

الجمهورية الجزائرية الديمقراطية الشعبية  
PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA  
وزارة التعليم العالي والبحث العلمي  
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH  
المدرسة العليا للإعلام الآلي - 80 ماي 5491 - بسيدي بلعباس  
HIGHER SCHOOL OF COMPUTER SCIENCE -8 MAI 1945- SIDI BEL ABBÈS  
(ESI-SBA)



## MASTER'S THESIS

To obtain a **master's degree**  
Stream: **Computer Science**  
Speciality: **Information Systems Engineering (ISI)**

---

# STATIC ANALYSIS FOR EARLY DETECTION OF VULNERABILITIES IN SOURCE CODE BASED ON ARTIFICIAL INTELLIGENCE

---

Presented by:  
Mr Remmane Mohamed

Presented on: **30/09/2025**

In front of a committee composed of :

Dr. Belfedhal Alaa Eddine	Supervisor
Dr. Serhane Oussama	Co-Supervisor
Dr. Chikh Asma	President
Dr. Neggaz Imene	Examiner

Academic year  
2024/2025

# Abstract

Software security has become a critical concern as modern applications grow increasingly complex and interconnected. Traditional static analysis tools, while widely adopted for detecting vulnerabilities in source code, often suffer from high false-positive rates and limited ability to capture deep semantic relationships in programs.

This thesis provides both the necessary background and a comprehensive review of recent research efforts in this domain, with a particular focus on Java source code. It first introduces the foundations of static code analysis, outlining its principles, strengths, and limitations and examines program representations such as Abstract Syntax Trees (ASTs), Control Flow Graphs (CFGs), and Data Flow Graphs (DFGs), alongside advanced neural architectures including Graph Neural Networks (GNNs), which aim to model both syntactic and semantic dependencies in code. Through a comparative analysis of existing works, the study highlights their strengths, limitations, and performance across commonly used benchmark datasets.

The findings reveal that hybrid code representations and graph-based deep learning models offer promising results, yet challenges persist regarding dataset quality, model generalization, reproducibility, and the gap between academic prototypes and industrial deployment. By synthesizing and critically evaluating the state of the art, this thesis contributes to a deeper understanding of current progress in automated vulnerability detection and outlines directions for future research.

**Keywords:** Static Code Analysis, Vulnerability Detection, AST, DFG, CFG, DL, ML, Software Vulnerability Detection, Graph Neural Networks (GNNs), Java Security.