



TP CYBERSÉCURITÉ : COOKIE

Objectif : découvrir les cookies, les repérer, mieux comprendre les messages relatifs au RGPD, faire du privacy-by-design

I. Question 1 :

- a. Qu'est-ce qu'un cookie dans le sens informatique du terme ? Montrez un exemple de contenu d'un cookie.

Un cookie est un petit fichier stocké par un serveur dans le terminal (ordinateur, téléphone, etc.) d'un utilisateur et associé à un domaine web (c'est à dire dans la majorité des cas à l'ensemble des pages d'un même site web). Ce fichier est automatiquement renvoyé lors de contacts ultérieurs avec le même domaine. (Définition issu du site de la [Cnil](#)).

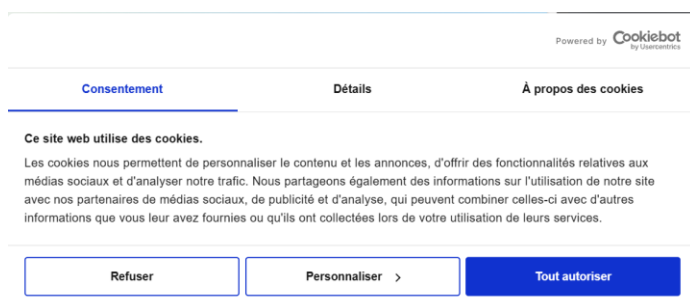


Figure 1: Cookie du site Cookiebot.com

Les cookies sont habituellement utilisés pour stocker des informations sur la session de l'utilisateur, les préférences du site, ou d'autres données utiles pour améliorer l'expérience de navigation.

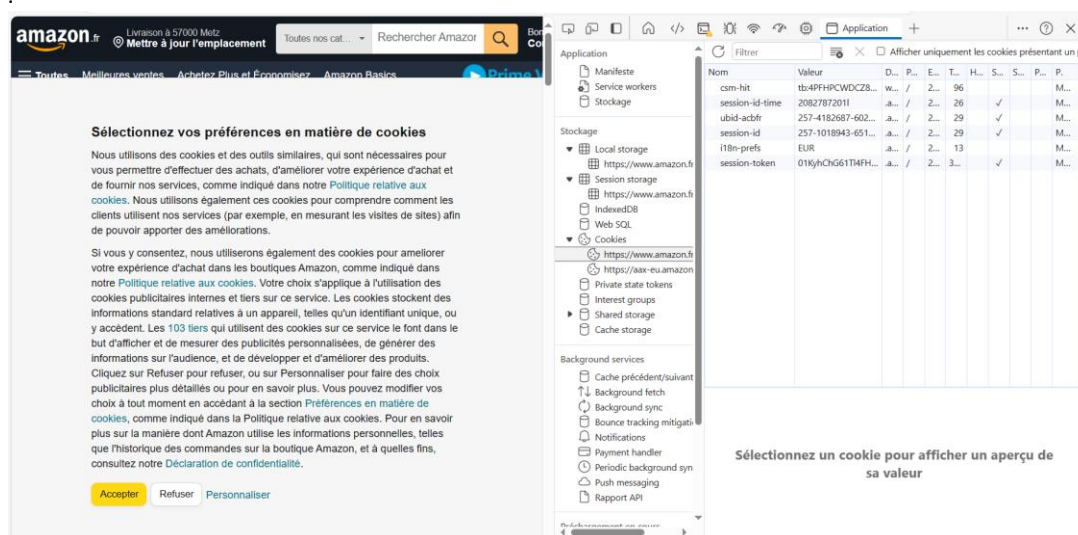


Figure 2: Cookies sur Amazon

b. Comment le lire quand on navigue sur Internet ? Est-ce une opération simple ?

Lire un cookie n'est pas une opération simple du côté navigateur car l'accès à ces informations sont souvent limité et sécurisé.

Mais il existe des moyens de contourner cette sécurité avec par exemple un [script java](#).

c. Comment lister tous les cookies en place dans un navigateur ? Quelle quantité de cookies avez-vous dans votre navigateur ?

Pour accéder aux cookies d'un navigateur (ici Edge), il suffit de cliquer sur les trois petits points en haut à droite puis paramètre, Cookies et autorisation de site, Cookie et données du site et enfin Tous les cookies et données du site.

