



INSTITUT NATIONAL DES SCIENCES APPLIQUÉES

Transformer-based Vulnerability Detection in Code at EditTime : Zero-shot, Few-shot, or Fine-tuning ?

Étude Bibliographique

Auteurs de l'article :

Aaron CHAN
Anant KHARKAR
Roshanak ZILOUCHIAN
MOGHADDAM
Yevhen MOHYLEVSKYY
Alec HELYAR
Eslam KAMAL
Mohamed ELKAMHAWY
Neel SUNDARESAN

Responsable du module :

Pascal BERTHOMÉ

Relecteurs :

Prénom NOM

Prénom NOM

Auteurs de l'étude :

Mohamed MOKRANI
Lamiaa BENEJMA
Mouna EL ARRAF
Thomas AUBIN

Résumé en quelques lignes du projet

Mots-clés : Transformeurs, Vulnérabilités logicielles, Détection de vulnérabilités

16 mars 2025

Résumé

Draft

Table des matières

Résumé	1
Introduction	6
I Contexte et problématique	1
I Présentation du domaine et des enjeux en cybersécurité	2
I.1	2
I.1.1	2
I.1.1.1	2
II Importance de la détection des vulnérabilités	4
II.1	4
II.1.1	4
II.1.1.1	4
II.2	5
III Problèmes des méthodes classiques et défis posés par la détection en temps réel	6
III.1	6
III.1.1	6
III.1.1.1	6
II Apports scientifiques de l'article	7
IV Explication des trois approches (Zero-shot, Few-shot, Fine-tuning)	8
IV.1	8
IV.1.1	8
IV.1.1.1	8
V Présentation des modèles utilisés (CodeBERT, Code-Davinci-002, Text-Davinci-003)	9
V.1	9
V.1.1	9
V.1.1.1	9
VI Expérimentations et résultats observés	10
VI.1	10
VI.1.1	10
VI.1.1.1	10
III Impacts et applications	11
VII Améliorations du développement logiciel :	12
VII.1 Des outils de détection classique : quel point de départ ?	12
VII.1.1	12
VII.1.1.1	12
VII.1.2 Détection de vulnérabilités par le Deep Learning : un bref état de l'art	12
VII.1.3 Cas particulier du code généré par des LLM	12
VII.2 Correction et complétion pendant la phase de développement : promesses et difficultés rencontrées	12

VII.3	Interprétation des métriques de classification présentées	12
VIII	Études de cas et intégration dans un IDE	13
VIII.1	Déploiement des modèles sur VSCode	13
VIII.1.1	Méthodologie inhérente au déploiement	13
VIII.1.2	Résultats obtenus	13
VIII.1.3	Cas de figure non ou partiellement couverts par l'étude	13
IX	Conséquences pour l'industrie et la recherche en cybersécurité :	14
IX.1	14
IX.1.1	14
IX.1.1.1	14
IV	Analyse critique et perspectives	15
X	Problèmes éthiques et limites des modèles d'IA	16
X.1	16
X.1.1	16
X.1.1.1	16
XI	Biais, responsabilité et risques d'utilisation malveillante	17
XI.1	17
XI.1.1	17
XI.1.1.1	17
XII	Suggestions d'améliorations et directions futures	18
XII.1	18
XII.1.1	18
XII.1.1.1	18
Conclusion		18
Annexe 1 :		1
Annexe 2 :		2
V	Bibliographie	3

Table des figures

I.1	Exemple de figure	2
I.2	Exemple avec plusieurs figures	3

Draft

Liste des tableaux

I.1	Exemple de tableau	3
I.2	Exemple de tableau coloré	3

Draft

Table des Équations

I.1 Une équation simple 2

Draft

Table des éléments de code

I.1	Un code Python	2
-----	--------------------------	---

Draft

Introduction

Draft

Première partie

Contexte et problématique

Chapitre I

Présentation du domaine et des enjeux en cybersécurité

I.1

I.1.1

I.1.1.1

$$a + b = c$$

(I.1)



FIGURE I.1 – Exemple de figure

```
1 print("This line will be printed.")  
2 print("Another line to print.")
```

Listing I.1 – Un code Python

Ceci est un exemple d'encadré. Il sert à mettre en évidence des parties importantes du rapport

Donnée

TABLE I.1 – Exemple de tableau

Tâche				
Donnée			0	0

TABLE I.2 – Exemple de tableau coloré



FIGURE I.2 – Exemple avec plusieurs figures

Chapitre II

Importance de la détection des vulnérabilités

II.1

II.1.1

II.1.1.1

Draft

II.2

some text

Draft

Chapitre III

Problèmes des méthodes classiques et défis posés par la détection en temps réel

III.1

III.1.1

III.1.1.1

Draft

Deuxième partie

Apports scientifiques de l'article

Chapitre IV

Explication des trois approches (Zero-shot, Few-shot, Fine-tuning)

IV.1

IV.1.1

IV.1.1.1

Draft

Chapitre V

Présentation des modèles utilisés (CodeBERT, Code-Davinci-002, Text-Davinci-003)

V.1

V.1.1

V.1.1.1

Draft

Chapitre VI

Expérimentations et résultats observés

VI.1

VI.1.1

VI.1.1.1

Draft

Troisième partie
Impacts et applications

Chapitre VII

Améliorations du développement logiciel :

VII.1 Des outils de détection classique : quel point de départ ?

VII.1.1

VII.1.1.1

VII.1.2 Détection de vulnérabilités par le Deep Learning : un bref état de l'art

VII.1.3 Cas particulier du code généré par des LLM

VII.2 Correction et complétion pendant la phase de développement : promesses et difficultés rencontrées

VII.3 Interprétation des métriques de classification présentées

Chapitre VIII

Études de cas et intégration dans un IDE

VIII.1 Déploiement des modèles sur VSCode

VIII.1.1 Méthodologie inhérente au déploiement

VIII.1.2 Résultats obtenus

VIII.1.3 Cas de figure non ou partiellement couverts par l'étude

Draft

Chapitre IX

Conséquences pour l'industrie et la recherche en cybersécurité :

IX.1

IX.1.1

IX.1.1.1

Draft

Quatrième partie
Analyse critique et perspectives

Chapitre X

Problèmes éthiques et limites des modèles d'IA

X.1

X.1.1

X.1.1.1

Draft

Chapitre XI

Biais, responsabilité et risques d'utilisation malveillante

XI.1

XI.1.1

XI.1.1.1

Draft

Chapitre XII

Suggestions d'améliorations et directions futures

XII.1

XII.1.1

XII.1.1.1

Draft

Conclusion

Annexe 1 :

Draft

Annexe 2 :

Draft

Cinquième partie

Bibliographie