

Authentification avec session dans Express

- HTTP est sans état; afin d'associer une demande à toute autre demande, on a besoin d'un moyen de stocker les données utilisateur entre les demandes HTTP.
- Les cookies et les paramètres d'URL sont tous deux des moyens appropriés pour transporter des données entre le client et le serveur.
- Mais ils sont à la fois lisibles et côté client.
- Les sessions résolvent exactement ce problème.
- On attribue au client un ID et il fait toutes les demandes supplémentaires à l'aide de cet ID.
- Les informations associées au client sont stockées sur le serveur lié à cet ID.

// Installer la session express

- Dans l'invite de commande taper :
`npm install --save express-session`

// Dans app.js

- Ajouter l'appel du module suivant :
`var session = require('express-session') ;`
- Mettre en place le middleware de session :
`app.use(session({secret: 'utilisateur'}));`

// Fichier app.js complet

```
var express = require('express');
var session = require('express-session');
var bodyParser = require('body-parser');
var app = express();
app.use(bodyParser.json());
app.use(bodyParser.urlencoded({extended: true}));
app.set('views', __dirname + '/views');
app.set('view engine', 'ejs');
const dbConfig = require('./config/database.config.js');
const mongoose = require('mongoose');
mongoose.Promise = global.Promise;
mongoose.connect(dbConfig.url,{
  useNewUrlParser: true,
  useUnifiedTopology: true
}).then(() => {
  console.log("Successfully connected to the database");
}).catch(err => {
  console.log('Could not connect to the database. Exiting now...', err);
  process.exit();
});
app.use(session({secret: 'utilisateur'}));
require('./routes/session.routes.js')(app);
app.listen(8000,function(){
  console.log("App Started on port 8000");
});
```

```
// Fichier config/database.config.js
```

```
module.exports = {  
  url: 'mongodb://localhost:27017/authentication'  
}
```

```
// Fichier models/session.model.js
```

```
const mongoose = require('mongoose');
```

```
const NoteSchema = mongoose.Schema({  
  email: String,  
  password: String  
});
```

```
module.exports = mongoose.model('Session', NoteSchema);
```

// Fichier routes/session.routes.js

```
module.exports = (app) => {  
  const Session = require('../models/session.model');  
  //Appel de la page index  
  app.get('/', function(req, res){  
    res.render('index.ejs');  
  });  
  //nouvel utilisateur, afficher le formulaire d'enregistrement  
  app.get('/newRegist', function(req, res){  
    res.render('indexRegistration.ejs');  
  });  
};
```

// Fichier routes/session.routes.js

//sauvegarde les informations dans la base de données puis dans la session

```
app.post('/login', async (req, res )=> {  
  try {  
    var session = new Session({  
      email:req.body.email|| "Untitled email",  
      password:req.body.pass|| "empty pass"  
    });  
    var result = await session.save();  
    req.session.email = req.body.email;  
    req.session.password = req.body.pass;  
    res.end('done');  
  } catch (error) {  
    res.status(500).send(error);  
  }  
});
```

// Fichier routes/session.routes.js

```
/* Suite à une opération d'enregistrement réussie on affichera welcome suivi de la
valeur de l'email correspondant. Sinon on demande l'identification de
l'utilisateur. */
```

```
app.get('/registration',function(req,res){
  if(req.session.email) {
    res.write('<h1>Welcome '+req.session.email+'</h1>');
    res.write('<a href="/logout">Logout</a>');
    res.end();
  } else {
    res.write('<h1>Please login first.</h1>');
    res.write('<a href="/">Login</a>');
    res.end();
  }
});
```

// Fichier routes/session.routes.js

//Détruire la session suite à une déconnexion.

```
app.get('/logout',function(req,res){
  res.locals.password = null;
  req.session.destroy(function(err) {
    if(err) {
      console.log(err);
    } else {
      res.redirect('/');
    }
  });
});
//Afficher le formulaire d'identification
app.get('/oldRegist',function(req,res){
  res.render('indexidentification.ejs');
});
```


