Formation snt – version alpha confidentialité
Activité confidentialité

Contenus	Capacités attendues
Identité numérique, e-réputation, identification, authentification	Connaître les principaux concepts liés à l'usage des réseaux sociaux.
Réseaux sociaux existants	Distinguer plusieurs réseaux sociaux selon leurs caractéristiques, y compris un ordre de grandeur de leurs nombres d'abonnés. **Paramétrer des abonnements pour assurer la confidentialité de données personnelles.**
Modèle économique des réseaux sociaux	Identifier les sources de revenus des entreprises de réseautage social.
Rayon, diamètre et centre d'un graphe	Déterminer ces caractéristiques sur des graphes simples.
Notion de « petit monde »	Expérience de Milgram Décrire comment l'information présentée par les réseaux sociaux est conditionnée par le choix préalable de ses amis.
Cyberviolence	Connaître les dispositions de l'article 222-33-2-2 du code pénal. Connaître les différentes formes de cyberviolence (harcèlement, discrimination, sexting...) et les ressources disponibles pour lutter contre la cyberviolence.

Table des matières

Activité confidentialité

Notes d’intention

La partie **Web** aborde les thèmes de cookies (fichiers installés par les sites sur votre ordinateur et contenant des informations diversement utiles pour les fonctionnalités des sites). On peut également parler dans cette partie Web des sociétés proposant un **suivi du trafic** de votre site Web gratuitement mais enregistrant un nombre incroyable de données sur les internautes. Ou des sociétés certifiant le **https** qui récupère de part le fonctionnement du https les demandes de connexions aux différents sites dont ils garantissent l’identité.

La partie **Internet** montre qu’on peut encore récupérer des informations à l’aide du réseau lui-même.

Mais une partie importante des fuites d’informations vient de l’utilisateur lui-même, notamment à cause d’une auto-diffusion très libérale sur les réseaux sociaux. Dans le même temps, une absence de présence sur les réseaux sociaux peut nous exposer à une usurpation d’identité ou à un manque totale de visibilité sur ce qui est dit.

Une des solutions est donc d’être présent sur les réseaux sociaux mais de contrôler ce qu’on montre ou non.

Or, il existe une multitude de réseaux sociaux et il serait illusoire de traiter de cette partie sur tous les réseaux où les élèves sont présents.

Le principe choisi est donc de présenter le principe de la confidentialité, du RGPD et de demander aux élèves de réaliser une fiche sur le réseau de leur choix.

Par contre, il doit être difficile de réellement comprendre le principe de ces filtrages sans rien comprendre au principe des sites dynamiques et aux tests réalisables. Une partie de ce document est donc dédié à des explications rapides visant à fournir une vision générale pas trop fausse sans rentrer dans trop de détails techniques.

Confidentialité sur les réseaux sociaux

I – Informations diffusées via les réseaux sociaux

Les réseaux sociaux ne reposent sur aucune contrainte organisationnelle : chacun peut s'organiser comme il le souhaite. Il existe donc autant de structures et de gestion de confidentialité que de réseaux sociaux différents.

Qu'est-ce qu'un réseau social ?

Un réseau social (informatique) est d'abord un **média social** : un dispositif permettant aux utilisateurs

- d'écrire du contenu
- de le partager
- en utilisant un outil technologique moderne.

Ce qui rend le réseau social informatique est le fait qu'il permettre la mise en relation des individus (contacter, commenter, liker …) et permet donc de créer des communautés virtuelles.

Par sa définition même, un réseau social doit donc enregistrer des données sur ses membres et permettre de les diffuser.

[Image CC3.0 – BY – SA : Grandjean, Martin (2014), auteur de « la connaissance est un réseau », les cahiers du numérique]

Contrôler les flux de données pour savoir qui voit quoi est donc extrêmement important.

01° Citez 2 réseaux sociaux et décrire rapidement le type de contenu transmis par l'utilisateur (et donc enregistré par le site).

