Doc Cyber
Les failles webs

1) Qu'est-ce qu'une application web ?

Une application web est une application manipulable directement en ligne :
- Grâce à un navigateur web
- Et qui nécessite donc pas d'utilisation
- Contrairement aux application mobiles
- Et pour le W3C, une application web est une application qui utilise le HTTP
- Comme un site web, une application web est généralement **installée sur un serveur**

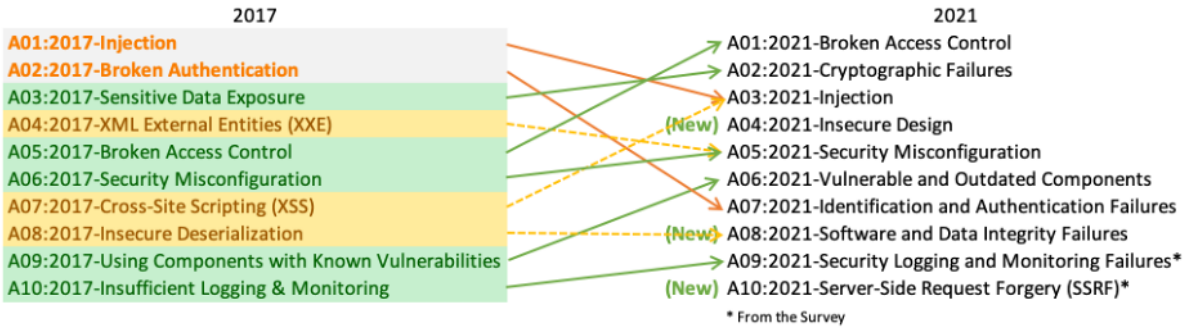
WEB → lieu pour échanger des informations
Mais il est également devenu un outil pour la vente et l'achat de bien matériel

Les acteurs de ce nouveau marché ont besoin de sécurité :
- Confidentialité
- Intégrité
- Disponibilité

2) Principaux organismes

4 Organisme Principaux de la sécurité web :
- ANSSI (Agence Nationale de Sécurité des Systèmes d'Information)
- CLUSIF(Club de la Sécurité de l'Information Français)
- WASC (Web Application Security Consortium)
- OWASP (Open Web Application Security Project)

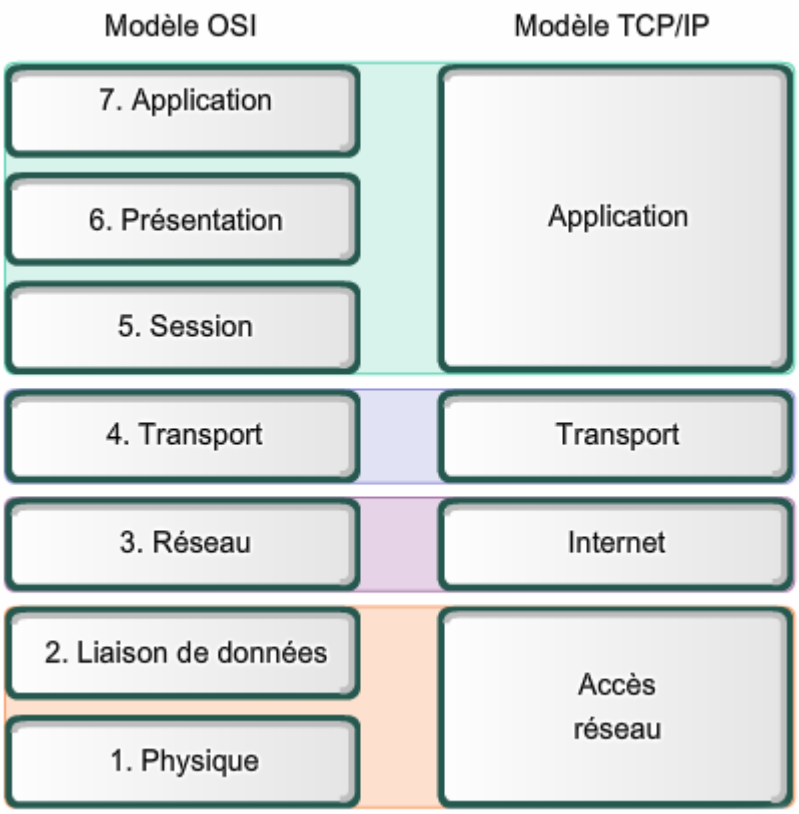
Le top 10 de l'OWASP :



