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. 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. 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.

1. 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.

1. État de l’art

3.1. Les différentes caractéristiques du site d'E-commerce.

1. 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. de notre outil pour une très bonne amélioration.

Au cours de la réalisation de notre projet, nous sommes appelés à simuler des attaques sur l’application E-commerce dans le but de déterminer son niveau de sécurité. Ces attaques sont effectuées en interne ou en externe sur l’application, et elles aident à identifier les vulnérabilités et les faiblesses qu'il contient et à découvrir les exploits qui pourraient réellement compromettre le système applicatif. Il s'agit d'un bilan de santé essentiel du site e-commerce qui informe les testeurs si des mesures correctives et de sécurité sont nécessaires doivent être prise.

4.1 Différentes approche de solutions possibles.

A ce niveau, nous devons repérer les potentielles failles et vulnérabilités des pratique de développement lors de la conception, du codage et de la publication de l’application d’E-commerce afin de les corrigees grâce à des solutions de sécurité dans le but d’apporter des solutions de sécurité maximale de l’application. Cela consiste ;

* Etudier les applications web et présenter du site d’E-commerce ;
* Déceler ses faiblesses et vulnérabilités de l’application web ;
* Proposer des solutions de sécurité pour améliorer les faiblesses et vulnérabilités de l’application d’E-commerce ;
* Exposer les résultats obtenus après tests et éventuelles difficultés rencontrées ;

4.2 Analyse de chaque approche de solutions.

L'intégration des tests d'intrusion d'applications Web dans un programme de sécurité présente plusieurs avantages clés.

* Il vous aide à satisfaire aux exigences de conformité. Les tests d'intrusion sont explicitement requis dans certains secteurs, et la réalisation de tests d'intrusion sur les applications Web permet de répondre à cette exigence.
* Il vous aide à évaluer votre infrastructure. L'infrastructure, comme le pare-feu et les serveurs DNS, est accessible au public. Toute modification apportée à l'infrastructure peut rendre un système vulnérable. Les tests d'intrusion d'applications Web aident à identifier les attaques réelles qui pourraient réussir à accéder à ces systèmes.
* Il identifie les vulnérabilités. Les tests d'intrusion des applications Web identifient les failles dans les applications ou les routes vulnérables dans l'infrastructure, avant qu'un attaquant ne le fasse.
* Il aide à confirmer les politiques de sécurité. Les tests d'intrusion des applications Web évaluent les stratégies de sécurité existantes pour détecter toute faiblesse.

4.3 Choix de la meilleure approche de solution.

4.5 Test de l'approche de solutions

5. Conclusion et Perspectives.

Dans cette section, nous ferons une conclusion au regard du travail établi, puis nous essayerons de donner des perspectives en vue d'autres améliorations futures.

De nombreux problèmes de sécurité des applications Web liés aux intrusions sont dus au développement rapide des applications Web. Pour réduire le risque de problèmes d'application Web, les développeurs d'applications Web doivent prendre des mesures pour écrire des applications sécurisées afin d'éviter les attaques connues. Lorsque de telles mesures échouent, il est important de détecter ces attaques et de trouver la source des attaques pour réduire les risques estimés. La détection d'intrusion est l'une des techniques puissantes conçues pour identifier et prévenir les dommages au système. La plupart des techniques défensives des systèmes d'intrusion Web ne sont pas capables de faire face à la complexité des cyberattaques dans les applications Web. Cependant, les approches d'apprentissage automatique pourraient aider à détecter les attaques d'applications Web connues et inconnues. Dans ce mémoire, nous présentons la conception d’une application d’E-commerce sur laquelle nous effectuerons des tests d’intrusion afin d’identifier de potentiels faiblesse et vulnérabilités auxquels nous proposerons des solutions de sécurité.