Pourquoi doit-on surveiller ce qu'on publie ?

Il a d'abord le fait que ce que vous publiez risque d'être consultable pendant très longtemps. La persistance de l'information rend ce qu'on publie d'autant plus critique qu'on ne sait pas quand nous allons la voir ressortir. Une phrase écrite lorsque vous aviez 15 ans peut ressurgir 10, 15 ou 20 ans plus tard.

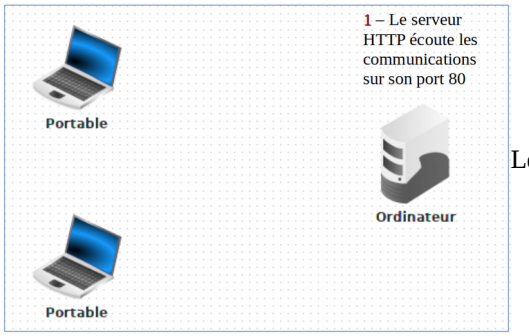
De la même façon, une photo peut être facilement enregistrée et ensuite diffusée sans que vous en ayez le moindre contrôle...

Dernier point : la Loi. Lorsqu'on écrit sur un site, il s'agit d'une publication. Or, le droit différencie les publications à public restreint, à public ciblé ou à diffusion massive. Savoir qui peut voir vos messages ou vidéos est donc d'autant plus important. En cas de plainte, la catégorie de diffusion aura un impact non négligeable sur la peine éventuelle.

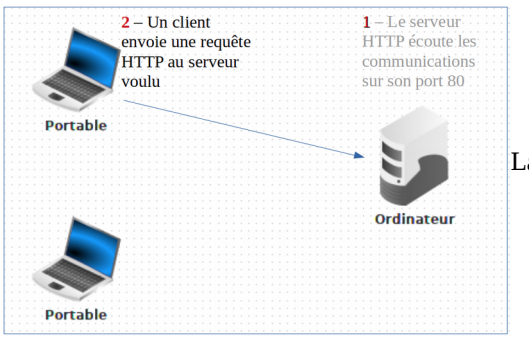
II – Gestion par les sites de réseaux sociaux

Les sites de réseaux sociaux ne sont pas des sites statiques : les pages visualisées ne sont pas des pages HTML stockées en dur sur le serveur. Il s'agit bien de **sites dynamiques** où le serveur interagit avec un programme de gestion et une base de données.

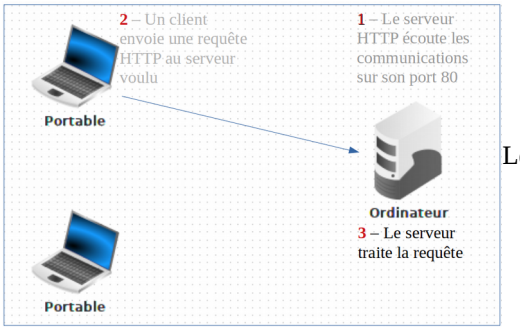
Pour rappel, voici comment réagit un **site statique** en HTTP :



Le serveur HTTP est en route et reste à l'écoute des communications.

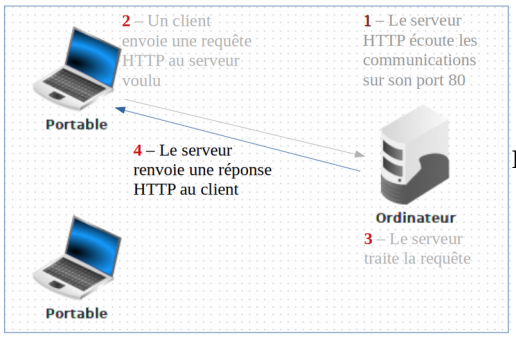


La requête contient le nom de la ressource voulue.



