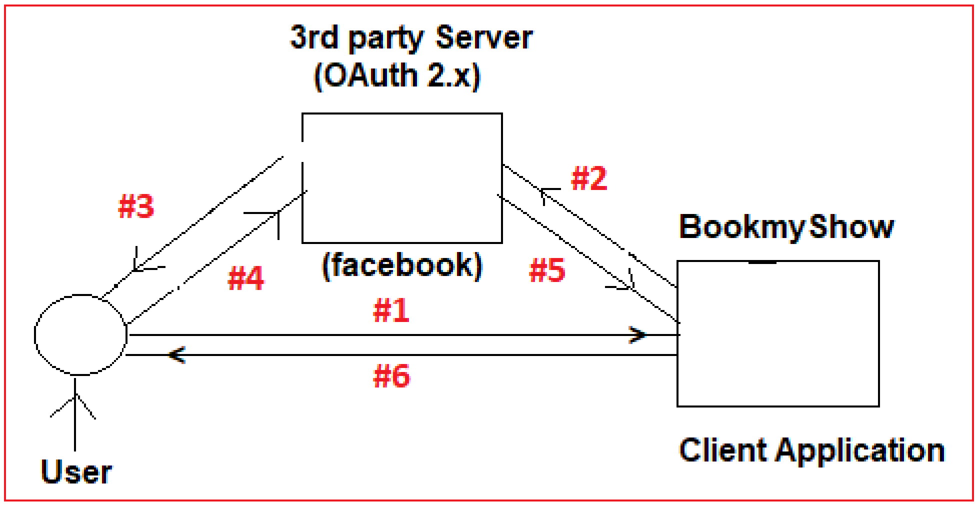
Spring Boot Outh2

OAuth 2.x:

- It is a standard and framework which provides 3rd party security services to client application which are registered on behalf of end user.



Flow:

1. Browser making request to client Application.
2. Client asking permission to third party.
3. Third party Application asking confirmation (Grant) to end user.
4. User confirmation.
5. Data shared from 3rd party Application to Client App.
6. Client gives response to end user.

- **The 3rd party Applications** are called **Authorization and Resource Servers** like Google, Facebook, GitHub, Twitter, LinkedIn … etc.

- **Client Applications** that are using OAuth2 is BookMyshow, redbus, yatra, MakeMyTrip, Avast, Zomato.. etc.

- OAuth 2.x standard is widely used in small/medium scale/daily used, business application.

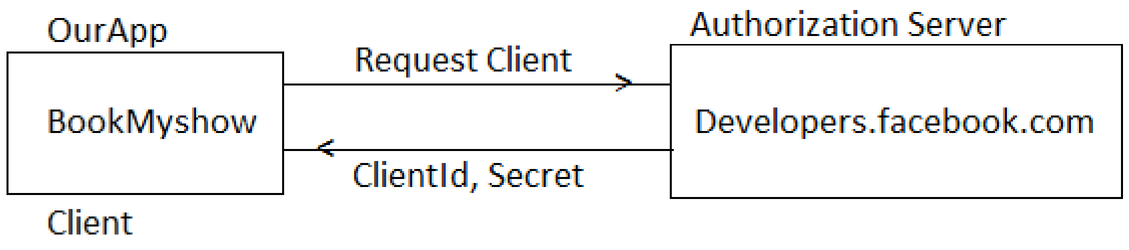
- OAuth2 Provide SSO (Single Sign on) for multiple applications acting as a one Service.
- OAuth2 may not be used for high level and Large scale applications like Banking, Creditcard, Stock Market, finance… etc. These applications use Spring Security ORM is used mostly.

Step 1: Register Client Application with Authorization Server

- Every Client Application (BookMyShow) must be registered with Authorization Server (Facebook)
  Eg: BookMyShow --- Register with --> Facebook Server

