RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

greta YVELINES ACADÉMIE DE VERSAILLES

VEILLE TECHNOLOGIQUE

LA SECURITE DES DONNEES WEB

Mendes Lopes Ermelindo | Epreuve E4 BTS SIO SLAM

Table des matières

Introduction

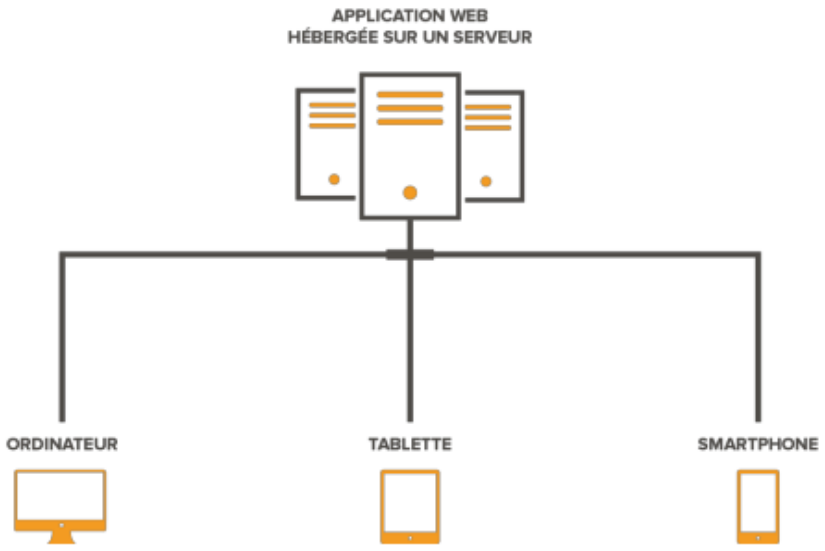
Depuis quelques années, développer un site web est devenu très accessible. De plus en plus de gens se lancent dans la réalisation de leur propre page. Mais très peu sont informés sur les vulnérabilités présentes dans leur réalisation (plus couramment appelées failles), et cela peut s'avérer très dangereux.

Une faille est une faiblesse dans un code qui peut être exploitée pour détourner un site de sa fonction première. Le pirate va pouvoir récupérer des données confidentielles (comme les infos personnelles des inscrits) ou modifier le comportement du site. Mais heureusement, il est possible de se protéger de ces fameuses failles par diverses techniques.

1. Qu'est-ce qu'une application Web ?

A. Typologie des applications web

Une application web est une extension dynamique d'un serveur web. Une application web est formée d'un ensemble de composants web, de ressources statiques (images, sons, ...), de bibliothèques et de classes utilitaires. Les composants web fournissent cette capacité d'extension.



Il existe deux formes de typologies des applications Web :

1. Orientée présentation, générant des pages contenant différents types de langage : HTML, SGML, XML, ... en réponse à des requêtes. Les pages générées peuvent être statiques (pages html) ou dynamiques (pages contenant du code exécuté sur le serveur).

2. Orientée service, implémentant un point d'accès à un service via le Web. Ce service est souvent invoqué par une application orientée présentation. Ce sont typiquement des services métiers. On parle de transactions B-to-B

Exemple : une entreprise envoie une requête contenant la destination de livraison d'une commande. Le service requis détermine la route à suivre dont le coût est moindre. La réponse n'est pas obligatoirement liée à l'invocation du service. Elle pourra faire l'objet d'une réponse séparée.

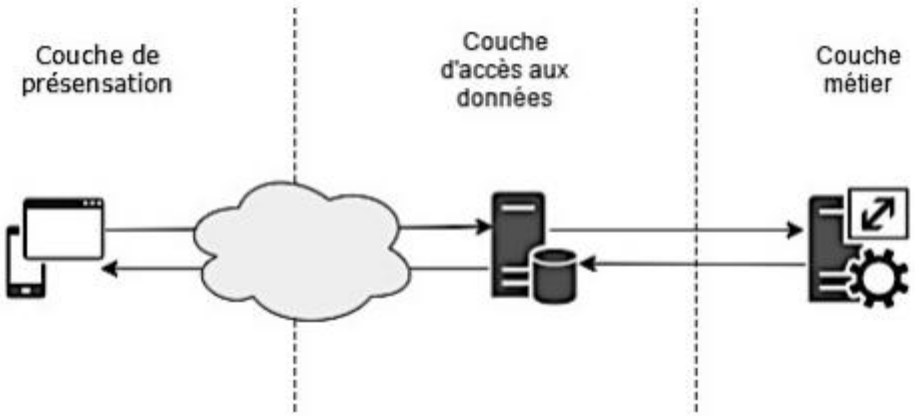
B. Architecture

L'architecture d'une application Web est dite « Architecture à 3-tiers » ou « Architecture à 3 niveaux ». Elle se présente en 3 couches :

1 Couche présentation : il s'agit de la partie de l'application responsable de la présentation des données, et de l'interaction avec l'utilisateur (application HTML exploitée par un navigateur Web ou WML pour être utilisée par un téléphone portable par exemple).