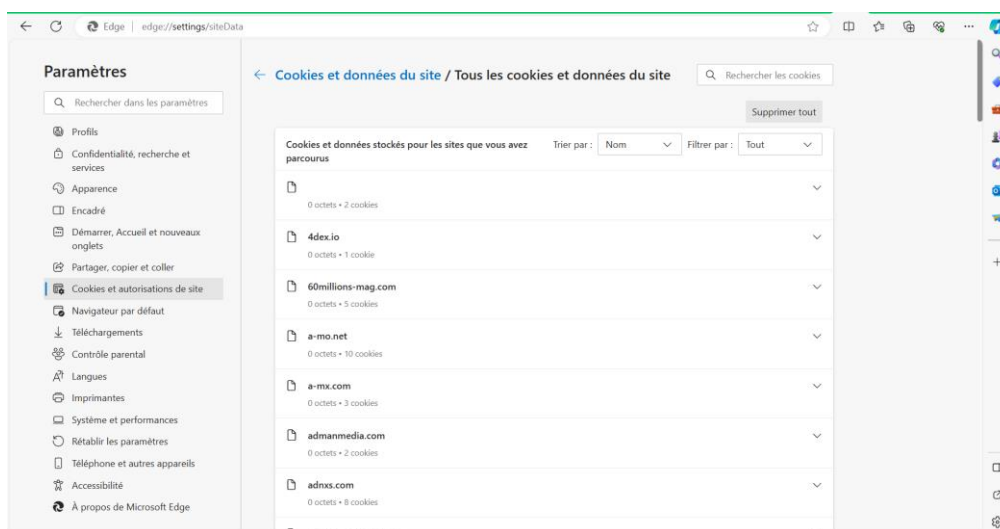


Figure 3: Listes des Cookies sur Edge

Comme on peut le voir ci-dessous, il y a 77 cookies de sites enregistrés sur le navigateur Edge.

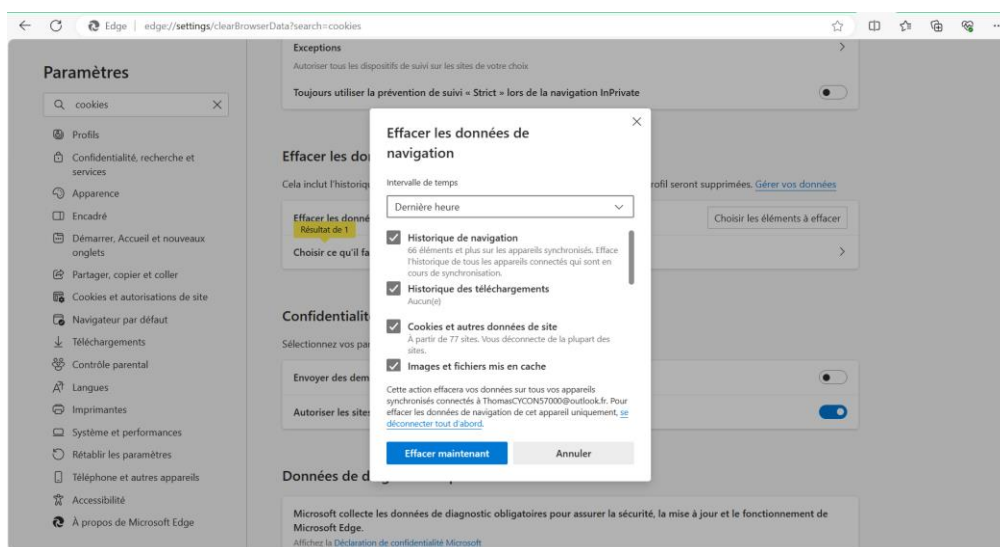


Figure 4 : Nombre de Cookies sur un navigateur

II. Question 2 :

a. Quels enjeux tournent autour de ces fichiers ?

Les cookies sont utilisés pour diverses opérations comme le stockage d'information de session, le suivi des préférences et paramètres, les publicités ciblées ...

Or malgré ces avantages, les cookies posent problèmes aux questions de confidentialité visant à protéger la vie privée des utilisateurs.

b. En quoi le RGPD change la donne ?

Les cookies étaient avant le RGPD gérés par les sites, il n'y avait pas de réglementation spécifique donc les sites web étant libres, les avertissements de cookies ou les pop-ups n'étaient pas toujours visibles ou claires. C'est pour cela qu'entre en jeu le Règlement Général sur la Protection des Données (RGPD) qui oblige les sites web à respecter la vie privée des utilisateurs.

