

# Instruction-Tuned Llama3 and DeepSeek-R1 Robustness Against Adversarial Code Security Perturbations

Assignee Research

June 4, 2026

## Abstract

This report synthesises findings from 11 peer-reviewed papers addressing the following research question: How does the robustness of instruction-tuned Llama3 compare to Deepseek R1 against taxonomy-specific adversarial perturbations in code security benchmarks. 5 claims were extracted from source literature; 5 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 5.4/10. This report is a machine-generated literature synthesis and does not constitute original research.

## 1 Introduction

This paper examines: GPT-4 Technical Report. Research question: How does the robustness of instruction-tuned Llama3 compare to Deepseek R1 against taxonomy-specific adversarial perturbations in code security benchmarks?.

## 2 Methodology

Systematic literature search across multiple databases yielded 11 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 5.4/10.

## 3 Results

11 papers retrieved. 5 claims extracted; 5 independently verified. Quality review score: 5.4/10.

## 4 Limitations

This report is a machine-generated literature synthesis and does not constitute original research. Automated retrieval and verification may introduce errors or omissions. Review scores reflect automated assessment, not human peer review. Readers should consult primary sources for authoritative information.

## 5 Extracted Claims

Claim	Verified	Confidence
Large Language Models (LLMs) suffer from inherent stochasticity, limiting their utility in high-stakes enterprise enviro	✓	0.41
The MFOUR Vibe Framework (MVF) is a platform-agnostic architectural standard that transforms probabilistic natural langu	✓	0.43
The MFOUR Vibe Framework (MVF) comprises a five-layer topology, including the Kernel Identity, Synaptic Routing, Interfa	✓	0.37
The Vibe Integrity Score (VIS) is a quantitative metric for evaluating the structural adherence of generative outputs.	✓	0.36
The MFOUR Vibe Framework (MVF) provides the foundational schema and logic protocols for building 'Glass Box' AI systems	✓	0.44

## References

- <https://doi.org/10.2196/53008>
- <https://doi.org/10.4230/lipics.cosit.2024.11>
- <https://doi.org/10.48550/arxiv.2403.05530>