

**Critique of a research article
regarding the research objectives.**

Prepared by

ALI MMADI, PhD student - Midocean University



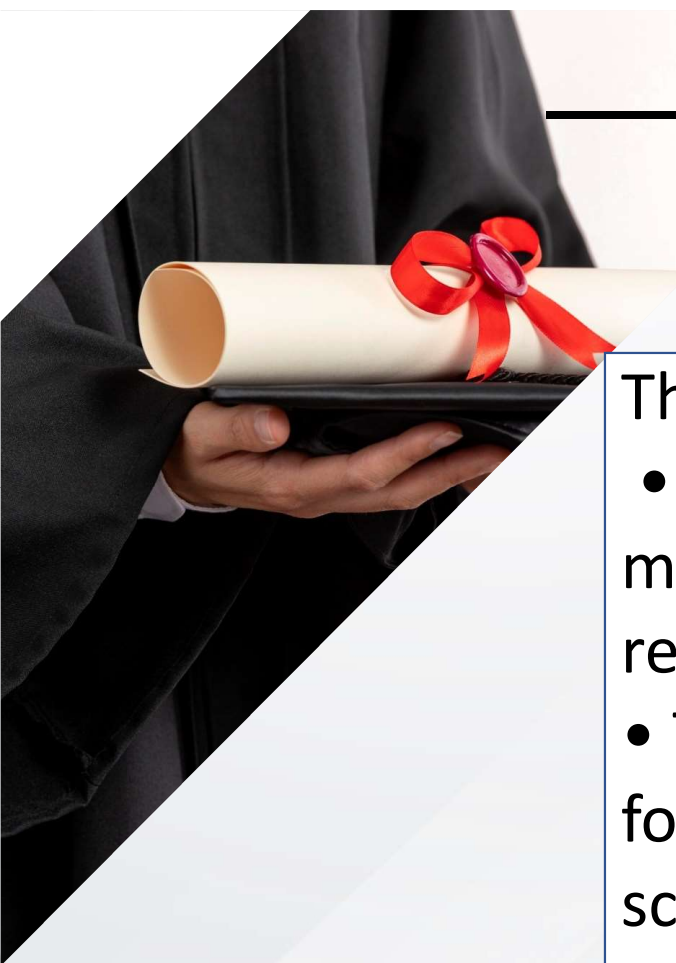
Literary Criticism (1)

Task 4

Offensive AI: Enhancing Directory Brute-Forcing Attack with the Use of Language Models" (Castagnaro et al., 2024)

INTRODUCTION

This assignment 4 offers a critical analysis of the research objectives in the article titled: "Offensive AI: Enhancing Directory Brute-Forcing Attack with the Use of Language Models," published in April 2024 on arXiv by Castagnaro, Conti, and Pajola. This article explores how language models can be used to enhance brute force attacks in web environments, particularly through intelligent directory enumeration.



Presentation of the Research Objectives

The article sets several clear objectives:

- To study the potential of large language models to dynamically generate URL paths from real data,
- To improve the speed and efficiency of brute force attacks in web penetration testing scenarios,
- To compare the performance of this AI-assisted approach with that of traditional tools (such as DirBuster and Gobuster).

Analysis of the article's objectives

What is positive about the objectives

1) Clarity:

The author clearly states what he wants to demonstrate: using AI to make attacks more effective.

2) Relevance:

Current topic, combining offensive cybersecurity and artificial intelligence.

3) Innovation: The idea of using language models to intelligently generate directories is new.

4) Technical validity: The article compares the performance of AI with that of traditional tools like DirBuster or Gobuster.method.

✗ Limitations or weaknesses of the objectives

1) No clear separation between types of objectives

:General and specific objectives are not separated. For example: there is a lack of explicit wording like:

General objective: improve brute-force techniques
Specific objective 1: use LLMs to generate priority paths

1) 2) Little consideration of ethics:

The fact that this is an offensive attack is not sufficiently regulated. There is a lack of an objective to ensure responsible use of this technology (e.g., within the legal framework of pentesting or academic research).

Suggestions for improvement

Add a clear section in the introduction titled “Research Objectives.” Structure the objectives into two parts:

General: demonstrate the feasibility of an AI-optimized attack Specific:

- 1) Compare the performance of AI vs classical tools
- 2) Assess speed, detection rate, etc.
- 3) Propose ethical oversight measures Introduce an objective for critical or ethical reflection (essential in cybersecurity).

CONCLUSION

The research objectives are innovative and clear, directly related to the evolution of AI-assisted brute force techniques. The proposed approach opens up important perspectives, but would benefit from a more rigorous structuring of the objectives and a more developed ethical dimension.

Bibliographic reference of the studied article

Castagnaro, C., Conti, M., & Pajola, L. (2024).
Offensive AI: Enhancing Directory Brute-Forcing Attack
with the Use of Language Models. arXiv preprint
arXiv:2404.14138.
<https://arxiv.org/abs/2404.14138>



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

