UNIVERSITE VIRTUELLE DU SENEGAL
foo nekk foofu la

Sécurisation et optimisation des applications mobiles et web

M. Birahim BABOU

Séquence 1 : Chapitre 1 : Principes de base

Table des matières

Table des figures

Table des tableaux

Introduction

Avec le développement de l'Internet, les administrations publiques et privées cherchent de plus en plus d'avoir une présence sur l'Internet via des sites web ou des applications web offrant des services aux citoyens ou aux tierces entités.

Cependant, les vulnérabilités de ces applications Web ou mobiles sont désormais le vecteur le plus important des attaques dirigées contre la sécurité des systèmes d'information de ces administrations.

En effet, d'après les différents rapports publiés par les observatoires et sociétés de sécurité informatiques, les attaques web sont en constante augmentation.

Les conséquences peuvent être très lourdes pour les administrations victimes de cette situation :

- Atteinte à l'image de l'administration ;
- Une défiguration du site pour relayer un message politique (hacktivisme), pour dénigrer ou pour revendiquer son attaque (ex : ADIE en 2019) ;
- Mise en danger de l'intégrité du système d'information ;
- Exfiltration des données et d'information sensibles.

A cet effet, les développeurs d'applications ne doivent plus se permettre de tolérer les problèmes les plus simples comme ceux présentés dans le Top 10 OWASP qui sont dus principalement à un développement et un déploiement non sécurisé d'une application web ou mobile.

Ainsi, la mise en place de méthodes et d'outils pour gérer le développement et le contrôle qualité des applications s'avère plus que nécessaire pour réduire leur vulnérabilité.

1. Chapitre 1 : Principes de base

1.1. Application web et mobile

Les applications Web sont définis comme étant des applications basées sur le protocole HTTP, indépendantes des plateformes et langages d'implémentation, reposant sur des architectures Web. Elles peuvent interagir avec d'autres applications de type Web ou autres.

C'est un programme qui est capable de réaliser tous les traitements autorisés par le langage utilisé pour le concevoir.
Les besoins d'une application sont :

- D'**interagir** avec l'utilisateur ;
- De **traiter** les demandes ;
- D'**accéder** aux données.

Une application mobile est un logiciel applicatif développé pour un appareil électronique mobile, tel qu'un assistant personnel, un téléphone portable, un smartphone, un baladeur numérique, une tablette tactile, ou encore certains ordinateurs fonctionnant avec le système d'exploitation Windows Phone ou Chrome OS.

Elles sont pour la plupart distribuées depuis des plateformes de téléchargement (parfois elles-mêmes contrôlées par les fabricants de smartphones) telles que l'App Store (plateforme d'Apple), le Google Play (plateforme de Google / Android), ou encore le Microsoft Store (plateforme de Microsoft pour Windows 10 Mobile). Mais des applications peuvent aussi être installées sur un ordinateur, grâce par exemple au logiciel iTunes distribué par Apple pour ses appareils. Les applications distribuées à partir des magasins d'applications sont soit payantes, soit gratuites, mais généralement avec des publicités.

Sur certaines plateformes, les applications peuvent aussi être installées à partir de sources tierces, via un site non affilié au distributeur d'origine. Sur Android, cela est possible en activant le mode développeur. Sur iOS, cette manipulation est possible soit en étant développeur Apple, soit en possédant un appareil jailbreaké.

1.2. Base de données

Une base de données (en anglais database), permet de stocker et de retrouver l'intégralité de données brutes ou d'informations en rapport avec un thème ou une activité ; celles-ci peuvent être de natures différentes et plus ou moins reliées entre elles.

En effet, leurs données peuvent y être très structurées (base de données relationnelles par exemple), ou bien hébergées sous la forme de données brutes déstructurées (base de données NoSQL Redis par exemple) qui, dans ce cas, seront ensuite parcourues de manière organisée au moment de la lecture via des moteurs spécifiques (comme Elasticsearch).

Une base de données peut être localisée dans un même lieu et sur un même support informatisé, ou réparties sur plusieurs machines à plusieurs endroits (base de données NoSQL par exemple).

La base de données est au centre des dispositifs informatiques de collecte, mise en forme, stockage et utilisation d'informations. Le dispositif comporte un système de gestion de base de données (abréviation : SGBD) : un logiciel moteur qui manipule la base de données et dirige l'accès à son contenu. De tels dispositifs comportent également des logiciels applicatifs, et un ensemble de règles relatives à l'accès et l'utilisation des informations2.

La manipulation de données est une des utilisations les plus courantes des ordinateurs. Les bases de données sont par exemple utilisées dans les secteurs de la finance, des assurances, des écoles, de l'épidémiologie, de l'administration publique (notamment les statistiques) et des médias.

Lorsque plusieurs objets nommés « bases de données » sont constitués sous forme de collection, on parle alors d'une banque de données.

1.3. Sécurité applicative (Définition selon ISO 27034)

«La sécurité des applications est un processus effectué pour appliquer des contrôles et des mesures aux applications d'une organisation afin de gérer le risque de leur utilisation».

