REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

N° d'ordre : .....

UNIVERSITE Mohammed BOUDIAF-M 'sila
FACULTE DE MATHEMATIQUES ET D'INFORMATIQUE
Département d'Informatique

MEMOIRE de fin d'études
Présenté pour l'obtention du diplôme de MASTER
Domaine : Mathématiques et Informatique
Filière : Informatique
Spécialité : Réseaux
Par : Fateh DEBIH

SUJET

Implémentation d'un scanner de vulnérabilité web SQL injection

SAOUDI Lalia	**Université de M'sila**	**Rapporteur**
BOUAMAMA Salim	**Université de M'sila**	**Président**
ATHMANI	**Université de M'sila**	**Examinateur**

Promotion : 2014 /2015

Introduction Générale :

L'information et la probabilité sont deux aspects identiques, l'une ne peut être distinguée de l'autre, l'une ne peut être définit isolément de l'autre. La probabilité tente de quantifier l'incertitude dans un système et l'information est définit comme une incertitude sur le système étudié. L'aléatoire se présente comme les mathématiques qui servent à décrire l'information plutôt que de quantifier l'ignorance. Ceci suppose que l'aléatoire est une puissance informationnelle plutôt qu'un manque informationnelle. Une bonne recherche devrait intégrer l'aléatoire dans sa démarche plutôt que de l'éviter. Les algorithmes les plus efficaces sont probabilistes plutôt qu'exactes. Une observation digne d'une profonde réflexion.

La sécurité de l'information œuvre à empêcher d'acquérir n'importe quelle information du système sujet de protection. Les mathématiques, les algorithmes et les mécanismes engagés pour mettre en œuvre un système de protection fiable et efficace devraient inclure et être définit suivant une manière aléatoire et probabiliste.

Le web est le système informationnel objet de cette étude. Le but est de concevoir une méthode de détection de vulnérabilité causée par certaines attaques spécifiques qui sont les injections SQL. Ce dernier est le type d'attaque le plus dangereux qui menace le web d'après l'OWASP. Un scanner web est le produit logiciel qui parcours un site web, définir des points d'entrées des données, et tester leurs éventuelles possibilités d'être exploiter par une injection SQL, qui détecte la vulnérabilité.

La démarche de conception de notre approche avance une question clef qui est : comment définir l'information portée par les pages web ? , et delà concevoir une méthode bénéficiant des propriétés aléatoires pour obtenir une méthode fiable, efficace et performante de détection d'injection SQL. La simplicité était le choix adopté dans toutes les phases de la mise en œuvre de la méthode. Ceci s'est révélé très bénéfique et plus que surprenant.

Une information est un format et un contenu, le web attache une importance accentuée pour le format de la page. Cette dernière est délicatement formatée par un ensemble de tags, implémentée par un langage dit de mark up. L'aspect structure cerne le contenu telle une enveloppe conservant l'information. Cette étroite liaison entre les deux aspects suggère que la structure est dépendante du contenu, d'où la supposition que la structure peut ,à elle seule, décrire certaines propriétés de la page web d'une manière satisfaisante sinon convaincante.

Cette supposition est fondamentale dans notre démarche de la détection d'injection SQL. La page web est vue en faisant abstraction de son contenu et ne considérant que sa structure à base de tags.

L'approche développée est de type black box, s'articulant sur l'analyse des pages de réponse induites par des requêtes spécifiques. Le choix des requêtes est un paramètre clé de la détection de la vulnérabilité. Une observation profonde nous a conduites à la déduction qu'une requête aléatoire, et un ensemble de requêtes valides qui génèrent les pages de réponses suffisantes pour décider de la vulnérabilité de la page web.

L'analyse des pages de réponses encapsule l'intelligence de notre approche, la décision se base sur le principe de la comparaison entre les pages de réponses des requêtes valides avec la page de réponse de la requête aléatoire. La formule de la détection est la simple identification des séquences de tags des deux pages de réponses sujettes de la comparaison.

La simplicité de l'approche incite à l'examiner sérieusement, donc, une série d'expérimentations sur un site web constitué de pages web choisies de façon à représenter différents domaines est engagée. Pour avoir une bonne évaluation de notre scanner, il serait comparé à deux scanners des plus populaires, l'un commercial Acunetix d'IBM et l'autre d'OWASP académique.

La qualité des résultats sont surprenant plus que la simplicité de la méthode développée. L'efficacité et la performance de la méthode, nous motivent sérieusement à découvrir ses limites et comprendre les mathématiques sous-jacentes qui l'interprètent.

