RAPHAEL TRABELSI & NATHAN HAYOUN

ORT DANIEL MAYER

2019/2020

La sécurité des développement web

Veille Technologique

Table des matières

I Présentation de la technologie

a) Définition

La sécurité des informations des utilisateurs est un enjeu crucial pour les entreprises comme pour les particuliers.
De nombreux sites web sont vulnérables face à des attaques informatiques, pouvant entrainer des vols de données tels que des mots de passes, des adresses mails, des cartes de crédits…
L'enjeu de la sécurité web est donc de mise. Celle-ci permet de prévenir et de protéger les sites web des accès non-autorisé, pouvant compromettre la pérennité des informations du site en question.
L'objectif de la sécurité des sites Web est de prévenir plusieurs types d'attaques. Plus formellement, la sécurité des sites Web est l'acte et la pratique qui consiste à protéger les sites web contre l'accès, l'utilisation, la modification, la destruction ou la perturbation non autorisées.
La mise en place d'une sécurité efficace se traduit par un effort de conception sur l'ensemble du site web.

b) Intérêt

A l'heure ou le monde panique de plus en plus avec la collecte des données sur internet, la sécurité devient un sujet des plus sensibles. Effectivement, si a l'époque cela ne concernais que les grandes entreprises, de nos jours, du fait du développement rapide d'internet et du big data, il devient urgent d'être et de savoir se protéger.
Il faut savoir aussi que 1 URL sur 13[1] est utilisée à des fins malveillantes. C'est pour cela que la sécurité web devient importante sinon sine qua non à internet.

c) Outils

Des outils existent afin de tester la sécurité des sites web. Ces scanner de vulnérabilités détectent les faiblesses pouvant être exploitées par les hackers. Nous pouvons citer Metasploit (le plus utilisé), Acunetix, ou SQLmap.
Nous pouvons utiliser des Framework coté client qui intègre avec eux des solutions de sécurité.

[1] **https://www.vaadata.com/blog/fr/statistiques-2017-attaques-web-mobile/**

Par ailleurs il est possible aussi, via l'OS Kali Linux d'établir un laboratoire de test, pour essayer la plupart des failles sur notre propre site et réaliser des pentest (test d'intrusion).

II Site consultées

Site consultées	https://developer.mozilla.org/fr/docs/Learn/Server-side/Premiers_pas/Website_security
	https://www.vaadata.com/blog/fr/statistiques-2017-attaques-web-mobile/
	carte-formule-bnpnet.com
	https://www.nbs-system.com/blog/scanner-automatique-de-vulnerabilites-lequel-choisir/
	https://fr.wikipedia.org/wiki/Scanneur_de_vuln%C3%A9rabilit%C3%A9
	https://secludit.com/blog/examen-tests-dintrusion/
	https://www.slideshare.net/hellosct1/comprendre-la-securite-web-77763122

Flux RSS sur Feedly	Actualités securite
	Blog officiel de Kaspersky
	CERT-FR
	Sécurité – Silicon
	Sécurité informatique : Toute l'actualité sur Le Monde.fr.

III Menaces

a) Perte financière

La sécurité est important au seins d'un site web. Ces failles peuvent souvent occasionnées des perte financière importante. Que ce soit au niveau de l'entreprise qui as vu son site internet piraté, mais aussi pour l'utilisateur lambda qui sera une victime collatéral. Les failles de type injection SQL permettent de récupérer des informations importantes tel que les codes de cartes bleu et donc vider les comptes bancaires de ses victimes. Mais aussi si l'entreprise possède un site de vente en ligne, ces derniers sont parfois bloqué pendant des heures. On peux cité l'exemple du PlayStation store qui le jour de noël a été rendu inaccessible par des pirates.

b) Vols de données

La collecte de données personnelles, toujours plus importante des utilisateurs d'un service web, ajoute un enjeu supplémentaire dans la sécurisation de ces mêmes données.
Les données les plus sensibles sont bien évidemment les données bancaires, et les mots de passes.
La sécurisation de ces données peut se faire sur deux axes :

- Virtuel, par l'intermédiaire d'un cryptage de ces informations dans la base de données.
- Physique en restreignant l'accès des personnes non-autorisés aux serveurs.

Le vol de données sur un site web implique deux parties, le webmaster ou la société qui gère le site web, et l'utilisateur. Les conséquences pour chacune d'entre-elles après un vol de données diffère. La société en charge du site web peut être condamné par rapport au vol des données. L'amende varie en fonction du nombre d'utilisateurs concernés, de la faille exploitée, et de la sensibilité des données. Elle peut également être condamnée à cause d'un collecte trop importantes de données.
Le piratage d'un site web peut avoir des répercussions désastreuses pour l'utilisateur. Celui-ci pout se voir affecté sur l'ensemble des sites web dans lesquels il s'est inscrit.

