

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

Auteurs de l'étude : Mohamed Mokrani Lamiaa Benejma Mouna El Arraf Thomas Aubin Responsable du module :
Pascal Berthomé
Relecteurs :
Prénom Nom
Prénom Nom

Résumé en quelques lignes du projet **Mots-clés :** Transformeurs, Vulnerabilités logicielles, Détection de vulnérabilités



Table des matières

Résumé	1
Introduction	6
I Contexte et problématique	1
I Présentation du domaine et des enjeux en cybersécurité I.1	2 2 2 2
II Importance de la détection des vulnérabilités II.1	4 4 4 5
III Problèmes des méthodes classiques et défis posés par la détection en temps réel III.1	66
II Apports scientifiques de l'article	7
IV Explication des trois approches (Zero-shot, Few-shot, Fine-tuning) IV.1	8 8 8
V Présentation des modèles utilisés (CodeBERT, Code-Davinci-002, Text-Davinci-003) V.1 V.1.1 V.1.1.1 VI Expérimentations et résultats observés VI.1 VI.1.1	9 9 9 10 10 10
III Impacts et applications	11
VII Améliorations du développement logiciel : VII.1 Des outils de détection classique : quel point de départ ?	12 12 12 12

VII.3 Interprétation des métriques de classification présentées	12
VIII Études de cas et intégration dans un IDE VIII.1 Déploiement des modèles sur VSCode	13 13
IX Conséquences pour l'industrie et la recherche en cybersécurité :	14
	14
IX.1.1 IX.1.1.1 IX.1.1.1	
IV Analyse critique et perspectives	15
X Problèmes éthiques et limites des modèles d'IA	16
X.1	16
X.1.1 X.1.1.1 X.1.1.1	
XI Biais, responsabilité et risques d'utilisation malveillante	17
XI.1 XI.1.1	17 17
XI.1.1.1	17
XII Suggestions d'améliorations et directions futures	18
XII.1	18
XII.1.1	
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



Liste des tableaux

I.1	Exemple de tableau
	Exemple de tableau coloré



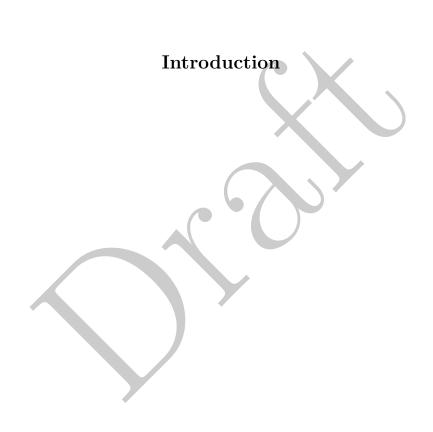
Table des Équations



Table des éléments de code

I.1 Un code Python	ก
1.1 Un code Evinon	 . /





Première partie Contexte et problématique

Chapitre I

Présentation du domaine et des enjeux en cybersécurité

I.1

I.1.1

I.1.1.1





 $\label{eq:figure} \mbox{Figure I.1 - Exemple de figure}$

```
print("This line will be printéd.")
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

 ${\it TABLE~I.1-Exemple~de~tableau}$

Tâche			
Donnée		0	0

Table I.2 – Exemple de tableau coloré

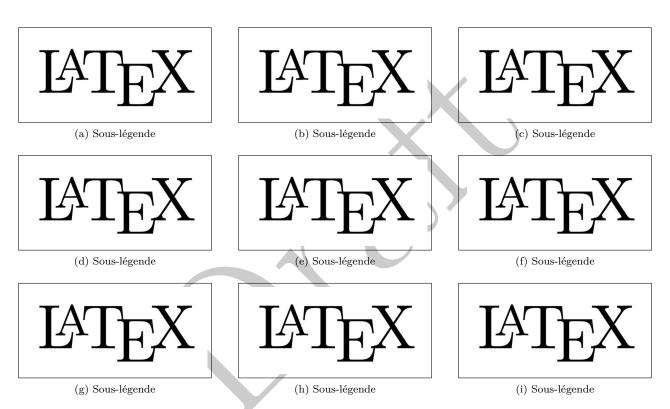


FIGURE I.2 – Exemple avec plusieurs figures

Chapitre II

Importance de la détection des vulnérabilités

II.1

II.1.1

II.1.1.1



II.2

some text



Chapitre III

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

III.1 III.1.1 III.1.1.1

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



Chapitre V

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

V.1 V.1.1

V.1.1.1



Chapitre VI

Expérimentations et résultats observés

VI.1

VI.1.1

VI.1.1.1



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

Chapitre IX

Conséquences pour l'industrie et la recherche en cybersécurité :

IX.1

IX.1.1

IX.1.1.1



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



Chapitre XI

Biais, responsabilité et risques d'utilisation malveillante

XI.1

XI.1.1

XI.1.1.1



Chapitre XII

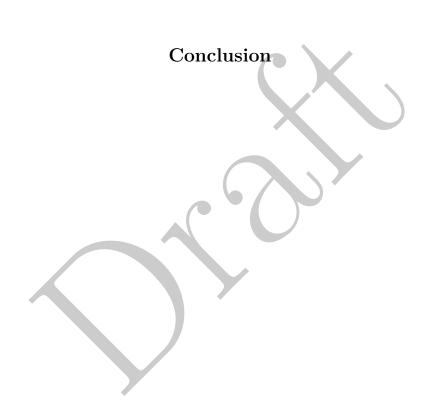
Suggestions d'améliorations et directions futures

XII.1

XII.1.1

XII.1.1.1





Annexe 1:



Annexe 2:



Cinquième partie Bibliographie