[La CNIL met à disposition un site](#) pour mettre son site en conformité selon le RGPD.

III. Question 3 :

a. Quels dangers gravitent autour de ces fichiers ?

Les sites de vente en ligne les utilisent massivement pour afficher des publicités ciblées en fonction de l'historique de navigation de l'internaute. Les cookies de suivi, qui ont une durée de vie illimitée et collectent toutes les informations concernant la navigation de l'utilisateur, sont utilisés pour obtenir un profil marketing détaillé. Il est courant que ces procédés se fassent sans que l'utilisateur en soit informé, et qu'il n'ait en général pas conscience des informations récupérées en rapport avec son profil.

« [Information provenant du site JDN](#) »

b. Quelles attaques sont possibles ?

Une récupération des cookies qui attire aussi les pirates : l'objectif étant pour eux d'en exploiter le contenu et d'utiliser ces données personnelles à des fins malveillantes pouvant aller jusqu'à la mise en place de cyberattaques. Le processus est relativement simple : si le pirate a un accès physique à la machine il lui suffit de copier ces données, accessibles en quelques clics, sur une clé USB. A distance la récupération des cookies est aussi plutôt aisée, puisqu'il suffit d'intercepter une requête HTTP par laquelle passent les cookies, à l'aide de techniques de type « sniffing ». L'utilisation des failles du navigateur sont aussi utilisées pour le vol de cookies : Firefox permet par exemple de récupérer les cookies en créant un site pirate qui aspire les cookies du site visé.

Selon les documents publiés par Edward Snowden en décembre 2013, la NSA a utilisé ces techniques pour surveiller la vie des internautes.

« [Information provenant du site JDN](#) »

IV. Question 4 :

a. Analysez les captures réalisées et fournies avec ce TP. Que pouvez-vous en dire ?

On peut voir que tous les cookies présentés sont assez différents les uns des autres, de plus ils n'offrent pas tous le même niveau d'information.

Sur certains on peut modifier les informations relevées par le cookie d'autres non.

D'autres ne nous offrent même pas le choix de refuser car le refus se fait sous la forme d'un abonnement payant.

b. Complétez avec d'autres captures de votre composition et tirez-en une conclusion



Votre vie privée est importante pour nous !

Lorsque vous visitez notre site, des compagnies pré-sélectionnées peuvent accéder à certaines informations sur votre appareil et sur cette page Web et les utiliser pour diffuser des annonces pertinentes ou du contenu personnalisé. Veuillez noter que ces annonces nous permettent de maintenir notre service gratuit. Les données à caractère personnel seront traitées sur la base du consentement conformément à l'article 6 (1) (a) du cadre du RGPD dans **le droit communautaire**, ou en tant qu'intérêt légitime conformément à l'article 6 (1) (f) de ce même cadre.

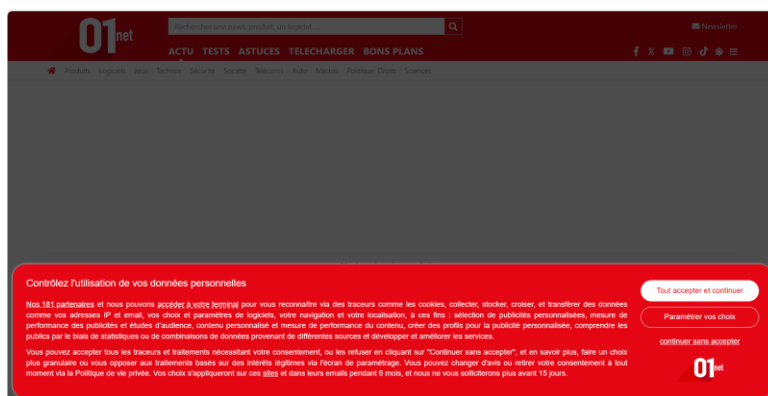
Comprenez pourquoi vous voyez cela

Nous, l'« Éditeur », et un groupe restreint de **partenaires de confiance** (796), dénommés « Fournisseurs », avons besoin de votre consentement à des fins de traitement des données. Ces objectifs incluent de stocker et/ou accéder à des informations stockées sur un terminal, comme la gestion des cookies et pour traiter des données personnelles telles que les informations standard envoyées par un terminal et d'autres identifiants uniques à des fins de publicités et contenu personnalisés, mesure de performance des publicités et du contenu, données d'audience et développement de produit. Avec votre consentement, nous et nos partenaires pouvons utiliser des données de géolocalisation précises et analyser activement les caractéristiques du terminal pour l'identification.