Ces dernières années, de nombreuses brèches ont été exploité par les hackeurs. Parmi les plus importantes, nous pouvons citer Adobe. Le site have i been pwned par exemple liste l'ensembles des sites web qui ont subit un vol de données.

c) Perte de données

Certaines failles notamment les injections SQL permettent un accès non autorisé dans les bases de données. Outre le fait que l'attaquant as accès a des données sensible, il peux en plus supprimer ces derniers. Cela peux causer un problème de taille. En effet deux cas de figure peux ce présenter. Soit l'entreprise avait une sauvegarde régulière de ses données soit elle n'en avait pas.
Si aucune sauvegarde n'existe, la perte de données est quasi fatal pour cette dernière. Effectivement il n'y as aucun moyen de récupérer les données perdue. Par exemple l'attaque de WannaCry, qui as bloqué les ordinateur de milliers d'hôpitaux. Ces derniers ce sont trouvé désemparé face au pirate avec le risque de perdre toutes les données vital de leurs patient.
En revanche si elle possédait des sauvegarde, le régime de l'entreprise est aussi ralenti. Il faut du temps avant de tout restaurer, ce qui entraine naturellement le travail ou la visibilité de l'entreprise.

IV Différentes faille

a) XSS

XSS est un terme utilisé pour décrire une attaque qui permet à l'attaquant d'injecter des scripts, exécutés côté-client, *au travers* du site web pour viser le navigateur web des autres utilisateurs. Comme le code injecté provient du site web le navigateur web le considère comme sûr, il peut de ce fait faire des choses comme transmettre le cookie d'authentification de l'utilisateur à l'attaquant. Une fois que l'attaquant obtient ce cookie il peut se connecter sur le site comme s'il était l'utilisateur attaqué et peut faire tout ce que l'utilisateur pourrait faire. En fonction du site sur lequel

l'attaque se produit, cela peut inclure l'accès aux détails de carte bancaire, les informations des contacts, la modification du mot de passe, etc.

b) Injection SQL

L'injection SQL est une vulnérabilité qui permet à un attaquant d'exécuter du code SQL frauduleux sur une base de données, permettant l'accès, la modification ou la suppression des données quel que soit le droit de l'utilisateur. Une attaque par injection réussie peut permettre l'usurpation d'un compte, la création d'un compte avec les droits administrateur, l'accès à toutes les données du serveur, ou la modification et ou destruction des données pour le rendre inutilisable.

Cette vulnérabilité est présente quand la saisie de l'utilisateur est transmise à une requête SQL sous-jacente qui peut modifier le sens de la requête

c) Falsification de requête inter-sites (CSRF)

Les attaques CSRF permettent à un utilisateur malveillant d'exécuter des actions à l'aide des identifiants d'un autre utilisateur sans que cet utilisateur ne soit informé ou consentant.
Ce type d'attaque s'explique mieux avec un exemple. Nathan est l'utilisateur malveillant qui sait qu'un site particulier permet à des utilisateurs authentifiés d'envoyer de l'argent vers un compte particulier en utilisant des requêtes HTTP POST qui incluent le numéro de compte et le montant. Nathan construit un formulaire qui inclut son numéro de compte et un montant dans des champs cachés (invisibles) et le transmet à un autre utilisateur du site (avec le bouton de validation) déguisé en un lien vers un site "pour devenir riche".
Si un utilisateur clique sur le bouton de validation, une requête HTTP POST, contenant les informations de transaction, va être transmise au serveur ainsi que le cookie que le navigateur web associe au site (l'ajout à la requête du cookie associé au site est le comportement normal du navigateur). Le serveur va vérifier le cookie d'authentification, et l'utiliser pour déterminer si l'utilisateur est ou n'est pas connecté et donc permet ou non la transaction.
Au final tout utilisateur qui va cliquer sur le bouton de validation, alors qu'il sera connecté sur le site d'échange d'argent, va autoriser la transaction. Nathan va devenir riche !

d) Tableau comparatif

Nom	Importance	Difficulté a mettre en place	Risques
XSS	★★★★☆	★☆☆☆☆	-Risques de pertes des données
Injection SQL	★★★★★	★★★☆☆	-Mis en périls des données personnels -Risque de perte de donnée
CSRF	★★★★☆	★★★★★	-Risque d'action non autorisé

V Conclusion

La multiplicité des failles existantes et leur nombre croissant démontre bien la fragilité de nos systèmes d'informations. Ces dernières peuvent être plus ou moins sophistiqués et faire de grands dégâts, en particulier pour les plus grandes entreprises.

La sécurité des développements web est donc primordiale, et permet d'assurer qu'aucune information ne soit compromise entre le client et le serveur.

Il n'y a pas de faille plus importante qu'une autre car « Ce qui est sécurisé à 99% n'est pas sécurisé » (Michel Kartner, Le Blog du Hacker)