

## TP Cookies – Bloc 3

### Questions 1 :

**Un cookie est une petite portion de données stockée par un serveur web sur le dispositif d'un utilisateur, tel qu'un ordinateur ou un téléphone, et est associé à un domaine internet spécifique (qui correspond généralement à l'ensemble des pages d'un site web unique). Les cookies ont été initialement conçus pour fournir aux sites web une certaine forme de mémoire, en facilitant l'interaction entre l'utilisateur et le site, et en améliorant l'expérience utilisateur en la rendant plus fluide et personnalisée.**

### **Exemple d'un cookie**



**Si vous voulez consulter vos cookies sur le site en consultation il faut faire un clic droit sur la page et faire « Inspecter ». Ensuite une fenêtre spécifique s'ouvre à gauche, il faut aller dans l'onglet « Application ». Ensuite il y aura une section « Cookies » qui contiendra tous les cookies du site web en question. En cliquant sur un cookie vous pourrez le voir en détail. C'est une opération simple qui ne demande pas de grandes capacités informatiques. Mon navigateur internet contient 167 Mo.**

### **Question 2 :**

**Les cookies sont essentiels bien qu'ils soient très peu connus des gens, ils permettent d'adapter les pubs ou autres en fonction de l'utilisateur. Même si ce processus peut être mis en doute en termes de confidentialité. Heureusement que le RGPD (Règlement Général sur la Protection des Données) est là !**

**Entré en vigueur en 2018, le RGPD impose des règles strictes sur la collecte et l'utilisation des données personnelles, en l'occurrence ici les cookies. Cela permet d'avoir l'accord de l'utilisateur avant d'utiliser certains cookies même s'il y a certains cookies obligatoires**

### **Questions 3 :**

**Les cookies, bien qu'utiles, peuvent poser des problèmes de sécurité et de confidentialité si leur utilisation est mal gérée ou exploitée par des attaquants malintentionnés. Voici quelques types d'attaques possibles :**

**Vol de cookies : Une attaque par vol de cookies consiste à intercepter les cookies d'un utilisateur pour accéder à ses sessions sur des sites web. Cela peut être réalisé par le biais d'une attaque dite "man-in-**

**the-middle", où l'attaquant intercepte la communication entre l'utilisateur et le site web.**

**Attaque par injection de cookies : L'attaquant peut créer un cookie malveillant et le placer dans le navigateur de l'utilisateur. Lorsque l'utilisateur visite ensuite le site web ciblé, le cookie malveillant peut être utilisé pour exécuter des actions non autorisées.**

**Cross-Site Scripting (XSS) : Le XSS est une faille de sécurité qui permet à un attaquant d'injecter du code malveillant dans les pages web vues par d'autres utilisateurs. Ce code malveillant peut être utilisé pour voler des cookies et accéder aux sessions de l'utilisateur.**

**Cross-Site Request Forgery (CSRF) : Dans une attaque CSRF, un attaquant peut forcer un utilisateur à exécuter des actions non désirées sur un site web sur lequel il est authentifié. Si le site fait confiance au cookie pour l'authentification, il pourrait alors exécuter l'action non désirée sans le savoir.**

Enfin, du point de vue de la confidentialité, certains cookies peuvent être utilisés pour suivre l'activité en ligne d'un utilisateur sur plusieurs sites web, ce qui peut être considéré comme une invasion de la vie privée. C'est pourquoi la régulation, comme le RGPD en Europe, a été mise en place pour protéger les utilisateurs

#### **Question 4 :**

*En analysant ces captures on voit qu'il existe des designs divers et variés pour les fenêtres de cookies. Selon le site elle sont plus ou moins grosses, plus ou moins détaillées et aussi plus ou moins modifiables. Certaines fenêtre offre une possibilité de choisir quelles informations peuvent être retenue (la plupart du temps il a forcément une option obligatoire). Certaines fenêtres sont agressives et prennent tout l'écran, ce qui n'est pas très accueillant pour un site web.*

*En conclusion il existe des variétés mais toutes ces fenêtres ont un seul et même but : avertir l'utilisateur et lui demander son accord pour utiliser ses données et être transparent avec celui-ci.*

#### **Question 5 :**



Continuer sans accepter

### **MS Corporation respecte votre vie privée**

Avec votre accord, nos partenaires et nous utilisons des cookies ou technologies similaires pour stocker et accéder à des informations personnelles comme votre visite sur ce site. Vous pouvez retirer votre consentement ou vous opposer aux traitements basés sur l'intérêt légitime à tout moment en cliquant sur "En savoir plus" ou dans notre politique de confidentialité sur ce site.

### **Avec nos partenaires, nous traitons les données suivantes :**

Données de géolocalisation précises et identification par analyse du terminal, Publicités et contenu personnalisés, mesure de performance des publicités et du contenu, données d'audience et développement de produit, Stocker et/ou accéder à des informations sur un terminal

[En savoir plus](#) [Accepter & Fermer](#)

Le logo est un logo qui m'appartient.