2 Couche métier : elle reçoit les requêtes utilisateur. Le serveur d'application fournit les traitements métiers. C'est là qu'est implémentée la logique du système et ses règles de gestion. Ce niveau protège les données d'un accès direct par les clients.

3 Couche d'accès aux données : couche responsable de la gestion des données. Cette couche permet de rendre l'accès aux données transparente (uniforme) quelle que soit la méthode utilisée pour les stocker (fichier, base de données...).



Cette architecture est avant tout un élément de structuration logique. Rien empêche aux 3 couches de s'exécuter sur une même machine.

2. Les principales failles de sécurités des application web

A. L'OWASP

OWASP (Open Web Application Security Project) est un guide de sécurisation des applications web, c'est un « ouvrage » de référence des bonnes/mauvaises pratiques de développement, d'une base sérieuse en termes de statistiques, et d'un ensemble de ressources amenant à une base de réflexion sur la sécurité.

La Fondation OWASP est entrée en ligne le 1er décembre 2001. Elle a été créée en tant qu'organisation caritative à but non lucratif aux Etats-Unis le 21 avril 2004 pour assurer la disponibilité et le soutien continu de notre travail à l'OWASP.

Le but d'OWASP est de permettre à la communauté mondiale prospérer en stimulent la visibilité et l'évolution de la sûreté et de la sécurité des logiciels dans le monde.

B. Top dix des risques de sécurité des applications

L'OWASP Top 10 est un document de sensibilisation puissant pour la sécurité des applications Web. Il représente un large consensus sur les risques de sécurité les plus critiques pour les applications Web. Les membres du projet incluent une variété d'experts en sécurité du monde entier qui ont partagé leur expertise pour produire cette liste.

L'adoption du Top 10 de l'OWASP est peut-être la première étape la plus efficace pour changer la culture de développement de logiciels au sein de votre organisation en une culture qui produit du code sécurisé.

Chaque année, le Top 10 de l'OWASP est mis à jour, le classement mis ci-dessous a été publié en novembre 2017 :

1. Contrôle d'accès défaillant
2. Défaillances cryptographiques
3. Injection
4. Conception non sécurisée
5. Erreur de configuration de sécurité
6. Composants vulnérables et obsolètes
7. Échecs d'identification et d'authentification
8. Manque d'intégrité des données et du logiciel
9. Carence des systèmes de journalisation et de surveillance
10. Falsification de requête côté serveur (SSRF)

C. Risques des failles

A 01 Contrôle d’accès défaillant :

Le contrôle d'accès applique une stratégie telle que les utilisateurs ne peuvent pas agir en dehors de leurs autorisations prévues. Les défaillances entraînent généralement la divulgation, la modification ou la destruction d'informations non autorisées de toutes les données ou l'exécution d'une fonctionnalité métier en dehors des limites de l'utilisateur. Les vulnérabilités courantes du contrôle d'accès incluent :

- Violation du principe du moindre privilège ou de refus par défaut, où l'accès ne doit être accordé que pour des capacités, des rôles ou des utilisateurs particuliers, mais est accessible à tous.
- Contourner les contrôles d'accès en modifiant l'URL (falsification de paramètres ou navigation forcée), l'état interne de l'application ou la page HTML, ou en utilisant un outil d'attaque modifiant les requêtes API.

A 02 Défaillances cryptographiques :

Des défaillances cryptographiques peuvent se produire en raison d'un manque de chiffrement ou d'un faible chiffrement en transit, ou en cas d'exposition accidentelle de données sensibles. Les attaques contre ces failles sont généralement spécifiques à l'application et nécessitent donc une approche de défense en profondeur pour les atténuer.

A03 Injections SQL :

Des failles d’injection, telles que des injections SQL, NoSQL, OS et LDAP, se produisent lorsque des données non approuvées sont envoyées à un interpréteur dans le cadre d'une commande ou d'une requête. Les données hostiles du pirate informatique peuvent inciter l'interpréteur à exécuter des commandes inattendues ou à accéder aux données sans autorisation appropriée.