Cahier de charge de Mémoire de Licence

Titre du Sujet : Test d'intrusion sur une application web : cas d'un site d'E-commerce

Grade et Spécialité : Licence en Sécurité Informatique

Étudiant : Bill Johson ADJAÏ

1. Contexte et problématique

Dans cette section, nous présentons dans un sens général les applications web, les sites d'E-commerce, et les différents problèmes auxquels elles sont confrontées. Puis nous essayerons d'introduire des approches de solutions.

1.1. Contexte du travail

L'informatique couvre de nos jours divers domaines tels que la communication, la gestion, la sécurité, le commerce et bien d'autres. Cette discipline de traitement automatique et rationnel de l'information est utilisée de nos jours par certaines entreprises pour l'automatisation de certaines tâches dans le but de renforcer la fiabilité, la disponibilité et les performances ainsi que la réduction des coûts d'exploitation. Le renforcement des niveaux de sécurité est devenu une nécessité primordiale, étant donné l'apparition des diverses formes d'attaques informatiques.
Nous sommes donc à l'ère où la protection et la sécurisation de l'information numérique représente un enjeu capital pour les entreprises. Ces acteurs sont de plus en plus sujets à la numérisation de leur processus d'affaires et des documents associés. Les attaques informatiques auxquelles ils sont exposés ont donc des impacts d'autant plus importants selon la criticité de l'information. Il est donc capital d'être en mesure d'assurer une gestion des problèmes de sécurité résultant de pratiques de développement non sécurisées lors de la conception, du codage et de la publication de logiciels ou d'un site vitrine d'une entreprise : c'est l'objectif principal des « Tests d'intrusion sur une application web ».
A travers ce travail, nous aurons pour objectif d'effectuer des tests d'intrusion sur un site d'e-commerce dans le but de déceler les faiblesses et vulnérabilités afin de mettre en place de nouvelles mesures de sécurité du système d'information.

1.2. Problématique et détermination des besoins

Force est de constater que la plupart des applications web ne sont pas à l'abri d'intrusions ou de menaces d'attaques connues des réseaux d'entreprise, une sûreté totale ne peut donc pas être garantie. Cette dernière ne dispose pas souvent d'outils de sécurité nécessaire pouvant lui garantir une prévention régulière et un rapport à jour de l'état de son trafics réseau ; ce

qui l'expose à des risques d'intrusion anodins ou graves. Elles ne peuvent pas se porter garant de la protection de la sécurité du serveur web et du serveur de base de données et autres données circonstancielles. Assurer la confirmation de la configuration sécurisée des navigateurs web et identifier les fonctionnalités pouvant causer des vulnérabilités. De plus, ces applications d'entreprise sont confrontées à des faiblesses de sécurité lies à l'authentification des utilisateurs, l'usurpation d'identité qui permettent aux acteurs malveillants (attaquant) de manipuler le code source, d'obtenir un accès non autorisé, de voler des données ou d'interférer de quelque manière que ce soit avec le fonctionnement normal de l'application et à faire perdre de l'argent, à en gagner et a d'autre fin.

Pour remédier à ce problème, des recherches ont été effectuées afin de proposer des tests d'intrusion qui permettra à la fois de collecter en temps réel des informations sur le trafic réseau, de surveiller les activités ayant lieu dans le réseau afin de détecter les éventuelles intrusions et menaces pour protéger le réseau contre celles-ci.

2. Objectifs et contributions

Dans cette section sont présentés les différents objectifs des tests d'intrusion, et notre contribution en vue d'une bonne amélioration des niveaux de sécurité de l'application.

2.1. Les objectifs des travaux (Généraux et spécifiques)

L'objectif principal de notre projet de mémoire est d'identifier et d'améliorer les problèmes de sécurité résultant des pratiques de développement non sécurisées lors de la conception, du codage et de la publication de logiciels ou de l'application web, il s'agira spécifiquement :

- De mettre en place une application e-commerce ;
- D'effectuer des tests d'intrusion sur l'application développée pour déceler les failles et vulnérabilités ;
- Proposer des solutions de sécurité après la détection des faiblisses et vulnérabilité de l'application ;

2.2. Les contributions des travaux

Ce travail rentre dans le contexte du développement des applications et de la sécurisation desdites applications après des testes de décèlement des limites que possèdent les applications. Il rentre en ligne de compte dans la lutte contre la cybercriminalité qui mine aujourd'hui le développement des nations qui optent pour le numérique dans domaines à savoir l'éducation, le commerce, la santé etc.

3. Brève description de la solution et choix d'outils

Dans cette section nous présenterons de façon concrète, les différentes approches de solutions, puis nous ferons un choix des outils qui vont permettre l'atteinte des résultats.

3-1- Matériels et technologies utilisés

Dans ce chapitre nous aurons a parcours plusieurs étapes au cours de la conceptions de l'applications web.

- La Modélisation de l'application web au cours duquel nous aurons à manipuler UML.
- L'application web sera programmer en HTML 5 pour l'Edition des textes, CSS 3 pour la mise en forme et phpMyAdmin pour la gestion de la base de données.
- L'environnement de travail est Android studio ;

Nous aborderons ensuite les outils d'analyser de sécurité et vulnérabilités du site Web à la recherche de vulnérabilités de sécurité, malware et les menaces en ligne tels que SUCURI, Qualys, HostedScan Security, Intruder, ImmuniWeb, Pentest-Tools afin de vérifier le niveau de sécurités.

A ces étapes nous réunirons assez d'informations sur l'état de sécurité du site web où nous aurons une idée des niveaux sécurisé ou vulnérable, voir les failles possibles tels que l'usurpations d'identité, les scripts d'intensité, les injections SQL et les attaques par déni de service dans le but final de proposer des solutions de sécurité appropriée pour mieux sécuriser l'application.