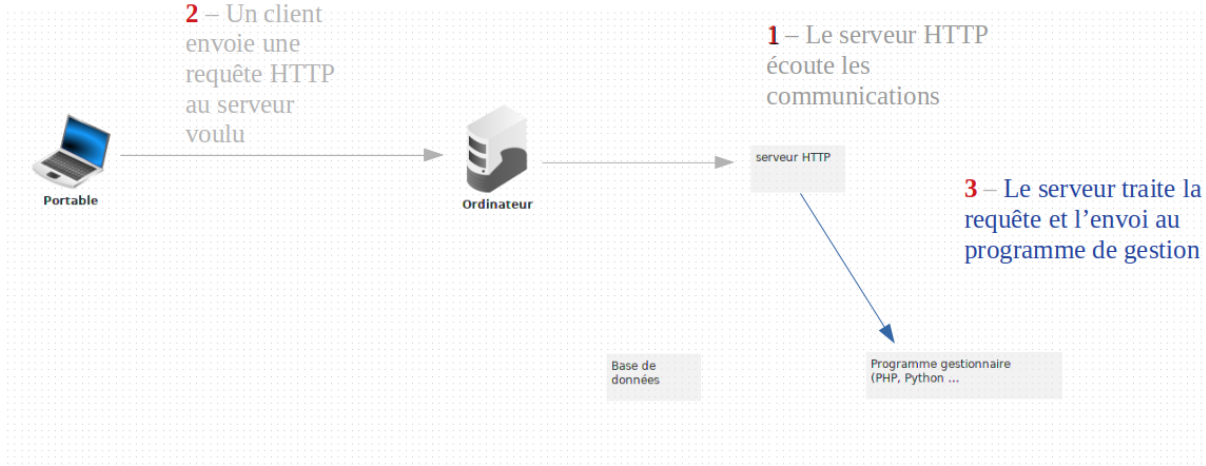
Le serveur vérifie si la ressource existe en mémoire.

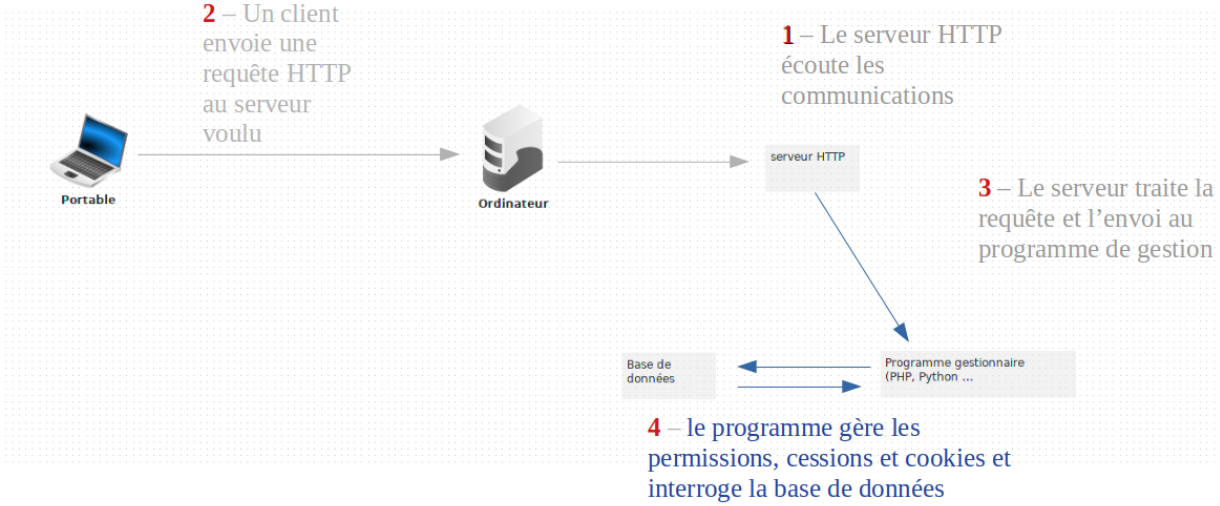
Si elle existe, il la transmet avec un code HTTP 200. Sinon, il transmet un code HTTP 404.