Plan du mémoire :

Le chapitre 1 expose le contexte de nos travaux : les applications web et leur sécurité. Dans la première partie, nous présentons les différentes architectures des applications web, les attaques qui menacent les applications web, et nous présentons aussi les attaques web « Les dix Risques de sécurité Applicatifs web les plus Critiques », et on va représenter l'injection SQL, les mécanismes d'injections et finalement les préjudices d'attaque par injection SQL.

Le chapitre 2 présente les moyens de protection détaillés des différentes techniques utilisées par les scanners des vulnérabilités Web existants, ainsi qu'une analyse critique de ces techniques.

Dans le chapitre 3 on va présenter une première contribution, qui porte sur la proposition d'une nouvelle approche pour la détection de vulnérabilités Web et du scanner de vulnérabilité qui a été développé, pour mettre en œuvre cette approche.et on l'architecture de notre scanner et leurs composants.

Dans le chapitre 4, comporte les expérimentaux et une analyse des résultats est comparés avec les approches utilisées par d'autres scanners de vulnérabilité (Acunetix et OWSP) à l'aide d'expérimentations ciblant des applications contenant des pages vulnérables différentes.

Conclusion Générale

Le web façonne progressivement notre mode de vie au point où on lui fait confiance pour nos informations les plus personnelles. Le mail et les réseaux sociaux sont des technologies qui s'imposent et enrichissent notre vie sociale et professionnelle en nous offrant de nouveaux styles de communication rapides, fiables et disponibles.

La sécurité des sites web est à considérer impérativement, ce n'est point une alternative. Le design d'un site web ne prend pas en compte la sécurité du site comme une notion basique. Cet état de fait, peut produire une application web vulnérable à certains types spécifiques d'attaques. Le plus dangereux d'entre eux est sans doute, l'injection SQL qui vise à extraire des données non autorisées de la base de données.

La découverte des pages vulnérables à l'injection SQL, est l'étape prémisse pour leur sécurisation. Le présent travail a abouti à la mise en œuvre d'une approche basée sur trois éléments : l'information de la page web considérée, les types de requêtes utilisés et le principe de la détection.

La structure de la page web qui n'est autre que la séquence des tags la constituant toute en faisant abstraction de son contenu est vue comme un potentiel informationnel suffisant pour représenter ce qui est nécessaire à considérer de la page pour notre système de détection de vulnérabilité.

La méthode est black box, d'où deux ensembles de pages de réponses sont générer pour l'analyse de détection. L'ensemble premier est constitué d'une seule requête aléatoire qui sera en quelque sorte un repère d'analyse pour un autre ensemble de pages de réponse généré par un certain nombre de requêtes valides choisis parmi les plus célèbres requêtes d'attaques SQL recensées par l'OWASP.

Les ingrédients étant préparés, l'analyse de vulnérabilité de la page web est formulée autour d'un principe simple réduit par l'identification parfaite des deux séquences de la page de réponse d'une requête valide avec celle de la page de réponse de l'unique requête aléatoire.

Une série sérieuse d'expérimentations a été élaborée pour analyser et valider l'efficacité et la performance de la méthode proposée. Deux scanners des plus populaires ont été utilisés pour renforcer la crédibilité des résultats avancés, l'un d'eux est professionnel, Acunetix d'IBM et l'autreest Académique d'OWASP. L'approche prouve une efficacité vérifiée face à ces deux scanners réputés.

La simplicité de l'approche face à sa haute efficacité et meilleure performance suggère une étude approfondie pour une meilleure compréhension.

Bibliographie

[1] Wikipédia, "**Application web**." http://fr.wikipedia.org/wiki/Application_web. Consulté le 25/05/2015

[2] J. Clarke, *SQL Injection Attacks and Defense*, Elsevier. USA: Chris Katsaropolous, 2012.

[3] Wikipédia, "SSL (Secure socket layer)," *Transport socket layer*. http://fr.wikipedia.org/wiki/Transport_Layer_Security. Consulté le 25/05/2015

[4] Wikipédia, "Open Web Application Security Project." http://fr.wikipedia.org/wiki/Open_Web_Application_Security_Project. Consulté le 25/05/2015

[5] OWASP, "Les dix Risques de sécurité Applicatifs web les plus Critiques." 2013.

[6] OWASP, "OWASP SQL injection." www.owasp.org.

[7] Serge Rufin Ngansop, "Étude et optimisation d'un nouveau mécanisme de sécurité pour protéger les applications Web contre les attaques par injection de code SQL," Université de Rennes 1, février 2009.

