الملخص

مع تزايد خدمات وحجم استعمال الانترنت في العالم تزايدت معه التهديدات و الخروقات الأمنية بشكل كبير،من بين نقاط ضعف تطبيقات الويب والأكثر خطورة هي حقن SQL الخبيثة حيث بمجرد إدخال هذه التعليمات الخبيثة تتسبب في استعراض شامل لبيانات سرية.

لذا فان الهدف من هده المذكرة هو إيجاد الطريقة المثلى لحماية تطبيقات الويب والبيانات الحساسة من المهاجمين والخروقات الأمنية عن طريق استخدام أنظمة التشفير الفعالة التي توفر بدورها درجة حماية كبيرة لتطبيقات الويب حيث قمنا بدراسة شاملة حول مختلف الاستراتيجيات التي تعتمد على التشفير في مضمونها وأمثلها كما تطرقنا إلى ما يسمى بالإمضاء الالكتروني ودوره الفعال في حماية البيانات حيث طبقنا بعض خوارزميات التشفير مثل RSA ECC, أيضا شرح بعض التقنيات المستخدمة لحماية ومنع الاستفسارات الملوثة التي يتم إدخالها من طرف المهاجم .

كلمات دلائلية:ECC،RSA، SQL، SQLI، NTRU، Elgmal ، PHPMyadmin

Abstract

With 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 access to sensitive and confidentiel data.

The purpose of this research paper is to find the best way to protect Web applications and sensitive data against hackers and security breaches through the use of effective encryption systems which, in turn, provide a significant degree of protection for Web applications. We made a thorough study of the different optimal strategies based on encryption in their content. We dealt with the e-Signature and its effective role in the protection of data. We applied encryption algorithms such as ECC, NTRUand of some of the techniques used to protect and prevent contaminated queries that are entered by the attacker.

Keys words:ECC, RSA, SQL, SQLI, NTRU, Elgmal, PHPMyadmin.

Résumé

Avec l’augmentation et la propagation de l’utilisation de l’internet dans le monde, les menaces de sécurité dans d'Internet ont augmenté de façon spectaculaire. Parmi les points vulnérables de ces applications 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.

Le but de ce mémoire est de trouver la meilleure façon de protéger les applications Web et les données sensibles contre les pirates et les failles de sécurité par l'utilisation des systèmes de cryptage efficaces qui, à leur tour, offrent un degré important de protection pour les applications Web. Nous avons fait une étude approfondie sur les différentesstratégies optimales qui se basent sur le chiffrement dans leur contenu.Nous avons mentionné l’e-Signature et son rôle efficace dans la protection des données. Nous avonségalement appliqué des algorithmes de chiffrement tels que ECC, RSAnous avons aussi expliqué quelques techniques utilisées pour protéger et prévenir les contaminées qui ont été entrées parattaquant.

Mottes clés: ECC, RSA, SQL, SQLI, NTRU, Elgmal, PHPMyadmin.