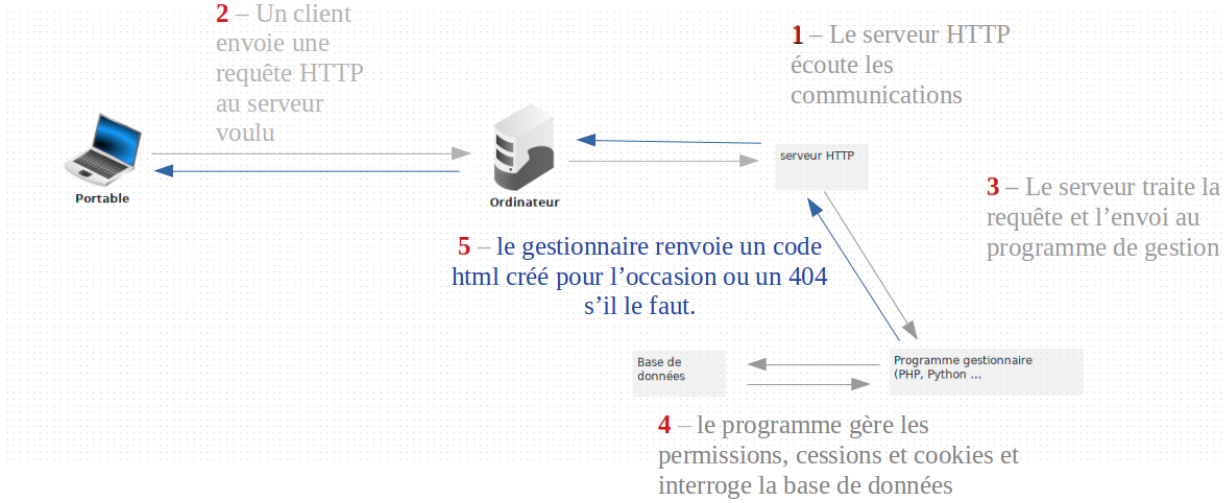


Dans tous les cas, une réponse HTTP est renvoyée.

Dans le cas des **sites dynamiques**, c'est un peu plus compliqué : il faut enregistrer les contenus et informations que le client veut transmettre, il faut les traiter, consulter ou modifier la base de données et créer la page HTML à la volée. Cela veut dire que la page est construite dynamiquement : l'ordinateur va générer un code HTML, la page n'est pas juste transmise à partir d'un fichier préexistant.







02° Si votre image est stockée dans une base de données, est-il possible de la transmettre sous condition ? Peut-on empêcher l'utilisateur d'avoir accès à son propre contenu ?

03° Complétez le code ci-dessous pour qu'il ne permette l'accès au contenu qu'à l'administrateur du site.

```
# Contient la ressource que l'utilisateur a envoyé sur le site, un jour
ressource = "Voici le message que l'utilisateur a envoyé un jour sur le site."
refus = "La ressource n'existe pas ou n'est pas accessible..."

# La variable membre contient le statut du membre. Valeur possible :
# 'admin', 'createur', 'contact' ou 'inconnu'
statut = 'admin'

print("Bonjour, vous avez actuellement le statut suivant :")
print(statut)
```

```
if statut == 'admin':
    print(refus)
elif statut == 'createur':
    print(refus)
elif statut == 'contact':
    print(refus)
elif statut == 'inconnu':
    print(refus)
```

Cette façon de faire n'est pas forcément adaptée : c'est clair pour un humain mais cela va être long de faire les cas un par un si on désire que certaines ressources soient accessibles à tous, d'autres aux contacts …

Il faut alors plutôt se demander comment gérer cela de façon facilement compréhensible par l'ordinateur.

