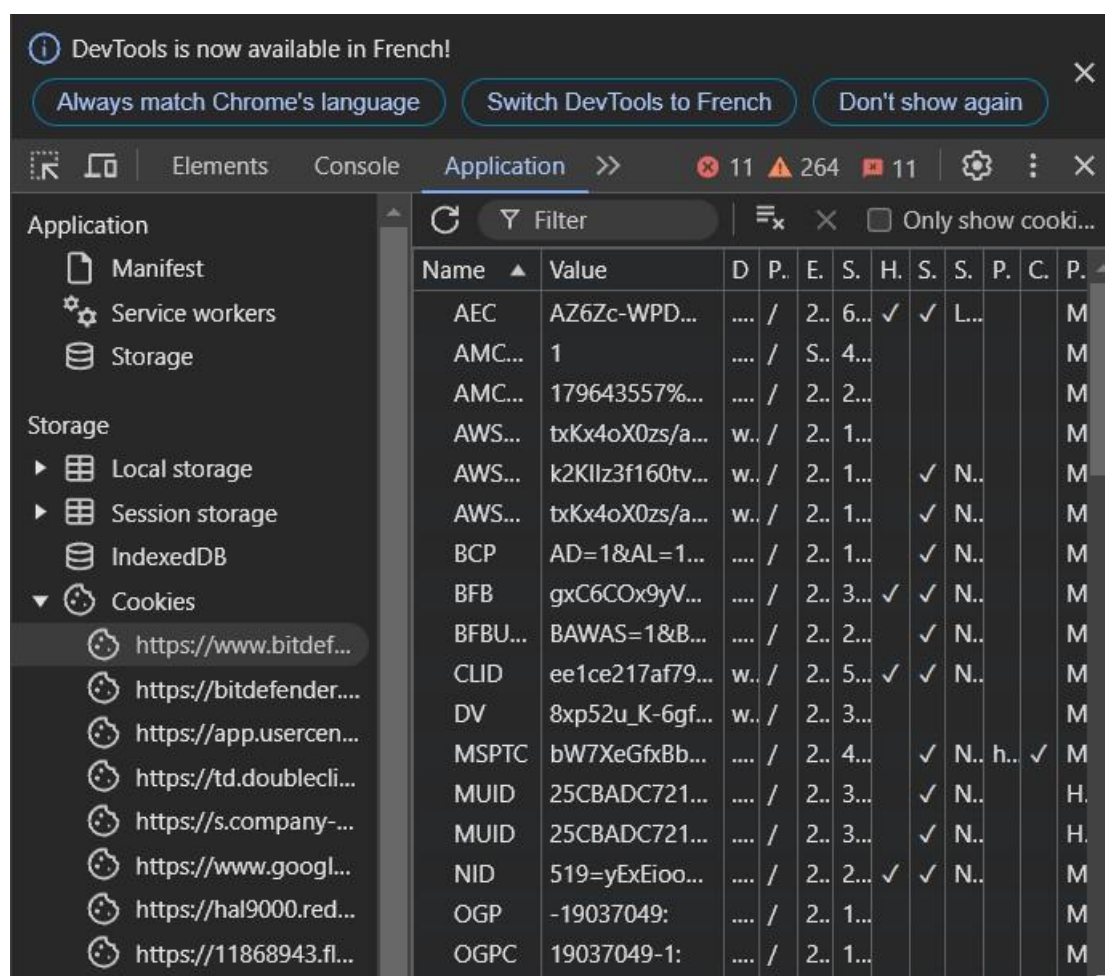


Qu'est-ce qu'un cookie dans le sens informatique du terme ?

