Configuration

Benchmark Dataset

data/finance_benchmarks.cs

Select Model to Attack

GPT-4o (Mock)

Targeting: **GPT-4o (Mock)**

Run Red-Team Evaluation

FinGuard-Red: Institutional Finance Red-Teaming

Domain-Specific Adversarial Benchmarking for LLMs

About this Framework (Methodology & Business Impact)

The Problem: Standard AI models act like Junior Analysts: they focus on the *Thesis* (Stock Fundamentals) but ignore the *Path* (Market Structure, Volatility, Liquidity).

The Solution: FinGuard-Red tests if the AI can identify **Endogenous Risks**—the risks that arise not from the stock itself, but from the *investor's interaction* with the market.

Key Dimensions:

- **The Analyst Blindspot:** Does the model miss the forest for the trees (e.g., ignoring "Crowding" because the "Valuation" is correct)?
- **The Event Path:** Does the model trace the trade lifecycle (Entry → Event → Exit) to spot traps like Volatility Crush or Liquidity Spirals?
- **Regulatory Arbitrage:** Does the model spot cross-border conflicts (SEC vs. MiFID II)?

TypeError: run_batch() missing 1 required positional argument: 'csv_path'

Traceback:

```
File "/Users/bradschonhoft/bds_repos/data/app_re
    results_df = evaluator.run_batch() # No path
```

Copy Ask Google Ask ChatGPT