// Fichier routes/session.routes.js

```
/* Vérifier les paramètres d'accès. S'ils existent dans la base de données, les  
enregistrer dans la session puis accéder à la page sécurisée. Sinon se rediriger  
vers le formulaire d'identification. */
```

```
app.post('/verification', async (req, res )=> {  
  try {  
    var result = await Session.findOne()  
      .where("password").in([req.body.password])  
      .exec();  
    req.session.email = result.email;  
    req.session.password = result.password;  
    res.redirect('/identification');  
  } catch (error) {  
    res.redirect('/oldRegist');  
  }  
});
```

// Fichier routes/session.routes.js

```
//Tester si la session est enregistrée
```

```
app.get('/identification', async (req, res )=> {  
    ssn = req.session.password;  
    try { if(ssn)  
        {  
            var result = await Session.find().exec();  
            res.redirect('/liste');  
        }  
    } catch (error) {  
        res.status(500).send(error);    }  
    });
```

```
/* La page liste est sécurisée. On utilise res.locals qui est un objet contenant  
des variables locales de réponse étendues à la demande*/
```

```
app.get('/liste',function(req,res){  
    res.locals.password = req.session.password;  
    res.render('menu.ejs'); });  
// fermeture de module.exports  
}
```

// Fichier views/include/head.ejs

```
<head>
  <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/css/bootstrap
.min.css" integrity="sha384-
Vkoo8x4CGs03+Hhxxv8T/Q5PaXtkKtu6ug5TOeNV6gBiFeWPGFN9MuhOf23Q9Ifjh" crossorigin="anonymous">
  <script src="https://code.jquery.com/jquery-3.4.1.slim.min.js" integrity="sha384-
J6qa4849blE2+poT4WnyKhv5vZF5SrPo0iEjwBvKU7imGFAV0wwj1yYfoRSJoZ+n" crossorigin="anonymous"></script>
  <script src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js" integrity="sha
384-
Q6E9RHvbIyZFJoft+2mJbHaEWldlvI9IOYy5n3zV9zzTtmI3UksdQRVvoxMfooAo" crossorigin="anonymous"></script>
  <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/js/bootstrap.min.js" integrity="s
ha384-
wfSDF2E50Y2D1uUdj003uMBJnjuUD4Ih7YwaYd1iqfktj0Uod8GCExl3Og8ifwB6" crossorigin="anonymous"></script>

  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/twitter-
bootstrap/4.1.3/css/bootstrap.css">
  <link rel="stylesheet" href="https://cdn.datatables.net/1.10.20/css/dataTables.bootstrap4.min.css
">
  <script src="https://code.jquery.com/jquery-3.3.1.js"></script>
  <script src="https://cdn.datatables.net/1.10.20/js/jquery.dataTables.min.js"></script>
  <script src="https://cdn.datatables.net/1.10.20/js/dataTables.bootstrap4.min.js"></script>
</head>
```

```
// Fichier views/index.ejs
```

```
<%- include ('./include/head') %>

<a class="btn btn-primary mr-2" href="/oldRegist" >
  Login
</a>
  <a class="btn btn-danger mr-2" href="/newRegist" >
    New User
  </a>
```

