SECURITE DES APPLICATIONS WEB

Evolution des applications web

Aux premiers jours de l’internet, le World Wide Web consistait en de simples pages web, des pages d’information constituée de ressources statistiques. Le flot d'informations était à sens unique, du serveur au navigateur. L’authentification des utilisateurs n’était souvent pas nécessaire car les mêmes informations étaient affichées à tous les utilisateurs. Les menaces de sécurité découlaient exclusivement de l’hébergement des sites web, c’est-à-dire au niveau des serveurs web. En cas d’attaque, il n’y avait que peu de risques car l’information au niveau des serveurs était déjà accessible au grand public. Les attaques consistaient donc le plus souvent à des démaquillages des sites web.  
Aujourd’hui, le World Wide Web est très différent de ce qu’il était à ses débuts. La majorité des sites web sont en réalité des applications web. Ils ne se limitent plus à l’affichage de ressources statistiques. De nouveaux sites web plus poussés apparaissent : les applications Web. Une application web est un site Web qui permet à ses utilisateurs de réaliser des tâches spécifiques. Le flux d’informations n’est plus à sens unique mais plutôt bidirectionnel entre le serveur et le client (navigateur, téléphone mobile, …). Le contenu présenté aux utilisateurs est spécifique à chaque utilisateur en fonction de préférences préalablement enregistrées ou d’autres paramètres de l’application. L’information traitée est très sensible de nos jours. En effet, les applications web prennent en charge des fonctionnalités très délicates telles que les transactions financières. Il y a de cela quelques années, lorsqu’on voulait faire une transaction financière, il fallait aller à la banque et un agent le faisait pour vous. Aujourd’hui, avec ces applications web, il est possible de faire ces transactions soient même en ligne en fournissant certaines informations. Ainsi, si un attaquant arrivait à compromettre ce genre d’applications par exemple, il lui serait facile de faire des transactions frauduleuses et vider votre compte bancaire. De même, de nos jours, toute présence sur le net requiert la fourniture de données privées, il ne serait pas bien que ces informations tombent entre les mains d’individus malintentionnés. Il y a aussi la multiplication des sites marchands sur le net qui permettent de faire des achats en ligne. Qu’un individu malintentionné arrive à compromettre ce genre d’applications représenteraient de gros risques à la fois pour les propriétaires de ces applications dont le business repose essentiellement sur ces applications mais aussi pour les utilisateurs qui auront fourni des informations très sensibles (mots de passe, numéros de carte de crédit entre autres). Voilà les enjeux de la sécurité des applications web.

Le Mobile dans tout cela

Applications web courantes

Les applications web peuvent assurer pratiquement toutes les fonctionnalités d’un logiciel bureau classique. Voici quelques types d’applications que l’on retrouve très souvent :

* Réseaux sociaux
* Vente en ligne
* E-Banking
* Mailing
* Médiathèques

En plus des applications web disponibles publiquement, nous avons les applications web internes aux entreprises qui soutiennent les entreprises dans l’accomplissement de tâches spécifiques : applications de gestion de ressources humaines et de la paie, applications de collaborations, applications de messagerie interne ainsi que les applications sur mesure propres au fonctionnement de l’entreprise (ERPs, applications de gestion des assurances, applications de gestion d’examens, etc.)  
La majorité de ces applications manipulent des données hautement sensibles et fournissent des informations très confidentielles. La sécurité y est donc très importante. Or, la tendance aujourd’hui est de faire héberger ces applications « internes » par des fournisseurs externes afin de réduire les coûts liés à la mise en place d’infrastructures internes.

La majorité des applications web existe aussi en version mobile. Ces applications mobiles utilisent soit des navigateurs embarqués, soit des APIS exposées par l’application web basées sur http. Les fonctions et les données manipulées par les applications web sont généralement les mêmes. Cela fait que les applications mobiles sont exposées aux mêmes risques que les applications web. Pour une organisation, prendre en charge la sécurité implique aussi très fortement la sécurité des applications mobiles qui sont très souvent plus critiques car étant hébergées sur le dispositif de l’utilisateur et hors du contrôle de l’organisation. Un utilisateur malintentionné peut même arriver à retrouver le code source de l’application par décompilation du fichier apk de l’application et le cas échéant compromettre la sécurité de l’application mobile.

