AVIS DE SOUTENANCE DE THESE

Le Doyen de la Faculté des Sciences Dhar El Mahraz –Fès – annonce que

Mme(elle) **LAMRANI ALAOUI Rokia**
Soutiendra : **le Vendredi 12/01/2024** à **14H45**
Lieu : ***FSDM – Centre Visioconférence***

Une thèse intitulée :

Contributions to Improving Web Applications Security Using Deep Learning

En vue d'obtenir le ***Doctorat***

FD : ***Sciences et Technologies de l'Information et de la Communication***
Spécialité : ***Informatique***

Devant le jury composé comme suit :

Nom et prénom	Etablissement	Grade	Qualité
Pr YAHYAOUY Ali	Faculté des Sciences Dhar El Mahraz, Fès	PES	Président
Pr OUANAN Mohammed	Faculté des Sciences, Meknès	PES	Rapporteur & Examinateur
Pr CHAOUI Nour El Houda	Ecole Supérieure de Technologie, Kénitra	PES	Rapporteur & Examinateur
Pr RIFFI Jamal	Faculté des Sciences Dhar El Mahraz, Fès	PH	Rapporteur & Examinateur
Pr BOUMHIDI Jaouad	Faculté des Sciences Dhar El Mahraz, Fès	PES	Examinateur
Pr LOQMAN Chakir	Faculté des Sciences Dhar El Mahraz, Fès	PES	Examinateur
Pr SABRI My Abdelouahed	Faculté des Sciences Dhar El Mahraz, Fès	PES	Examinateur
Pr SATORI Hassan	Faculté des Sciences Dhar El Mahraz, Fès	PES	Examinateur
Pr NFAOUI El Habib	Faculté des Sciences Dhar El Mahraz, Fès	PES	Directeur de thèse

Résumé :

Les organisations et les entreprises sont maintenant plus que jamais concernées par l'atténuation des cyberattaques. En effet, une cyberattaque réussie peut causer à l'entreprise une perte financière importante et une atteinte à sa réputation.

De nos jours, les applications web sont omniprésentes dans notre vie quotidienne et sont utilisées dans les domaines de l'éducation, de la santé et de la finance. Elles présentent cependant différents inconvénients liés à la sécurité et à la protection des données personnelles et des biens publics. En effet, dans une enquête menée en 2019, il a été constaté que 9 applications web sur 10 sont vulnérables, et que des violations de données sensibles sont possibles sur 68% des applications web, et que les intrusions réseau sont provoquées par des activités non autorisées d'accès aux serveurs web dans 8% des cas. Les techniques traditionnelles de renforcement de la sécurité web, telles que les outils d'analyse de code statiques et dynamiques et les pare-feu d'applications web basés sur des signatures, ne peuvent pas détecter les attaques Zero-Day et ne peuvent pas non plus corréler et analyser les événements pour détecter les chaˆınes d'attaques. De plus, les pare-feu d'applications web doivent être régulièrement mis à jour avec la signature de nouvelles vulnérabilités web. Ainsi, l'utilisation de systèmes de détection d'intrusion Web basés sur des modèles d'apprentissage automatique (Machine Learning) et d'apprentissage profond (Deep Learning) est une solution prometteuse pour une détection efficace des attaques web. L'objectif principal de cette thèse est de proposer des approches basées sur le Deep Learning pour détecter les attaques web dans les requêtes HTTP.

À cette fin, nous avons suivi les étapes suivantes :

1. Nous avons mené une revue systématique de la littérature (SLR) pour avoir un aperçu précis des travaux de recherche sur les approches basées sur le Deep Learning pour la détection des attaques web dans les requêtes HTTP.
2. Sur la base de l'analyse des résultats obtenus grâce au SLR, nous avons proposé une méthode de Deep Learning pour détecter les attaques web, et une autre méthode de Deep Learning pour détecter une attaque web spécifique, à savoir l'attaque Cross Site Scripting (XSS). La première méthode a détecté les attaques Web avec une précision de 80%, tandis que la seconde méthode a détecté les attaques XSS avec une précision de 99%.
3. Ensuite, nous avons étudié les attaques adverses (Adversarial attacks) contre des modèles de détection d'attaques Web basés sur le Deep Learning. En effet, les modèles de Deep Learning sont intrinsèquement vulnérables aux attaques adverses qui visent à tromper le modèle de détection en classant mal les requêtes HTTP malveillantes. Ainsi, nous avons proposé une approche automatique de génération d'attaques adverses afin d'améliorer la défense des modèles de détection d'attaques web contre les attaques adverses. Nous avons également fourni quelques lignes directrices pour le développement de modèles de détection capables de se défendre contre les attaques adverses dans le contexte particulier de la détection des attaques Web.

Mots clés : Applications Web, Sécurité Web, Attaques Web, Vulnérabilités Web, Deep Learning, Classification textuelle

CONTRIBUTIONS TO IMPROVING WEB APPLICATIONS SECURITY USING DEEP LEARNING

Abstract :
Organizations and enterprises are more concerned now than never before about the mitigation of cyber-attacks. Indeed, a successful cyber-attack can cause the enterprise an important financial loss and a reputation damage.

Nowadays, web applications are omnipresent in our daily lives being used in education, healthcare, and financial institutions. However, they present different drawbacks related to the security and protection of personal data and public goods. Indeed, in a survey conducted in 2019, it was found that 9 of 10 web applications are vulnerable, and that sensitive data breaches are possible on 68\% of web applications, and that network intrusions are caused by unauthorized access to web servers in 8\% of cases. Traditional web security techniques, such as static and dynamic code analysis tools and Web Application Firewalls (WAF), cannot detect zero-day attacks and cannot correlate and analyze events for detection of attacks chains. Moreover, WAFs should regularly be updated with the signature of new web vulnerabilities.Thus, using web intrusion detection systems based on machine learning and deep learning models is a promising solution to efficient detection of web attacks. In this thesis, we proposed deep learning based approaches for detecting web attacks in HTTP Web requests.

To this end, we followed the next steps:

1- We conducted a Systematic Literature review to have an accurate overview of research works on Deep Learning based approaches for the detection of web attacks in HTTP Web requests.

2- Based on the analysis of the results obtained from the SLR study, we proposed a Deep Learning method for detecting web attacks, and another Deep Learning method for detecting a specific Web attack.

3- Afterwards, we studied Adversarial attacks against Deep Learning based web attacks detection models. Indeed, Deep Learning models are inherently vulnerable to adversarial attacks, which aim to deceive the detection model into mis-classifying malicious HTTP web requests. Thus, it is important to evaluate the robustness of the detection model against adversarial attacks before its deployment to production in real web applications. To this end, we proposed an automatic approach for the generation of adversarial attacks, in order to improve the defense of Web attacks detection models against adversarial attacks. We also provided some guidelines to the development of detection models that can defend against adversarial attacks in the particular context of web attacks detection.

***Keywords*:** Web Applications, Web Security, Web Attacks, Web Vulnerabilities, Deep Learning, Text Classification**.**