**Atividade de Aula – Trabalho Prático**

|  |  |
| --- | --- |
| **Disciplina** | **AAS - Autenticação e Autorização em Soluções Web** |

|  |  |
| --- | --- |
| Nome do aluno | **Gabriel de Souza Tamiozzo** |
| Nome do aluno | **Paulo César da Silva** |
| Nome do aluno | **Bruno da Silva Pontes** |
| Nome do aluno | **Paulo Cezar da Silva Junior** |
| Nome do aluno |  |

**Objetivos**

Exercitar os seguintes conceitos vistos em sala de aula:

* OAuth 2.0
* Authorization Code flow

**Enunciado**

O grupo deverá desenvolver uma aplicação web que receberá requisições de acesso a dados de contas de usuário. Caso uma conta não seja localizada em sua base, a aplicação solicitará autorização para realizar a leitura dos dados de uma conta do Facebook. A atividade deverá ser desenvolvida utilizando Spring Boot ou Node.js.

**Atividades**

Essa atividade destina-se a realizar o desenvolvimento de uma aplicação que lê dados de uma conta do Facebook para armazená-los em seu cadastro. Para tal, é necessário que seja realizado o cadastro na plataforma de desenvolvedores do Facebook (<https://developers.facebook.com/>) e cadastrar uma nova aplicação. Após realizar o cadastro, é importante certificar-se de:

* Obter corretamente os valores do: client\_id, client\_secret e accesstoken.
* Configurar a URL da sua aplicação para o endereço local, por exemplo: [http://localhost:8080](http://localhost:8080/).
* Liberar as configurações de segurança da sua aplicação para permitir o redirecionamento de URLs de quaisquer domínios.

Sua aplicação deverá definir dois endpoints com as seguintes características:

* ENDPOINT 01:
  + GET /conta/*{id}*: ao acessar esse endereço, a aplicação verifica se o id informado se encontra na base de dados. Caso o registro exista, deve ser retornado. Caso contrário será enviada uma resposta de redirecionamento, iniciando o fluxo de login no facebook (mais detalhes adiante).
* ENDPOINT 02:
  + GET /conta/cadastro/*{id}*?code=*{code*}&state=*{state}*: ao acessar esse endereço, a aplicação espera receber o código de autorização e o estado. Esse endereço será utilizado para indicar concessão de acesso por parte do usuário. Após receber o código do Facebook, a aplicação irá acessar os dados, armazená-los e redirecionar o usuário para o ENDPOINT 01.

Para realizar tal atividade, deverá ser definida uma única entidade chamada **Conta**. Suas únicas propriedades são: id, nome e idFacebook.

Sobre o fluxo a ser implementado:

1. Um usuário, utilizando o navegador, acessa o **ENDPOINT 01** da aplicação. Caso não seja encontrado um registro de conta com o identificador fornecido, o usuário é redirecionado para a URL:

[https://www.facebook.com/v3.3/dialog/oauth?client\_id={CLIENT\_ID}  
&redirect\_uri={REDIRECT\_URI}&state={STATE](https://www.facebook.com/v3.3/dialog/oauth?client_id=%7bCLIENT_ID%7d&redirect_uri=%7bREDIRECT_URI%7d&state=%7bSTATE)}

* **CLIENT\_ID:** número identificador da sua aplicação, obtido no momento de registro da mesma.
* **REDIRECT\_URI:** endereço para o qual o Facebook irá redirecionar a navegação após o login, ou seja: **ENDPOINT 02**.
* **STATE:** texto a ser utilizado por motivos de segurança.

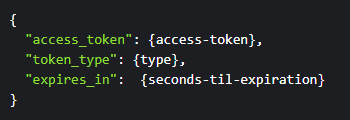
Após ser redirecionado, o usuário entra com os dados na página de login do Facebook. A aplicação cliente, nesse momento, apenas aguarda uma requisição.