Avantages des applications Web

Il n'est pas difficile de voir pourquoi les applications Web ont pris de l’ampleur. En plus des motivations financières évidentes (possibilité de toucher plus de clients à travers le net), il y a plusieurs autres facteurs techniques :

* Le protocole HTTP permettant au client et au serveur de communiquer facilement via TCP/IP et que l’on peut associer à d’autres protocoles. Pour le rendre plus sûr par exemple, il est associé à TLS donnant HTTPS
* L’accès à ces applications web ne nécessite qu’un navigateur. Chaque internaute dispose déjà d'un navigateur installé sur son ordinateur ou son appareil mobile. De même les navigateurs web sont aujourd’hui très avancés donnant des expériences utilisateur très satisfaisantes
* La maintenance est simplifiée car toutes les opérations se font sur le serveur évitant ainsi la nécessité de distribuer et de gérer séparément un logiciel client. De même, les changements ont un effet immédiat
* Les technologies de base et les langages utilisés pour développer des applications web sont relativement simples. Un large éventail de plates-formes et d'outils de développement sont disponible pour faciliter le développement d'applications puissantes.

Sécurité des applications Web

Comme avec toute nouvelle technologie, les applications Web ont apporté avec eux de nouvelles vulnérabilités.

Les attaques les plus redoutées contre les applications Web sont celles qui exposent des données sensibles ou qui aux attaquants d’avoir accès à des privilèges qu’ils ne devraient pas. Et il faut noter que ce genre d’attaques se produit très souvent malgré toutes les mesures de sécurité prises. Un autre type d’attaques très fréquent est le déni de service qui rend une application web indisponible. Ils peuvent parfois être utilisés pour acquérir un avantage concurrentiel par rapport à ses pairs dans les domaines du trading financier, des jeux, des ventes en ligne, etc.

Les techniques d’attaques des applications ont évolué au fil du temps et sont devenues plus poussées. De nouvelles techniques d’attaques, non prises en compte lors de la conception des applications sont apparues tout comme d’autres vulnérabilités sont devenues moins fréquentes.

Tout au long de cette évolution, des applications web de premier plan ont été compromis : Myspace, Sony, entre autres. Et la menace est toujours présente. Aujourd’hui, la sécurité des applications Web est devenue un domaine très important pour ne pas dire critique. Les organisations mobilisent des ressources importantes pour garantir la sécurité de leurs applications car il en va même de leurs renommées.

Les technologies des applications web

Les applications web emploient une myriade de technologies :

* des langages côté client
* des langages côté serveur
* des langages mobiles
* des standards permettant de formaliser les données que s’échangent le serveur et les différents clients
* des langages pour la manipulation des données persistantes
* des protocoles de communication entre client et serveur

Elles reposent aussi sur un ensemble d’infrastructures :

* serveurs web
* serveurs d’application
* serveurs proxy
* serveurs de données

La sécurité des applications web implique la sécurité au niveau de ces infrastructures qui communiquent en réseau (sécurité réseau) mais aussi la sécurité lors de l’utilisation des technologies web (sécurité applicative).

Cette utilisation de technologies multiples n’est pas sans effet sur la sécurité. En effet, chacune de ces technologies présente certaines vulnérabilités. Ainsi, plus on en utilise, plus les failles de sécurité sont susceptibles d’être plus présentes dans nos applications. Et les attaquants sont bien conscients de cela et n’hésitent pas exploiter la moindre faille présente sur une de ces technologies. C’est pourquoi, lorsqu’on veut assurer la sécurité des applications web et mobiles, il faut prendre en compte toutes ces technologies.

Ces technologies varient d’une application web à une autre mais en général le même protocole est utilisé à la fois pour les applications web et mobiles : le protocole HTTP est le protocole de communication de base dans le World Wide Web et est utilisé par toutes les applications Web de nos jours. HTTP ne cryptant pas les communications, les rendant visibles à toute personne disposant des outils nécessaires, des données confidentielles peuvent tomber entre les mains d’individus malintentionnés. De ce fait, HTTP est utilisé de nos jours avec TLS donnant HTTPS qui permet de protéger la confidentialité et l’intégrité des données échangées. Ainsi, pour toute communication impliquant des données sensibles, HTTPS est utilisé. La tendance est même de faire en sorte que HTTPS, plus sûr soit utilisé partout sur le Web.