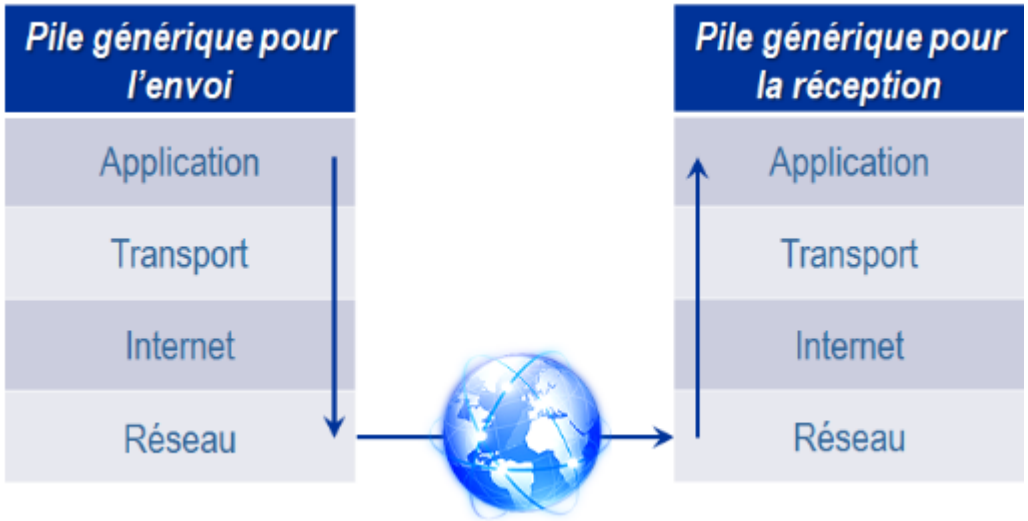
3) Architecture des applications web

HTTP = HyperText Transfer Protocol (Port 80)
HTTPS = HyperText Transfer Protocol Secure (Port 443)

On utilise aujourd'hui le protocole https



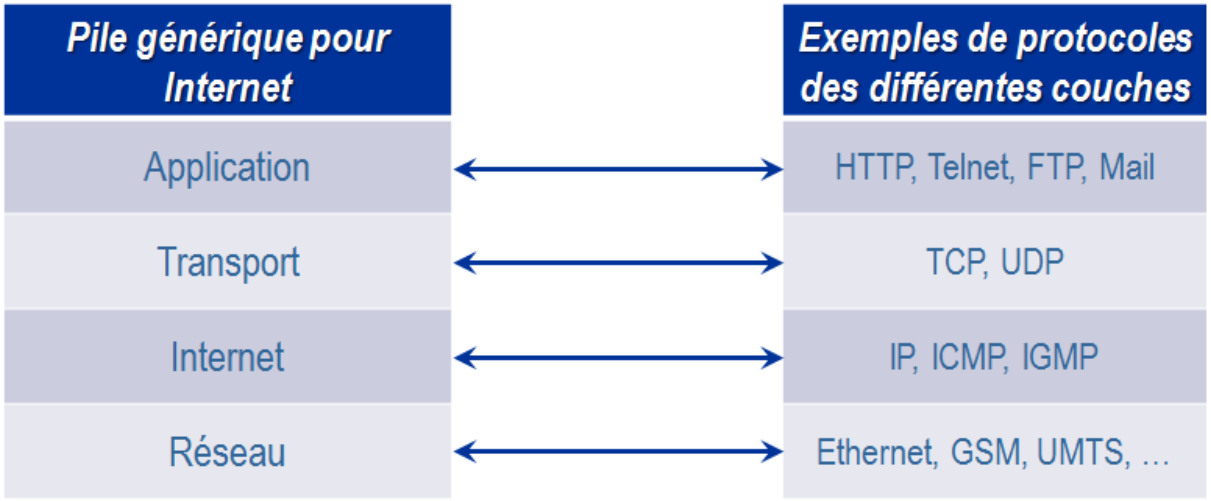
Transfert des données à travers la pile de protocoles d'internet :



