Programmation Web – Avancé

JavaScript & Node.js

Gestion de sessions côté client

Gestion de sessions côté client

Et si le client se souvenait de ses données de session ?

Gestion de sessions : généralités

- Gestion de sessions côté serveur VS côté client :
  - Différences ?
  - Avantages & inconvénients ?
- Côté serveur : **stateful server**
  => NOK pour une RESTful API
- Côté client : **stateless server**

Où sauvegarder de manière persistante des données côté client ?

- Web Storage
- Cookies
- NB :
  - Cache
  - IndexDB

Web storage : localStorage & sessionStorage

- « Key-value store » : toujours des strings
- **localStorage** [88.] : pas d'expiration
- **sessionStorage** : effacé à la fin d'une session

Web storage : localStorage & sessionStorage

◉ getItem()

```
const STORE_NAME = "user";
const getUserSessionData = () => {
  const retrievedUser = localStorage.getItem(STORE_NAME);
  if (!retrievedUser) return;
  return JSON.parse(retrievedUser);
};
```

Web storage : localStorage & sessionStorage

- setItem()

```
const setUserSessionData = (user) => {
  const storageValue = JSON.stringify(user);
  localStorage.setItem(STORE_NAME, storageValue);
};
```

Web storage : localStorage & sessionStorage

- removeItem()

```
const removeSessionData = () => {
  localStorage.removeItem(STORE_NAME);
};
```

- localStorage.clear()

Web storage

- **DEMO : Création d'une SPA pour une pizzeria : Step 3 : Sauvegarde du token et du username côté client, affichage du username pour tout utilisateur authentifié & logout**
  - On fait quoi pour l'affichage du username ?
  - On fait quoi au logout ?

Les cookies

- Données envoyées par un serveur vers un client
- But :
  - **Gestion de session**
  - Personnalisation
  - Tracking
- Autrefois : « general client-storage »

Les cookies

- Envoi automatique des cookies pour chaque requête vers le domaine
- Actuellement :
  - Protection contre les attaques XSS : utilisation de **HttpOnly** pour rendre les cookies inaccessible au JS
  - Ou utilisation du **localStorage** mis à disposition par les browsers modernes plutôt que les cookies

Gestion de session côté client avec Express

- Session middleware : **cookie-session** [86.]
- Enregistrement de données de session dans le cookie
- Installation : **npm install cookie-session**

Gestion de session côté client avec Express

- Utilisation du middleware :

```
var cookieSession = require("cookie-session");
let expiryDate = new Date(Date.now() + 60 * 60 * 1000); // 1h;
app.use(
  cookieSession({
    name: "user",
    keys: ["689HiHoveryDi79*"],
    cookie: {
      httpOnly: true,
      expires: expiryDate,
    },
  })
);
```

Gestion de session côté client avec Express

- Données de sessions attachées aux cookies :
  - Lecture & modification de données : **req.session** (comme pour **express-session**)

```
router.post("/login", async function (req, res, n
ext) {
  // …
  // Create the session data
  req.session.username = authenticatedUser.userna
me;
  req.session.token = authenticatedUser.token;

  return res.json({ username: authenticatedUser.u
sername });
});


const authorizeFromCookie = (req, res, next) => {
  // Read the session data
  let token = req.session.token;
  if (!token) return res.status(401).end();
  try {
    const decoded = jwt.verify(token, jwtSecret);
    // …
```

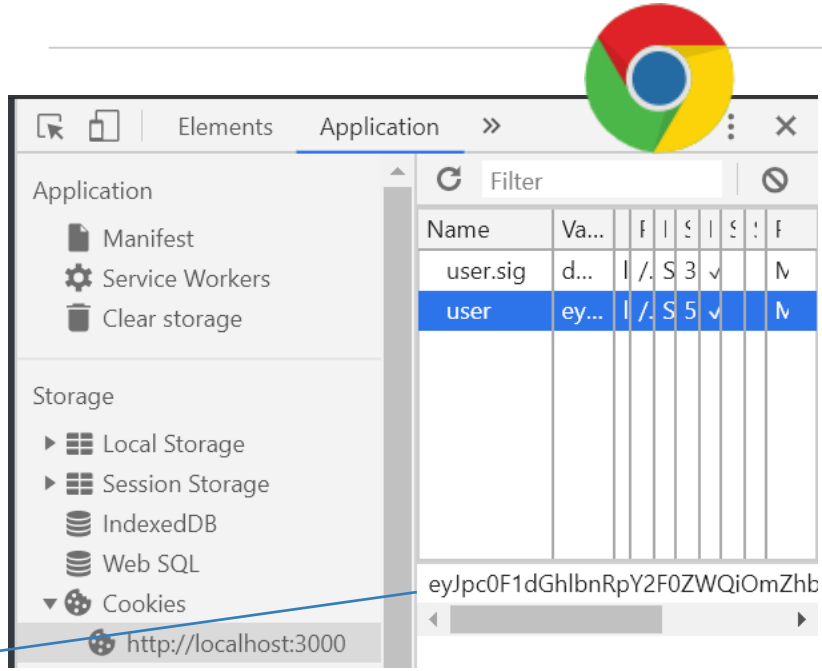
Gestion de session côté client avec Express

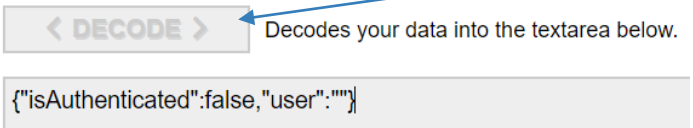
- Données de sessions attachées aux cookies :
  - Effacer une session : **req.session = null**

```
/* Logout a user : POST /auths/logout */
router.get("/logout", async function (req, res, next) {
  req.session = null;
  return res.status(200).end();
});
```

Visualisation des cookies au sein du browser

- **cookieName**
  - Base64 encoded
  - Décodeur base64 [87.]
- **cookieName.sig** : prévention contre le « tampering »





Vue du cookie au chargement de MyCMS

Cookies et session côté client

- DEMO : Création d'une RESTfull API pour une pizzeria : Step 8 –Sauvegarde du token au sein d'un cookie côté client
- Frontend : Réutilisation de la DEMO : Création d'une SPA pour une pizzeria : Step 3
  - Tout fonctionne ? Des changements à faire ?