Pour cela, nous allons plutôt créer une codification chiffrée :

```
statut = 01 # le statut est inconnu : c'est le plus petit rang
statut = 02 # un membre faisant parti des contacts du créateur de la ressource
statut = 03 # le créateur de la ressource
statut = 04 # un membre de l'administration du site
```

Ensuite, on peut créer une variable `autorisation` pour chaque ressource :

```
autorisation = 01 # tout le monde peut voir la ressource
autorisation = 02 # les contacts, le créateur et l'administration peut voir la ressource
autorisation = 03 # le créateur et l'administration peut voir la ressource
autorisation = 04 # seule l'administration peut voir la ressource
```

Nous pourrons ainsi gérer facilement tous les cas de figures à l'aide de quelques lignes de code simplement :

04° Complétez le code ci-dessous pour qu'il permette ou non l'accès au contenu en utilisant les variables `membre` et `autorisation`. Faire différents tests en faisant varier les valeurs attribuées à `membre` et `autorisation`. Il faudra remplacer `???` par l'un des cas suivants : **<** ou **<=** ou **>** ou **>=** ou **==**.

```
# Les informations sur le ressource : son contenu et le type d'accès autorisé
ressource = "Voici le message que l'utilisateur a envoyé un jour sur le site."
autorisation = 03

# Le message en cas de refus d'accès
refus = "La ressource n'existe pas ou n'est pas accessible..."

# La variable membre contient un nombre caractérisant le statut du membre demandant l'accès
membre =  02

print(f"Bonjour, vous avez actuellement le statut {membre}")
if membre ??? 'admin':
    print(ressource)
else:
    print(refus)
```

05° Moralité : le fait de supprimer un contenu sur sa propre page veut-il dire que le contenu est réellement supprimé de la base de données ?

III – RGPD

Depuis 2018, le règlement général sur la protection des données (RGPD) responsabilise les organismes publics et privés qui traitent les données des citoyens européens. Que la société soit européenne ou non.

Les grands principes du RGPD sont :

- le consentement : le site doit demander l'autorisation d'enregistrer vos données.
- la transparence : l'entreprise doit expliquer ce qu'elle fait des données enregistrées.

- le droit des personnes : les utilisateurs doivent pouvoir récupérer leurs données pour les porter sur un autre site, doivent disposer d'un droit à l'oubli …
- la responsabilité : les sociétés doivent nommer un responsable des données, signaler aux utilisateurs les fuites d'informations personnelles et doivent concevoir des systèmes de traitement protégeant les données de part la conception même du système.

IV – Confidentialité et réseaux sociaux

Il existe trop de réseaux sociaux pour parvenir présenter de façon excaustive la gestion des paramètres de confidentialité. Il existe quelques critères nous permettant de classifier les réseaux sociaux.
Nous allons ici nous attarder sur les critères suivants :

1. Thème global du réseau social : quel est le type de communauté qu'il tente de fédérer ?
2. Informations nécessaires à transmettre lors de la création du compte
3. Moyens de se connecter (mot de passe, email, numéro de téléphone . . .)
4. Contributions principales réalisées par les membres du réseau (textes, photos, vidéos . . .)
5. Contenus publiés par un membre accessibles par quelqu'un d'extérieur (non connecté au réseau social)
6. Contenus publiés par un membre accessibles par quelqu'un du même réseau social
7. Contenus publiés par un membre accessibles par quelqu'un du réseau reconnu comme fiable (ami, contact…)
8. Le système d'identification permet-il de s'identifier sur d'autres applications ou sites ?
9. Comment restreindre les droits d'accès de vos contenus sur le réseau social choisi ? Quels sont les choix disponibles ?

06° Chaque groupe devra travailler sur le réseau social de son choix et devra réaliser un diaporama incluant au moins une diapositive pour chacun des 9 points ci-dessus.