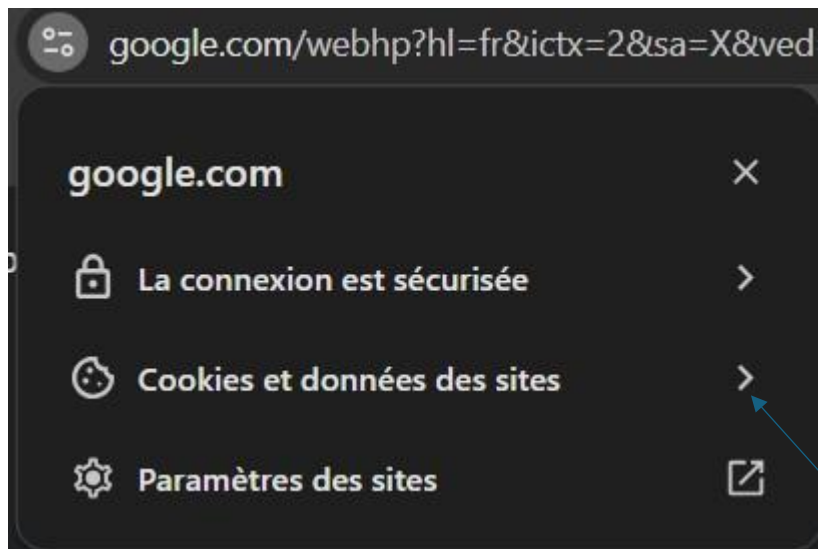
Un cookie, en informatique et plus précisément sur le web, est un petit fichier texte que les sites web enregistrent sur l'appareil d'un utilisateur (ordinateur, smartphone, etc.) lorsqu'il visite ces sites. Voici un exemple concret de contenu d'un cookie



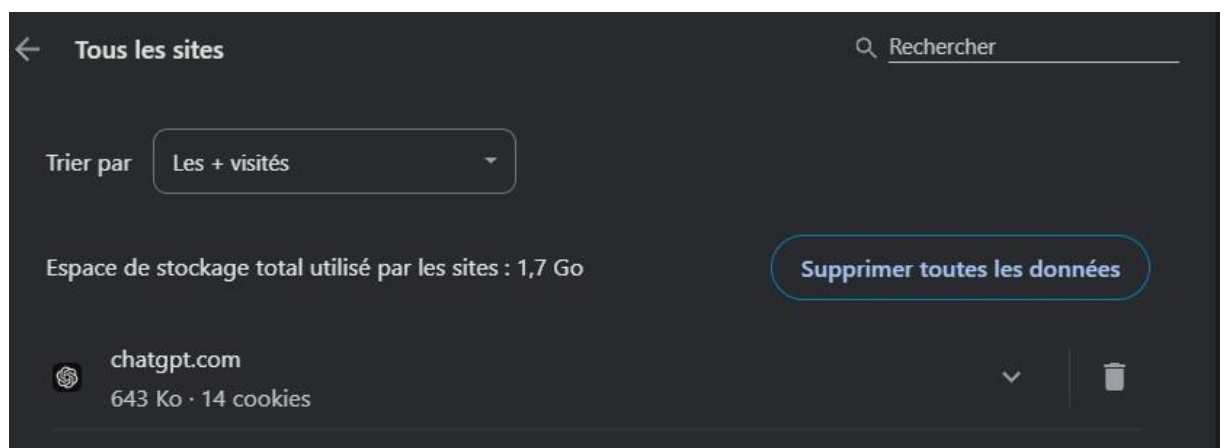
Source : <https://www.bitdefender.fr/consumer/support/answer/48120/?srsId=AfmBOogEyfvKJvTLO2qWEGrPv6boTti2mpulXvU1dFuaFXuIPTSrcALP>

C'est une opération plutôt simple de lire un cookie sur internet, généralement lorsqu'on entre sur n'importe quel site c'est généralement afficher en bas de de page.

Pour lister la quantité de cookie dans un navigateur :



Les quantités de cookies dans mon navigateur est de 1,7 Go



Quels enjeux tournent autour de ces fichiers ? En quoi le RGPD change la donne ?