«Les contrôles et les mesures peuvent être appliquées à l'application elle-même (ses processus, les composants, les logiciels et résultats), à ses données (données de configuration, les données de l'utilisateur, les données de l'organisation), et à toutes les technologies, les processus et acteurs impliqués dans le cycle de vie de l'application».

La sécurité applicative ne couvre pas uniquement la portion logicielle. Elle couvre également tous les contrôles et mesures impliqués dans le cycle de vie de l'application.

Au sens large, la sécurité c'est l'ensemble des moyens (techniques, organisationnels, humains, légaux) pour **minimiser la surface d'exposition d'une application ou d'un système contre les menaces** :

- **Passives** visant à écouter ou copier des informations illégalement ;
- **Actives** consistant à altérer des informations ou le bon fonctionnement d'un service.

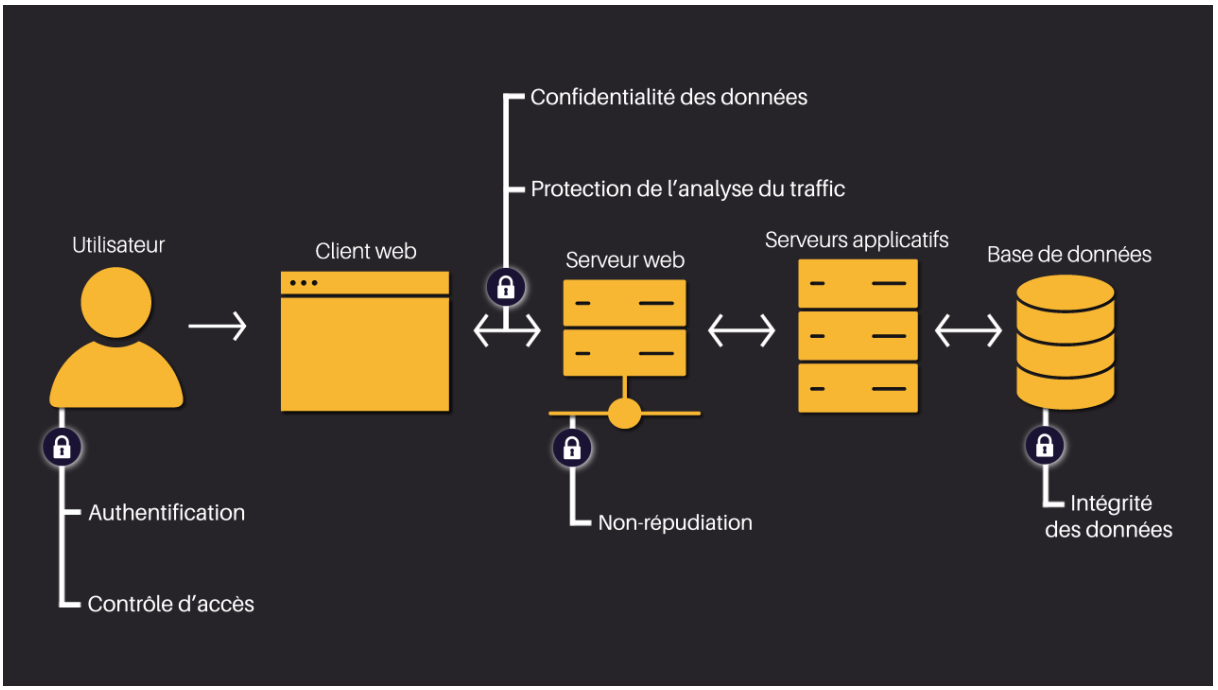

Figure 1: Application des concepts de sécurité à une application Web

1.4. Les différents types de menaces

Toutes menaces montre un système informatique appartient à l'un des types de menaces suivants :

- Interruption
- Interception
- Modification
- Insertion

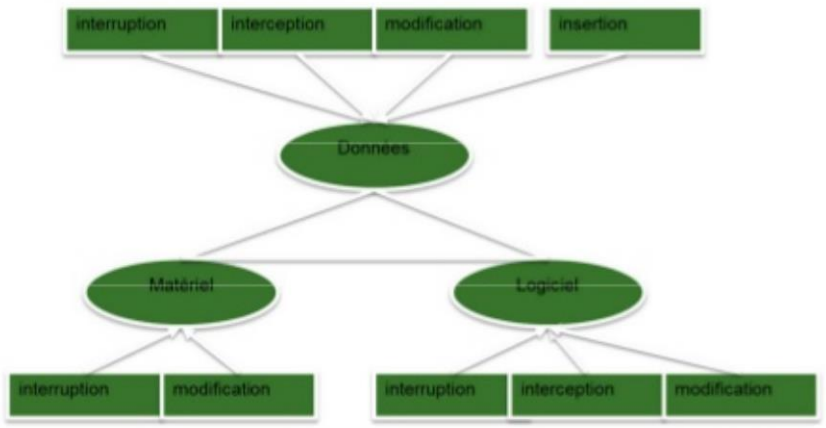

Figure 2: Les différents types de menaces

1.5. Introduction au hacking et jargon

Figure 3: Les différentes étapes du hacking

1.5.1. Collecte d'informations

La prise d'empreinte est une étape préalable à toute attaque. Elle consiste à rassembler le maximum d'informations :

- Adressage réseau
- Nom de domaine
- Protocole de réseau
- Système
- Services
- Architectures des serveurs
- Utilisateurs
- Etc.