Web 2.0

C’est un concept qui a fait son apparition ces dernières années faisant référence au Web tel que nous le connaissons aujourd’hui avec notamment l’utilisation intensive d'Ajax pour effectuer des requêtes asynchrones en coulisse pour enrichir l’expérience utilisateur, l’utilisation de nouvelles technologies côté client telles XML et JSON, la multiplication des sites Web de partage et d’interaction tels que les blogs et les réseaux sociaux.

Il est clair que ces nouvelles tendances technologiques apportent avec elles leurs enjeux en matière de sécurité mais ne définissent un cadre particulier de sécurité. Le contexte de sécurité ne change pas. Les vulnérabilités que l’on rencontre dans ce contexte sont généralement identiques ou étroitement dérivées de celles que l’on rencontrait avant l’avènement de ces technologies. Il n’est pas judicieux de parler de Sécurité du Web 2.0

Sécurité des applications Web

Le problème de la sécurité dans les applications Web est un fait et les différents acteurs du Web commencent à en être conscients. Cependant, on rencontre très souvent des applications qui assurent qu’elles sont sécurisées car utilisant telle technologie (SSL par exemple). Les utilisateurs sont souvent invités à vérifier le certificat du site, à admirer les protocoles cryptographiques utilisés et, sur cette base, faire confiance au site Web. De plus, elles citent parfois leur conformité à une certaine norme comme gage de sécurité (PCI-DSS par exemple).

Ce qu’il faut avoir, c’est qu’il s’agit très souvent de marketing pour attirer plus de clients. En fait, la majorité des applications Web sont peu sûres, malgré la large utilisation du protocole SSL et l’adoption de certaines normes.

C’est dans ce sens que des initiatives ont été prises pour adresser les problèmes de sécurité rencontrés le plus souvent au niveau des applications Web et mobiles afin d’éveiller les organisations et les inciter à prendre ces problèmes à la source. Parmi ces initiatives, nous avons l’OWASP Top 10 et le Mobile 10 de l’OWASP qui produisent périodiquement respectivement un classement des dix vulnérabilités les plus fréquentes au niveau des applications Web et des dix vulnérabilités les plus fréquentes au niveau des applications mobiles.

Problème principal

De ces remarques sur la sécurité des applications Web, ce que l’on remarque est que le problème fondamental est que l’utilisateur peut soumettre des données arbitraires. Et ce sont ces données qui sont à la base des traitements faits par l’application. Or ces données peuvent compromettre l'application en interférant avec sa logique et son comportement et obtenir un accès non autorisé à ses données et fonctionnalités.

L'application doit supposer que toutes les entrées sont potentiellement malicieuses, ce qui n’est souvent pas le cas. Très souvent, les applications Web font confiance aux données soumises par les utilisateurs et prennent des décisions de sécurité sur cette base.

La soumission de données malicieuses peut se faire de diverses manières:

* les utilisateurs peuvent interférer avec n'importe quelle donnée transmise entre le client et le serveur, y compris les paramètres de requête, les cookies et les en-têtes http en utilisant un proxy entre le client et le serveur. Tous les contrôles de sécurité implémentés côté client peuvent être ainsi contournés. On parle d’attaque par l’homme du milieu ;
* les utilisateurs peuvent envoyer les données sur des formats différents de ceux attendus par l’application. Toute hypothèse des développeurs sur la façon dont les utilisateurs interagiront avec l'application peut être violée entrainant l’application à se comporter d’une matière inattendue ;
* les utilisateurs ne sont pas limités à utiliser uniquement un navigateur Web pour accéder à l'application. De nombreux outils largement disponibles fonctionnent tel un navigateur et peuvent aider à des attaques contre les applications Web.
* etc.

La majorité des attaques contre les applications Web impliquent l'envoi de données inattendues au serveur pour provoquer un comportement inattendu dévoilant des failles exploitables.

