Université de Rouen

UFR Sciences et Techniques

Année-universitaire : 2019/2020

Projet Annuel

Thème : WebSSO

Premier travail

Les cookies

Client :

Mr Sofiane BENMEKKI

Master 1 Informatique Parcours SSI

Protocole http :

L'***Hypertext Transfer Protocol*** (**http**) est un protocole de communication client-serveur développé pour le World Wide Web. HTTPS (avec S pour *secured*, soit

« sécurisé ») est la variante du HTTP *sécurisée* par l'usage des protocoles SSL ou TLS.

Identification :

HTTP permet l'identification du visiteur par transmission d'un nom et d'un mot de passe.

Il existe deux modes d'identification :

- *Basic* et *Digest* (RFC 2617). Le premier mode transmet le mot de passe en clair, et ne doit donc être utilisé qu'avec le protocole HTTPS.
- Le deuxième mode permet une identification sans transmettre le mot de passe en clair. L'identification est cependant souvent effectuée par une couche applicative supérieure à HTTP.

Les cookies :

Un cookie est un petit fichier que l'on enregistre sur l'ordinateur du visiteur (disque dur). Ce fichier contient du texte et permet de retenir des informations sur le visiteur. Ce stockage est réalisé par votre navigateur.

Le cookie est envoyé, non pas comme une pièce jointe d'email, mais placé dans l'entête HTTP de la requête, tout comme une autorisation ou un type de contenu.

Les cookies ne sont pas des virus, juste ils sauvegardent des informations sur vos recherche par exemple et a la prochaine authentification, ils vont vous affichez uniquement des publicités sur ceux qui vous intéressent.

Généralement, chaque cookie stocke une information à la fois. Si vous voulez stocker le pseudonyme du visiteur de votre site et sa date de naissance, il est donc recommandé de créer deux cookies.

On peut afficher à l'intérieur du navigateur la liste des cookies qui sont stockés et on peut choisir de les supprimer à tout moment.

Chaque site web peut écrire plusieurs cookies. Chacun d'eux a un nom, une valeur et une date d'expiration. Après cette date, ils sont automatiquement supprimés par le navigateur. Donc, les cookies sont des informations temporaires qu'on stocke sur l'ordinateur des visiteurs.

lorsque le serveur reçoit une requête HTTP vierge de tout cookie, il en crée un et le transmet avec la réponse grâce à la fonction Set-Cookie. Le client reçoit la

réponse, crée le cookie dans un fichier texte, sur votre disque dur. A la prochaine connexion, il transmettra à Google.fr les informations contenues dans le cookie.

Ecrire un cookie :

Pour écrire un cookie, on utilise la fonction PHP **setcookie.** On lui donne en général trois paramètres, dans l'ordre suivant :

- Le nom du cookie
- La valeur du cookie
- La date d'expiration

Pour la date d'expiration, il faut ajouter au moment actuel qu'on peut l'obtenir on utilisant la fonction **time()** le nombre du secondes au bout duquel il doit expirer.

La sécurité :

Les cookies contiennent des données personnalisées de votre compte, de votre ordinateur. Les cookies sont donc des données sensibles d'un point de vue de la sécurité. Il faut donc les considérer comme des données personnelles que personne ne doit obtenir.

Vole de cookies :

Le but du hacker, est donc généralement de voler le cookie de sa victime pour en exploiter le contenu. Un cookie associé à un site web ne peut pas être envoyé à un autre site web. Malheureusement, un certain nombre de failles permettent de voler des cookies.

Vole par accès physique à la machine :
Si le hacker a accès physiquement à la machine, rien de plus simple que de récupérer les cookies ! Il va dans le répertoire de stockage des cookies en fonction du système d'exploitation et copie les cookies sur disquette.

Vole par sniffing / man in the middle
Comme nous l'avons vu, les cookies passent par les requêtes HTTP. Si l'attaquant peut intercepter les requêtes HTTP, soit à l'aide d'un sniffer, soit par attaque par le milieu, il peut donc récupérer tous les cookies sans aucun problème. A condition bien sur que le flux HTTP ne soit pas chiffré (HTTPS, VPN...).

Vulnérabilité du navigateur
Chaque nouvelle version, comporte un nombre de failles impressionnant. Parmi toutes ces failles, il y en a certaines qui concernent tout particulièrement les cookies.

Exploitation des cookies volés
Une fois qu'un hacker a votre cookie, il peut l'exploiter

Récupération des données d'authentification

- Un site bien connu a stocké le couple login/mot de passe de l'authentification, en clair dans le cookie ! Nul besoin donc d'être un hacker hors du commun pour comprendre qu'il est enfantin d'exploiter ces informations.

- Un autre superbe exemple d'une absence totale de protection des données sensibles : PHPNuke stocke le mot de passe Admin encodé en base 64 !

- Rappelons que "base 64" n'est pas un algorithme de chiffrement, mais un algorithme d'encodage de données. Rien de plus simple donc, pour décoder ce mot de passe.
  Référence : http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-08/0226.html

Les solutions

Côté client

- Désactiver les cookies. Mais beaucoup de sites web ont besoin de cette fonctionnalité pour leur propre fonctionnement, pénalisant l'internaute qui ne supporte pas les cookies.

Côté site web
La sécurité au niveau des cookies est à la charge du webmaster. Lui seul doit prendre en compte la sécurité de son site et des internautes qui le visite.

- Ne jamais stocker les informations concernant l'authentification de l'internaute en clair ou encodé.

- Si vous utilisez un ID de session, ne jamais faire un ID incrémenté "simplement".

- Utilisez un ID de session aléatoire.

- Utilisez un ID de session à chaque requête HTTP.
- Utiliser un système de dé-login qui efface le cookie.
- Vérifiez que vos cookies ne sont pas sensibles à une replay attack.
- Chiffrer les cookies : Un cookie peut être chiffré en partie ou en totalité. Mais attention, utilisez un chiffrement fort !
- Utilisez des protocoles sécurisés comme HTTPS.
- En aucun cas, un cookie ne doit être utilisé pour reconnaître automatiquement un internaute. Au mieux, un internaute devra, à chaque visite de votre site, s'authentifier pour recevoir un nouveau cookie.

Références :

- *Wikipedia*
- *Openclassroom*
- *Sécurité info*