Session web

Yves Denneulin

Notion de session

- Authentification
- navigation sous une identité
  - introduction de la notion d'état
    - http est un protocole sans état
- déconnexion

Identification d'une session par le serveur

- Existence d'une donnée partagée entre le client qui a ouvert la session et le serveur
  - doit être secrète
  - ne doit pas pouvoir être volée
  - doit être unique à la session (réutilisation ?)
  - secret partagé

Adresse IP du client

- Facile à faire pour le serveur
- Difficile à voler ?
- Unicité non garantie
  - les étudiants sur ensibull
  - non applicable (mais ça a été fait)

Utilisation des cookies

- cookie : information envoyée par le serveur et stockée par le client
- le serveur peut les demander plus tard
- unicité : dépend du serveur -> OK
- vol possible ? oui!
  - espionnage
  - programme intrus
  - autres sites webs (xss)

utilisation d'identifieur de session

- typiquement dans les URL
- un paramètre passé à chaque demande de page
- unicité : dépend du serveur
- vol possible : oui
  - espionnage
  - éventuellement deviner un actuel (aléatoire)
- important : expiration

identificateur dynamique de session

- passé en paramètre dans l'URL
- dynamique : changé à chaque page
- expiration courte (pas de rejeu possible)
- unicité : serveur
- vol : difficile ET visible!

dans ce que vous utilisez

- les cookies par défaut
- une option vous permet d'utiliser des sessions id statiques

Vol de session

- espionnage de l'authentification
  - communication chiffrée obligatoire
  - pas de malware sur les clients
- intrusion sur les serveurs
  - vol des couples login/mdp