Couche “ Réseau “ : Transmission physique

- **Ethernet**
- **3G**
- **4G**

Piles de protocoles d’Internet



La couche “Internet”

- La couche internet est la couche qui indique ou les données doivent être envoyées sans garantie que la destination sera bien atteinte
- Chaque paquet est transmis individuellement et peut emprunter un chemin différent des autres

La couche internet <ICMP> (Internet Control Message Protocol) :

- **ICMP** permet de vérifier que des messages peuvent être échangées
- **ICMP** est “fiable”
- **ICMP** est particulièrement ?

La couche internet <IP> (Internet Protocol) :

- **IP** est utilisé pour la plupart des communication internet
- **IP** est dit non fiable
- car protocole n’offre aucune garantie
    - L’ordre d’arrivée des paquet
    - la perte ou la destruction de paquet
    - la duplication des paquet
- si besoin le contrôle peut être réalisé par la couche supérieur “Transport”

La couche “Transport”

La couche “transport” peut utiliser un des protocoles suivant :

- **TCP** (Transmission Control Protocol)
- **UDP** (User Datagram Protocol)

La couche de transport <TCP>

- **TCP** s’assure que
    - Les paquets sont reçu dans le même ordre qu’ils ont été envoyés
    - et que les paquets perdus sont à nouveau envoyés
- **TCP** est donc un moyen de transmission fiable

Switch = Brancher plusieurs appareils sur un appareil switch, à partir d'une seule prise ethernet.
Hub = Ancêtre claqué au sol du switch
Routeur = Fait le lien entre plusieur réseau local

La couche transport <**UDP**>

- **UDP** permet un protocole simplifié
- **UDP** permet de transmettre des informations plus rapidement que TCP
  moins d'information partagé

La couche “Applications”

La couche Applications est celle qui permet aux utilisateurs de communiquer sur internet
La couche peut utiliser

- **SSH** (Secure Shell
- **FTP** (File transfer Protocol) Pour la transmission de fichier
- **SMTP**(Simple Mail Transfer Protocole)
- **HTTP** (HyperText Transfer Protocol)

La couche application: **HTTP**

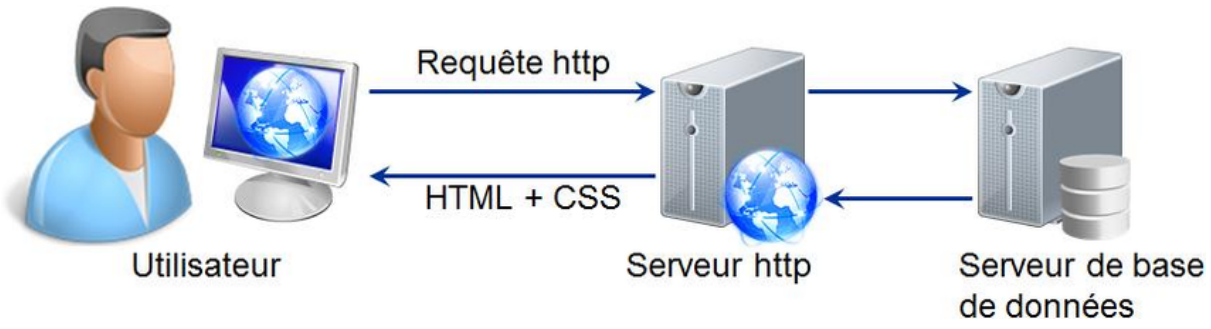
- La couche application **HTTP** est de type application de type texte basé sur le principe requête / réponse.
- L’utilisateur envoi, via son navigateur un message (**la requête**) au serveur HTTP
- Chaque requête est traitée individuellement et de façon unique
- Ensuite le serveur renvoie un message (**la réponse**) au navigateur
- HTTP est un protocole **déconnecté,**
- C'est-à-dire que le protocole ne permet pas d'établir des communications entre requête pour partager des informations.
- C’est pourquoi le navigateur intègre le système de “cookies” qui permet de **conserver le résultat d’une requête**.