1.5.2. Balayage du réseau

Lorsque la topologie du réseau est identifié, le pirate peut scanner :

- Les adresses actives du réseau
- Les ports ouverts
- Les types d'OS
- Les services
- Etc.

1.5.3. Repérage des failles

Après avoir établi l'inventaire du parc logiciel, matériel, système, d'utilisateurs, etc., il reste à vérifier si des failles existent avec ces exemples d'outils de d'identification de faiblesses et de détection d'intrusion potentielles en sécurité informatique :

- CERT
- Nessus
- Snort
- Metasploit
- Etc.

1.5.4. Intrusion

Lorsque la cartographie des ressources est dressées, il sera possible de préparer son intrusion :

- Accéder à des comptes valides
- Injecter le code
- Metasploit

1.5.5. Extension des privilèges

Lorsque l'accès est fonctionnel, on peut chercher à avoir des privilèges root.

1.5.6. Compromission

1.5.7. Porte dérobée

Après avoir accéder au système, on peut créer artificiellement une porte d'entrée en installant une application tierce afin de créer la faille de sécurité.

1.5.8. Nettoyage des traces

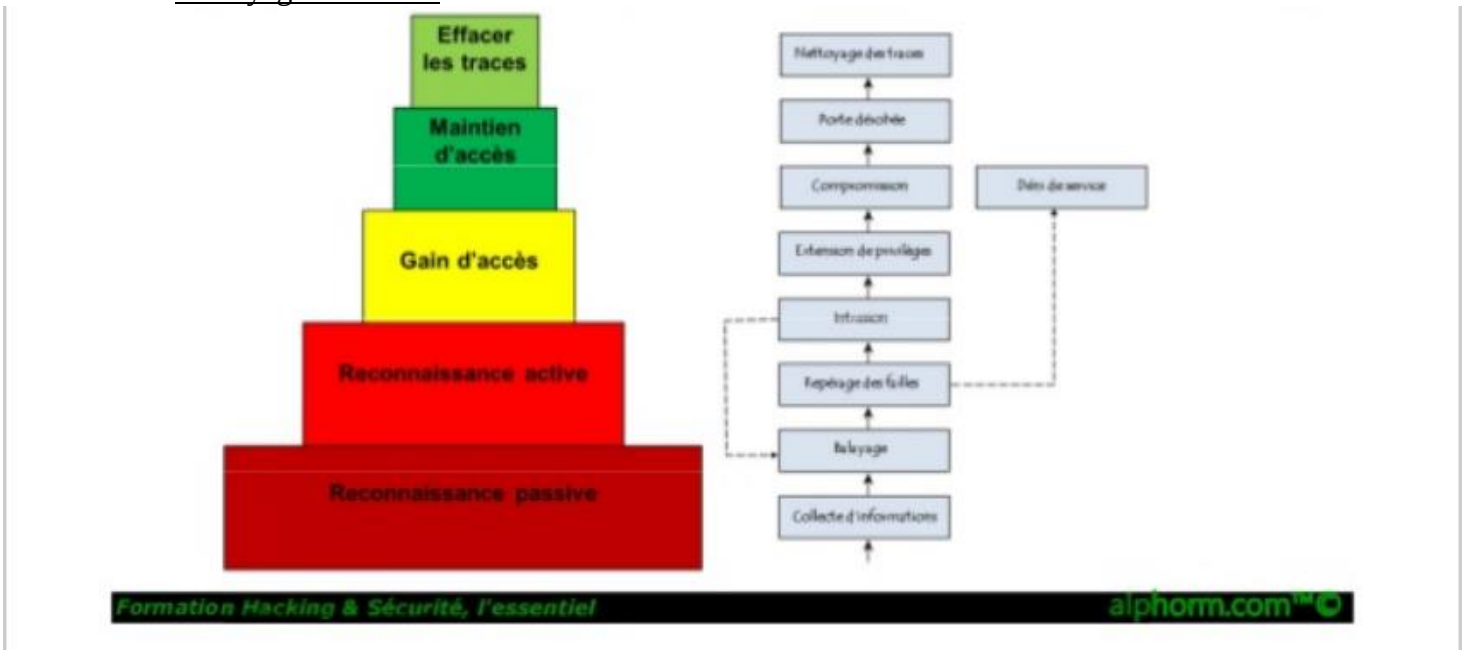

Figure 4: Suite étapes du hacking