[8] Commentçamarche, "attaques par manipulation d'url." http://www.commentcamarche.net/contents/61-attaques-par-manipulation-d-url. Consulté le 25/04/2015

[9] MOHAMED YASSIN, "PROTECTION AUTOMATIQUE DES APPLICATIONS WEB CONTRE L'ATTAQUE PAR INJECTION SQL," UNIVERSITÉ DU QUÉBEC À MONTRÉAL, 2014.

[10] Zhendong Su ,Gary Wassermann, "The Essence of Command Injection Attacks in Web Applications," *POPL '06*, Charleston, South Carolina, USA., 11-Jan-2006

[11] Rim Akrout, "Analyse des vulnérabilités et évaluation de systèmes de détection d'intrusions pour les applications Web," Université de Toulouse, 2012.

[12] "Les procédure stockées." http://fr.wikipedia.org.

[13] "SQL injection protection." http://www.cgsecurity.org/Articles/sql_injection/.

[14] William G.J. Halfond and Alessandro Orso, "Preventing SQL Injection Attacks Using AMNESIA," *ICSE'06*, 20-May-2006.

[15] Russell A. McClure and Ingolf H. Krüger, "SQL DOM: Compile Time Checking of Dynamic SQL Statements," *ICSE'05*, University of California, San Diego, 15-May-2005.

[16] OWASP, "Les scanner web." www.owasp.org.

[17] Wikipédia, "Netbeans." http://fr.wikipedia.org/wiki/NetBeans. Consulté le 03-Juin-2015.

[18] Wikipédia, "Mysql. " http://fr.wikipedia.org/wiki/Mysql. Consulté le 03-Juin-2015.

[19] Wikipédia, "Appserv" ,http://fr.wikipedia.org/wiki/Appserv Consulté le 03-Juin-2015.

[20] Wikipédia, "PHP." [Online]. http://fr.wikipedia.org/wiki/PHP. Consulté le 03-Juin-2015.

[21] Wikipédia, "OWASP ZAP", http : //en.wikipedia.org/wiki/OWASP_ZAP, Consulté Le 05-Juin-2015.

[22] Acunetix, " Introduction to Acunetix Web Vulnerability Scanner",https://www.acunetix.com/support/docs/introduction/

الملخص:

مع تزايد خدمات وحجم استعمال الانترنت في العالم، ازداد التهديدات الأمنية في شبكة الانترنت بشكل كبير واحدة من نقاط الضعف تطبيقات الويب والأكثر خطورة هي حقن أوامرSQL ، والذي يتركز على إدراج جزء من أوامر SQL الخبيثة، ومن ثمة يقوم نظام إدارة قواعد البيانات تنفيذ هذه الأوامر، ويؤدي بالتالي إلى استعراض شامل لبيانات سرية، استنادا إلى الأبحاث الإحصائية فإن كان له تأثير على التعاملات البنكية والتجارية .العثور على حل مناسب لوقف أو التخفيف من هذا المشكل وإدخال تقنيات تمكننا من الكشف عن هذا الخطر المحدق، في هذا البحث استعرضنا واحدة من الكواشف التي من الممكن اكتشاف هذه الثغرات.

الكلمات المفتاحية :أمن المواقع، الثغرات، حقن أ وامرSQL ، تطبيقات الويب، أجهزة الفحص.

Résumé :

Avec l'augmentation et la propagation de l'utilisation de l'internet dans le monde, les menaces de sécurité dans l'Internet ont augmenté de façon spectaculaire. Parmi les points vulnérables de ces application web c'est l'injection SQL, qui se base sur l'insertion des requêtes malveillantes vers SGBD, ce denier exécute ces requêtes ce qui lui permet d'accéder à des données sensibles et confidentielles, après des recherches et des statistiques eu un impact sur les relations bancaires et d'affaires. Pour remédier ce problème nous avons proposé d'intégré des techniques, et présenté l'un des scanners qui permet de détecter ces failles de sécurité. Les résultats obtenus sont encourageants et peuvent être ouvrir des nouvelles perspectives.

Mots clé : Sécurité des application web, Failles, Injection SQL , Applications web, scanners

Abstract :

With the increase and the spread of Internet use in the world, security threats in the Internet increased dramatically. Among the vulnerabilities of the web application is SQL injection, which is based on the insertion of malicious requests to the DBMS, which executes these requests denier allowing him access to sensitive and confidential data, after research and statistics had an impact on banking and business relationships. To remedy this problem we proposed integrated techniques, and presented one of the scanners that can detect these vulnerabilities. The results are encouraging and may open new perspectives.

Key words: web application security, Rifts, SQL Injection, Web Applications, scanners .