- Résumé des protocoles par couche :
- Couche réseau Ethernet ou 3G ou 4G
- Couche internet IP ou ICMP

La décennie 1970-1980 était dominée par le système mainframe.
La décennie 1980-1990 à vue l’émergence du mode client/serveur.

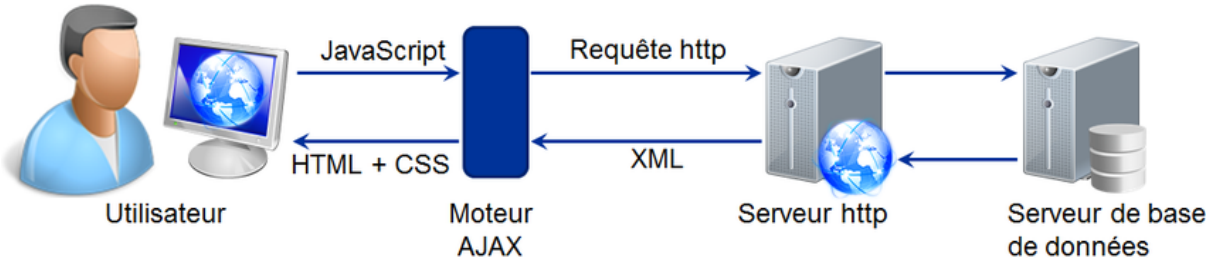
Début des années 90

- Les applications web ont suivi cette évolution, avec les **applets**.



XMLHttpRequest - norme HTML5

Les scripts côté client -**AJAX**



Cross Site Scripting
2 types d'attaques :

- Par réflexion
- Stockée

Violation et gestion d'authentification et de session

- usurpation d'identité
- points de faiblesse

<u>Mécanisme d'authentification le plus commun :</u>

L'utilisateur non authentifié demande l'accès à une page web
Le serveur renvoie une page de login
utilisateur fournit un identifiant et un mdp
le serveur web fait appel à un service pour vérifier le compte
Si le compte est valide, un identifiant de session est fourni à l'utilisateur

HTTP est un protocole déconnecté
Entre 2 requêtes HTTP, la connexion entre le navigateur et le serveur est coupée.
Donc le serveur HTTP ne peux pas reconnaître un utilisateur

Un identifiant de session est envoyé à chaque page entre client et serveur :
un cookie
un paramètre dans l'url
un champ invisible dans le formulaire

l'utilisateur peut utiliser l'app web tant que session est ouverte

Attaque pour usurper identité :
Attaque sur le système d'authentification
Les usurpation de session

Attaque de la force brute = tester plein de couples identifiant / mot de passe .
L'attaque est facilitée si le message d'erreur donne l'origine de l'échec d'authentification.

Page de réinitialisation de mdp sont une faille importante

Voler un identifiant de session :

générer des valeur et tenter de les utiliser comme identifiant

Faille XSS pour récupérer un id de session

sur fichier log …
par hameçonnage (phishing)

LES BONNES PRATIQUES ☺

Autoriser uniquement les mot de passes sécurisés
En cas d'erreur de saisie, le développeur ne doit pas fournir d'indice.

RÈGLE D'OR

utiliser un système existant éprouvé

Important : ne pas dev son propre mécanisme d'auth
c'est mieux d'utiliser un système existant éprouvé

identifiant de session doivent avoir une durée de vie limitée.