other MEV attacks

evolvyn
mateena sadaf
khushi kalinge
nhikhitha m
Shamita Ramesh
Sahana G A

Problem Statement

- MEV (Maximal Extractable Value) bots exploit DeFi traders and NFT buyers by front-running with higher gas fees.

- Leads to slippage, unfair trades, and financial losses for regular users.

- Need real-time detection and prevention solution.

Project Goals

- Detect suspicious mempool behavior (sandwich attacks, front-running, MEV patterns).
- Visualize flagged transactions, impacted users, and estimated slippage losses in real-time.
- Optionally integrate private transaction relayer to safely submit transactions.
- Bonus: Provide simulation mode for users to test transactions pre-submission for MEV risks.

Technologies Used

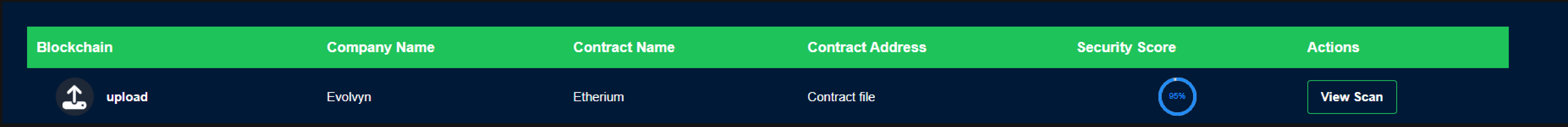
Smart Contracts: Solidity with optimizations and secure patterns

Blockchain: Ethereum (or target chain)

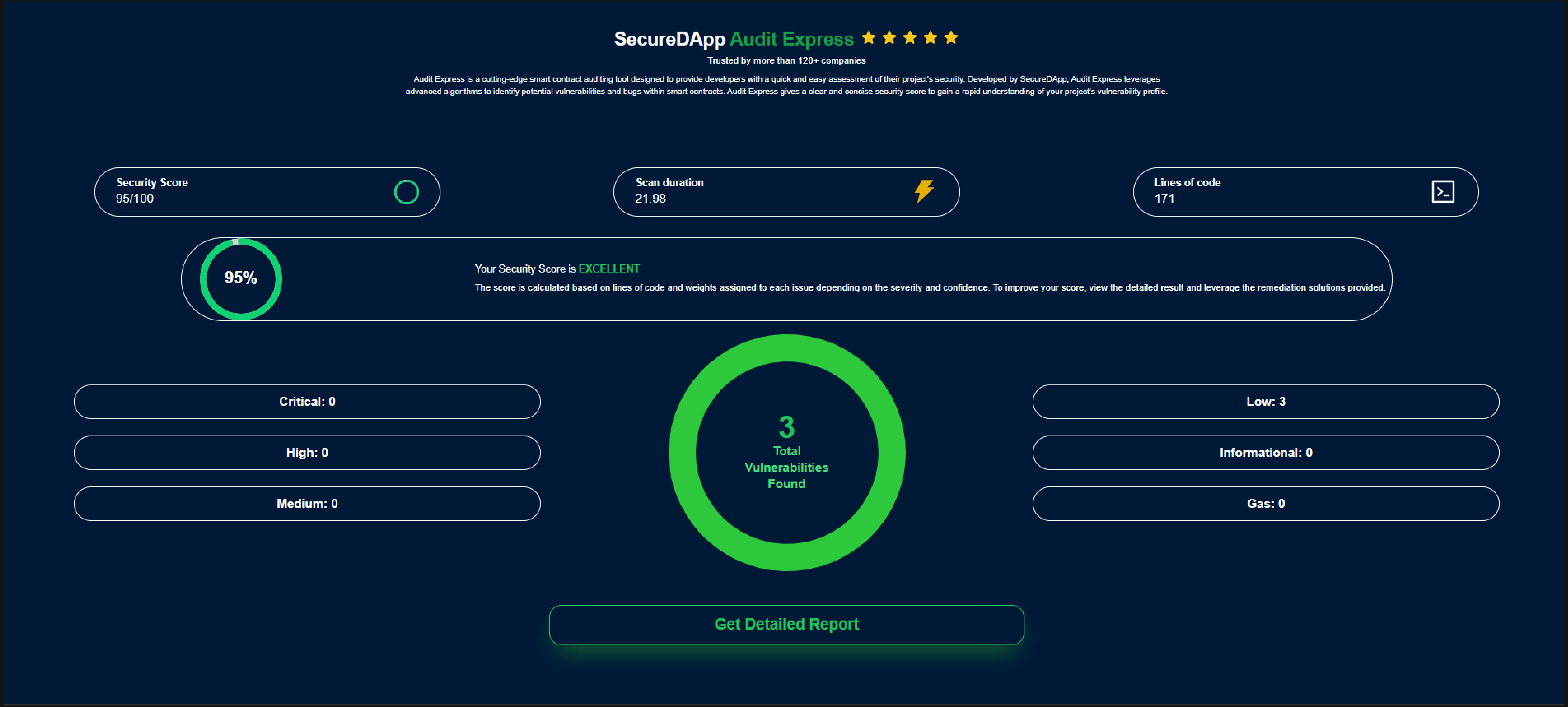
Smart Contracts: Solidity with optimizations and secure patterns

Tools: Flashbots relayer (optional), Etherscan API for transaction details

Frontend: React (based on screenshots)



Blockchain	Company Name	Contract Name	Contract Address	Security Score	Actions
upload	Evolvyn	Etherium	Contract file	95%	View Scan



SecureDApp Audit Express ★★★★★

Trusted by more than 120+ companies

Audit Express is a cutting-edge smart contract auditing tool designed to provide developers with a quick and easy assessment of their project's security. Developed by SecureDApp, Audit Express leverages advanced algorithms to identify potential vulnerabilities and bugs within smart contracts. Audit Express gives a clear and concise security score to gain a rapid understanding of your project's vulnerability profile.

Security Score
95/100

Scan duration
21.98

Lines of code
171

95%

Your Security Score is EXCELLENT

The score is calculated based on lines of code and weights assigned to each issue depending on the severity and confidence. To improve your score, view the detailed result and leverage the remediation solutions provided.

Critical: 0

High: 0

Medium: 0

3
Total Vulnerabilities Found

Low: 3

Informational: 0

Gas: 0

Smart Contract Development and Audit of Telecommunications

- Reviewed and optimized provided Solidity contract to eliminate high-severity vulnerabilities.
- Improved AuditExpress score significantly (mention before/after if available).
- Refactored code for efficiency and security best practices.
- Flattened contract for audit submission.

Key Features - Dashboard Overview

REAL-TIME MEMPOOL MONITORING FOR PENDING TRANSACTIONS AND GAS PRICE.

TOP MEV THREAT DETECTION WITH ESTIMATED EXTRACTION VALUE AND RISK LABELS.

MEV BOTS AND SANDWICH ATTACK ATTEMPTS TRACKED LIVE.

Key Features – Attack Detection

- DETECTION OF FRONT-RUNNING, SANDWICH ATTACKS, FLASH LOANS, AND SLIPPAGE EXPLOITS.
- 24-HOUR ATTACK TYPE DISTRIBUTION GRAPH FOR INSIGHTS INTO ATTACK PATTERNS.
- CLEAR METRICS ON DETECTED ATTACKS AND RISK LEVELS.

Conclusion and Future Work

- Achieved effective real-time MEV attack detection and user protection dashboard.

- Smart contract robustness enhanced through audit and optimization.

- *Future enhancements*:
- Integration of private relayer like Flashbots
- Expanded attack detection types
- Automated mitigation or blocking mechanisms