Facteurs participant à l’insécurité des applications Web

Comme nous l’avons dit, le principal problème de sécurité rencontré par la majorité des applications Web est le fait qu’elles accepter et traitent des données non fiables qui peuvent être malveillantes.

Cependant, plusieurs autres facteurs contribuent à cet état de fait et expliquent pourquoi tant d'applications Web et mobiles sont vulnérables.

* Bien que la prise de conscience quant aux problèmes de sécurité des applications Web ait augmenté ces dernières années grâce aux différentes initiatives dans ce sens, elle reste moins développée que dans des domaines plus anciens tels que les réseaux et les systèmes d'exploitation. De fausses idées existent encore à propos de la plupart des concepts de base de la sécurité des applications Web. De nos jours, le travail d’un développeur Web consiste de plus en plus à intégrer, réutiliser des dizaines, voire des centaines, de composants tiers, conçus pour abstraire la complexité inhérente à ces différents composants et à réduire les temps de développement. Cependant, il est courant de voir des développeurs Web expérimentés faire des hypothèses sur la sécurité de leurs applications basées sur les frameworks qu’ils utilisent et à qui l’explication de simples failles de sécurité vient comme une révélation.
* Pour réduire les temps de développement des applications web, de plus en plus de composants tiers sont réutilisés. Cependant, ces composants ont parfois des failles de sécurité qui ouvrent des brèches aux attaquants. Et très souvent, avant que ces failles de sécurité ne soient découvertes par les éditeurs et ne soient corrigées par des patchs, elles sont déjà exploitées.
* De nos jours, de plus en plus d’outils sont créés afin de permettre à des non professionnels de l’informatique de pouvoir créer de puissantes applications Web en quelques clics. Ces outils fournissent du code prêt à l’emploi et pouvant gérer de nombreux cas de figures : blogs, vente en ligne, entre autres. Ils fournissent de nombreuses fonctionnalités prêtes à l’emploi incluant même des fonctionnalités de sécurité telles que l’authentification, la gestion des utilisateurs entre autres. Ces outils permettent la création d’applications sans nécessiter une compréhension technique de la façon dont les applications fonctionnent ou des risques potentiels qu'elles peuvent contenir et comment ils doivent être pris en compte. Et il y a une énorme différence entre produire un code fonctionnel et un code sécurisé. Or ce genre d’outils est très utilisé et parfois même par des entreprises de renom. Il n’est pas rare que des failles de sécurité soient découvertes dans ces outils. Ainsi, quand une vulnérabilité est découverte, il affecte de nombreuses applications à la fois.
* Les menaces évoluent très rapidement. De même, elles apparaissent plus rapidement qu’elles ne sont résolues. Il est courant que les défenses acceptées pour une certaine menace d’être dépassées par de nouvelles formes d’attaques. Une équipe de développement qui commence un projet avec une connaissance avancée de plusieurs menaces et de leurs contre-mesures peut être complètement dépassée avant la fin du projet du fait de l’évolution rapide des techniques d’attaques.
* Le développement des applications Web est très souvent soumis à des contraintes de temps et de ressources. Pour la plupart des organisations, il est impossible d’engager une équipe d’experts sécurité dédiée à la gestion des besoins de sécurité. De même, dans le cycle de développement logiciel, les considérations de sécurité ne sont pas très souvent prises en compte. En effet, la plupart des méthodologies utilisées de nos jours sont des méthodes agiles. Elles sont orientées rapidité de développement, c’est-à-dire produire plus de fonctionnalités très rapidement. Et dans ces méthodologies agiles, les exigences de sécurité tombent dans le champ des exigences non fonctionnelles. Aussi, les fonctions de sécurité n’ont pas la même visibilité que les fonctions business de l’application. Les équipes de développement dans les méthodologies agiles sont amenées à produire des fonctionnalités qui sont visibles pour le client. La

Tous ces facteurs contribuent à rendre les applications Web vulnérables.

Les mécanismes de sécurité de base

User access

User input

Handling attackers

Espace administration

Le nouveau perimetre de securite

- securite maintenant sur le niveau applicatif (look at the note) et u cote des utilisateurs (proteger les utilisateurs)

summary