Vous pouvez consentir au traitement décrit ci-dessus ou accéder à des informations plus détaillées et personnaliser vos choix. Le consentement donné ne s'appliquera qu'à ce site. Veuillez prendre en considération que le traitement de

Personnalisez vos choix

Accepter tout et consulter le site



[Continuer sans accepter →](#)



Ce site web et [ses partenaires](#) utilisent des traceurs pour afficher et personnaliser des contenus, les partager sur les réseaux sociaux, visualiser des contenus multimédia, mesurer l'audience et cibler des annonces sur des sites tiers. Vous pouvez les accepter ou les refuser. Vous pourrez revenir sur votre choix en cliquant sur « Gérer mes cookies » en bas de page. Si vous cliquez sur « Continuer sans accepter », des traceurs exemptés du recueil du consentement seront déposés. Vous pouvez vous y opposer en cliquant sur « Paramétrer les cookies » et en désactivant le bouton prévu à cet effet. [En savoir plus sur l'utilisation des cookies.](#)

Paramétrer les cookies

Accepter

Comme on peut le voir tous les cookies sont différents avec plus ou moins d'information et la possibilité ou non de les accepter

V. Question 5 (BONUS) :

- a. Conclusion étant tirée, réalisez une maquette correcte adaptée à un site Internet e-commerce. Esquissez le cahier des charges qui permet de valider ou non votre création ou celle de vos camarades

Cahier des Charges :

Un cookie doit avoir (information provenant du site developer.mozilla.org)

- ✓ Un Nom afin de pouvoir l'identifier
- ✓ Une Valeur qui représente l'information associé au nom
- ✓ Une Date d'expiration ou de durée de vie
- ✓ Un domaine et chemin du cookie
- ✓ Sécurité et attribut http-Only

Une bannière de cookie doit obligatoirement :

- ✓ Informer l'utilisateur sur l'ensemble des finalités d'usages liées aux traceurs et une liste, régulièrement mise à jour, des responsables du ou des traitements de données accessible directement ou indirectement (via lien hypertexte) sur le premier niveau d'information
- ✓ Permettre à l'utilisateur de consentir par un acte positif clair
- ✓ Permettre à l'utilisateur de faire un choix par finalité, il est recommandé de permettre à l'utilisateur de donner son consentement de façon indépendante et spécifique pour chaque finalité, par exemple au moyen de cases à cocher. Il est possible de proposer à l'utilisateur de consentir de manière globale à un ensemble de finalités, en intégrant, par exemple, des boutons « tout accepter » ou « tout refuser », mais uniquement si l'ensemble des finalités est présenté préalablement.
- ✓ Permettre à l'utilisateur d'exercer ses choix avec le même degré de simplicité : La CNIL recommande que le choix exprimé par les utilisateurs, qu'il s'agisse d'un consentement ou d'un refus, soit enregistré de manière à ne pas les solliciter à nouveau pendant un certain laps de temps. Une durée de six mois, tant pour le consentement que le refus est en général appropriée.
- ✓ Permettre à l'utilisateur de revenir sur sa décision à tout moment

Gérer mes cookies

Nous conservons votre choix pendant 6 mois. Vous pouvez changer d'avis à tout moment en cliquant sur l'icône "gérer les cookies" en bas à gauche de chaque page de notre site

TOUT REFUSER TOUT ACCEPTER

- Publicité personnalisée**
Notre site E-commerce.fr et nos partenaires, en utilisant des traceurs afin d'afficher de la publicité personnalisée en fonction de votre navigation et de votre profil
Afficher plus d'information
- Publicité géolocalisée**
Notre site E-commerce.fr et nos partenaires, en utilisant des traceurs pour vous adresser de la publicité en fonction de votre localisation?
Afficher plus d'information
- Partage sur les réseaux sociaux**
Notre site E-commerce.fr et nos partenaires, en utilisant des traceurs pour vous permettre de partager sur les réseaux sociaux
Afficher plus d'information

[Consulter la politique cookies](#) **VALIDER MES CHOIX**

Figure 5 : Exemple de Cookie qui respectent les lois de la RGPD

Autres exemples provenant du site de la CNIL