Les cookies, essentiels pour le web, posent des enjeux de vie privée, sécurité et conformité. Ils permettent le suivi des comportements et le ciblage publicitaire, mais doivent être utilisés avec transparence et consentement, notamment sous le RGPD. Les cookies non sécurisés peuvent être exploités lors d'attaques. L'évolution vers des alternatives sans cookies tiers, comme le Privacy Sandbox, vise à protéger la vie privée tout en maintenant la performance.

Quant à la RGPD, celle-ci impose des règles strictes sur la gestion des cookies en exigeant un consentement explicite des utilisateurs avant leur utilisation. Il renforce la transparence, le contrôle des données personnelles et la responsabilité des entreprises, sous peine de sanctions en cas de non-respect.

Quels dangers gravitent autour de ces fichiers ? Quelles attaques sont possibles ?

Outre les problèmes de confidentialité, les cookies tiers peuvent également présenter des risques pour la sécurité. Ils peuvent être utilisés par des acteurs malveillants à des fins préjudiciables, comme le suivi des utilisateurs pour voler des données à caractère personnel ou propager des logiciels malveillants.

Source : <https://www.gerrishlegal.com/blog-fr/quels-sont-les-risques-lis-aux-cookieters-#:~:text=Outre%20les%20probl%C3%A8mes%20de%20confidentialit%C3%A9,ou%20propager%20des%20logiciels%20malveillants.>

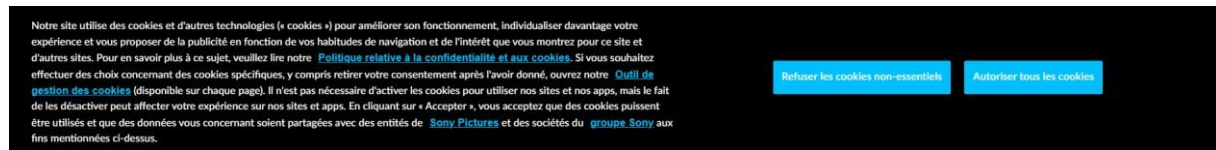
Les attaquants peuvent intercepter les cookies avant leur renvoi vers le serveur pour en extraire des informations ou pour les modifier. De faux cookies peuvent également être entièrement créés afin d'usurper l'identité d'un utilisateur pour accéder à des données supplémentaires. Source :

https://www.f5.com/fr_fr/glossary/cookiepoisoning#:~:text=Les%20attaquants%20peuvent%20intercepter%20les,acc%C3%A9der%20%C3%A0%20des%20donn%C3%A9es%20suppl%C3%A9mentaires.

Analysez les captures réalisées et fournies avec ce TP. Que pouvez-vous en dire ? Complétez avec d'autres captures de votre composition et tirez-en une conclusion. Vos autres captures pourront être rajoutées dans ce répertoire afin que tout le monde en profite.

La conformité des sites web au respect des données des utilisateurs varie. Certains respectent les réglementations, comme le RGPD, en obtenant un consentement clair pour l'utilisation des cookies et en offrant une transparence sur la collecte de données. Permettant en revanche, ne respectent pas pleinement la loi, pratiquant des méthodes opaques, ne

permettant pas toujours aux utilisateurs de contrôler leurs données ou partageant des informations sans consentement explicite. Cette absence de respect des règles peut entraîner des sanctions et une perte de confiance des utilisateurs.



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.

Checklist :

Activer les cookies uniquement après consentement : Aucun cookie nécessitant le consentement ne doit être activé avant l'autorisation explicite de l'utilisateur.

Obtenir un consentement explicite : L'utilisateur doit effectuer une action claire, comme cliquer sur un bouton, pour accepter les cookies.

Fournir une information claire et accessible : Expliquez en termes simples pourquoi les cookies sont utilisés, leur finalité et les données collectées. Proposez :

- Une bannière concise pour un aperçu rapide.
- Un niveau détaillé accessible pour des informations approfondies.

Permettre le retrait du consentement à tout moment : Offrez une option simple et visible pour que l'utilisateur puisse modifier ou retirer son consentement.