// Fichier views/IndexRegistration.ejs

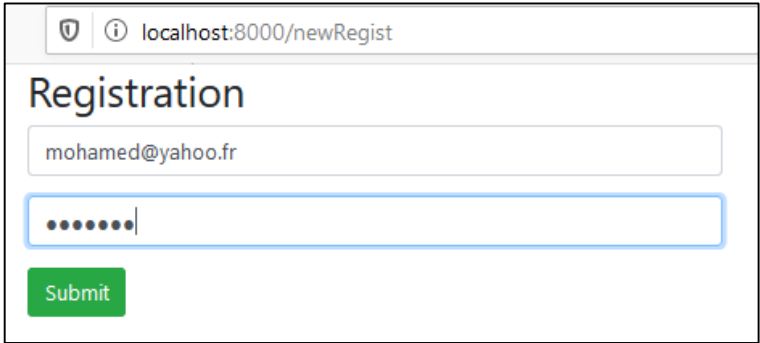
```
<html> <head>
  <%- include ('./include/head') %>
  <title>Registration</title>
  <script src="//ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.js"></script>
  <script>
    $(document).ready(function(){
      var email, password;
      $("#submit").click(function(){
        email = $("#email").val();
        password = $("#password").val();
        $.post("http://localhost:8000/login", {
          email: email,
          pass: password
        }, function(data) {
if(data==='done') {  window.location.href="/registration";  }
          });
        });
      });
    });
  </script>    </head>
```

// Fichier views/IndexRegistration.ejs

```
<body>
  <div class="container">    <h2>Registration</h2>
    <div class="row">
      <div class="col-sm-3 col-md-6"
        <div class="form-group">
<div class="form-group">
&ltinput type="text" size="40" placeholder="Type your email" id="email" class="form-control">
</div>
&ltdiv class="form-group">
&ltinput type="password" size="40" placeholder="Type your password" id="password" class="form-control">
</div>
&ltdiv class="form-group">
&ltinput type="button" value="Submit" id="submit" class="btn btn-success">
</div>
      </div>
    </div>
  </div>
</div>
</body></html>
```

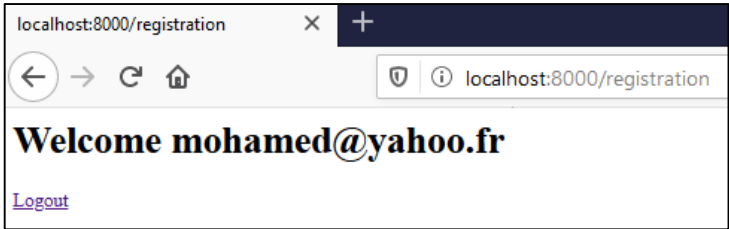
Résultat :

Etat 1 :



A screenshot of a web browser window with the address bar showing 'localhost:8000/newRegist'. The page title is 'Registration'. It contains a text input field with the email 'mohamed@yahoo.fr', a password input field with seven dots, and a green 'Submit' button.

Etat 2 :



A screenshot of a web browser window with the address bar showing 'localhost:8000/registration'. The page displays a welcome message 'Welcome mohamed@yahoo.fr' in bold black text, followed by a purple 'Logout' link.

// Fichier views/indexIdentification.ejs



```
<html>    <head>        <%- include ('./include/head') %>        <title>Identification</title>
    </head>
    <body>
        <div class="container">
            <h2>Log In</h2>
            <div class="row">
                <div class="col-sm-3 col-md-6">
                    <div class="form-group">
                        <form method="post" action="verification">
                            <div class="form-group">
                                <input type="text" size="40" placeholder="Type your email" name="email" id="email" class="form-control">
                            </div>
                            <div class="form-group">
                                <input type="password" size="40" placeholder="Type your password" name="password" id="password" class="form-control">
                            </div>
                            <div class="form-group"></div>
                                <input type="submit" value="Log In" id="submit" class="btn btn-success">
                            </div>
                        </form>
                    </div>
                </div>
            </div>
        </div>
    </div>
</body> </html>
```


// Fichier views/menu.ejs

```
<html>
  <head>
<%- include ('../include/head') %>
</head>
<body>
<div class="container">
  <div class="jumbotron">
    <% if (locals.password == null) { %>
    <div>Access Denied</div>
    <% } else { %>
      <div>Menu</div>
      <div> Reserved space</div>
      <div> <a href="/logout">Logout</a></div>
    <% } %>
  </div>
</div>
</body>
</html>
```

Résultat :

Etat 1 :

 localhost:8000/oldRegist

Log In

Log In

Etat 2 :

Menu

Reserved space

Logout