1. A aplicação cliente recebe o redirecionamento no **ENDPOINT 02** e se prepara para realizar três requisições em sequência para o Facebook, antes de enviar uma resposta para o usuário.
   1. A primeira requisição irá buscar o token de acesso, enviando como parâmetro o código de acesso recebido:

[https://graph.facebook.com/v3.3/oauth/access\_token?client\_id=**{CLIENT\_ID}**&redirect\_uri=**{REDIRECT\_URI}**&state=**{STATE}**&client\_secret=**{SECRET}**&code=**{CODE**](https://graph.facebook.com/v3.3/oauth/access_token?client_id=%7bCLIENT_ID%7d&redirect_uri=%7bREDIRECT_URI%7d&state=%7bSTATE%7d&client_secret=%7bSECRET%7d&code=%7bCODE)**}**

* **CLIENT\_ID:** número identificador da sua aplicação, obtido no momento de registro da mesma.
* **REDIRECT\_URI:** endereço para o qual foi solicitado que o Facebook retornasse após o login. É uma verificação de segurança.
* **STATE:** texto a ser utilizado por motivos de segurança.
* **CODE:** código de autorização enviado pelo servidor de autenticação.

Como resposta é esperado um Json conforme a próxima imagem. Sua aplicação poderá, contudo, ler somente o **access\_token** desse arquivo e ignorar o restante dos dados.



* 1. De posse do **acess\_token**,é necessário realizar uma requisição para obter o identificador da conta no facebook:

[https://graph.facebook.com/debug\_token?input\_token=**{INPUT\_TOKEN}**&access\_token=**{ACCESS\_TOKEN**](https://graph.facebook.com/debug_token?input_token=%7bINPUT_TOKEN%7d&access_token=%7bACCESS_TOKEN)**}**

* **INPUT\_TOKEN:** token recebido na resposta da requisição 2.1, no campo access\_token.
* **ACCESS\_TOKEN:** access token da aplicação, obtido ao registrar a aplicação.

Como resposta é esperado um Json conforme a próxima imagem. Sua aplicação poderá, contudo, ler somente o **data.user\_id** desse arquivo e ignorar o restante dos dados.



* 1. Para realizar a leitura do nome a aplicação poderá fazer a última chamada para o servidor de dados no endereço:

[https://graph.facebook.com/**{ID\_USUARIO\_FACEBOOK}/**?access\_token=](https://graph.facebook.com/%7bID_USUARIO_FACEBOOK%7d/?acess_token=)**{INPUT\_TOKEN}**

* **ID\_USUARIO\_FACEBOOK**: identificador obtido na resposta da requisição 2.2, no campo data.user\_id.
* **INPUT\_TOKEN**: token recebido na resposta da requisição 2.1, no campo access\_token.

Será recebido como resposta um payload contendo id e nome do usuário. Esses dados, juntamente com o id do usuário no Facebook, devem ser utilizados para persistir os dados e redirecionar para o primeiro end-point, exibindo corretamente os dados.

**Entrega da atividade:**

1. O grupo deverá compactar a solução desenvolvida e anexar o arquivo no **Canvas**, com o nome de todos os integrantes do grupo no arquivo.

Dicas para realização da atividade:

* Para realizar o redirecionamento de uma chamada do navegador, a resposta deve ser um HTTP 307 (redirecionamento temporário). Além disso, o cabeçalho da resposta deve conter uma chave “Location”, cujo valor é o endereço para o qual queremos redirecionar o usuário final.
* Não se afobe, um passo de cada vez: primeiro, tente implementar o segundo end-point. Para isso digite a URL retornada pelo primeiro end-point diretamente no navegador.
* Não se preocupe com fluxos alternativos e tratamento de erros. Trata-se de uma atividade acadêmica que nunca será colocada em produção.
* Seja prático: se você acha que pode ajudar, utilize trechos produzidos nas atividades prévias dessa disciplina. Além disso, não implemente algo que não tenha sido solicitado.
* Para obter maiores informações, consulte livremente a base de conhecimentos da comunidade: <https://developers.facebook.com/docs/facebook-login/manually-build-a-login-flow>