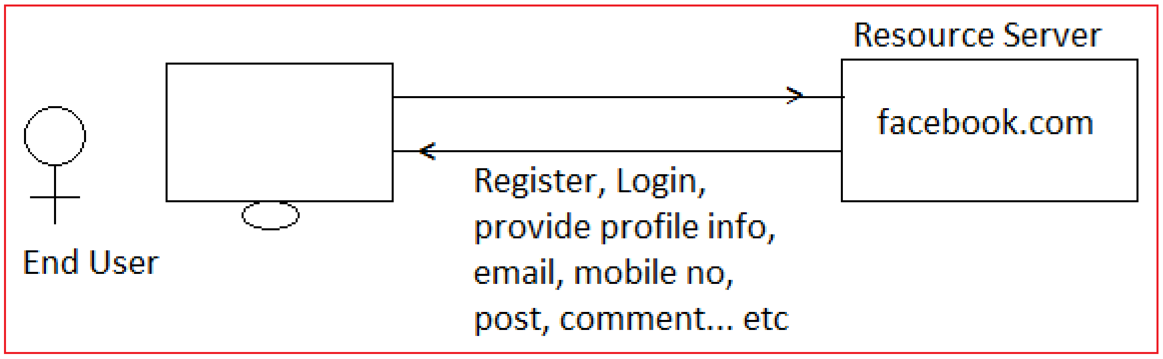
- Client Application gets **clientId** and **clientSecret** (like Password) on Successful registration at Authorization Server.

- This is like one time setup between Client Application and Authorization Server.

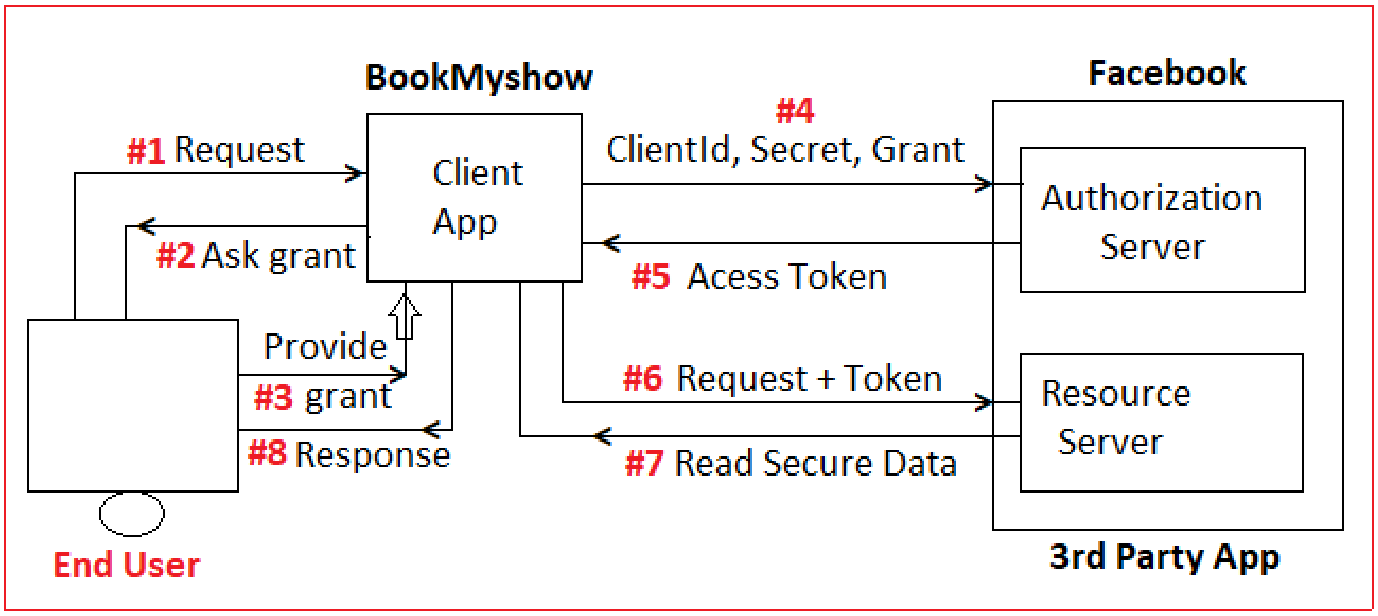


Step 2: End User must be Registered with Resource Server

- User must be register and Login with 3rd party Resource Servers (Like facebook.com).
- User need to provide profile information, basic data, comments, posts, photos… etc.
- User Id and password will never be shared with Client Application.
- Only Users Public and General information is shared with Client Application.



Request Work flow of OAuth2:



1. End user makes request using browser to client application (BookMyshow) request for “verify using 3rd party service” ex: Facebook, Google… etc.

2. Client Application will ask for Grant from end user, which confirms that access user data.

3. End user has to provide Grant (Permission) to access data.

4. Client makes request to Authorization server using ClientId, secret, user grant.

5. Auth server verifies details and goes to token Management process.
   A unique number is generated, called as Token which works for User+Client combination.

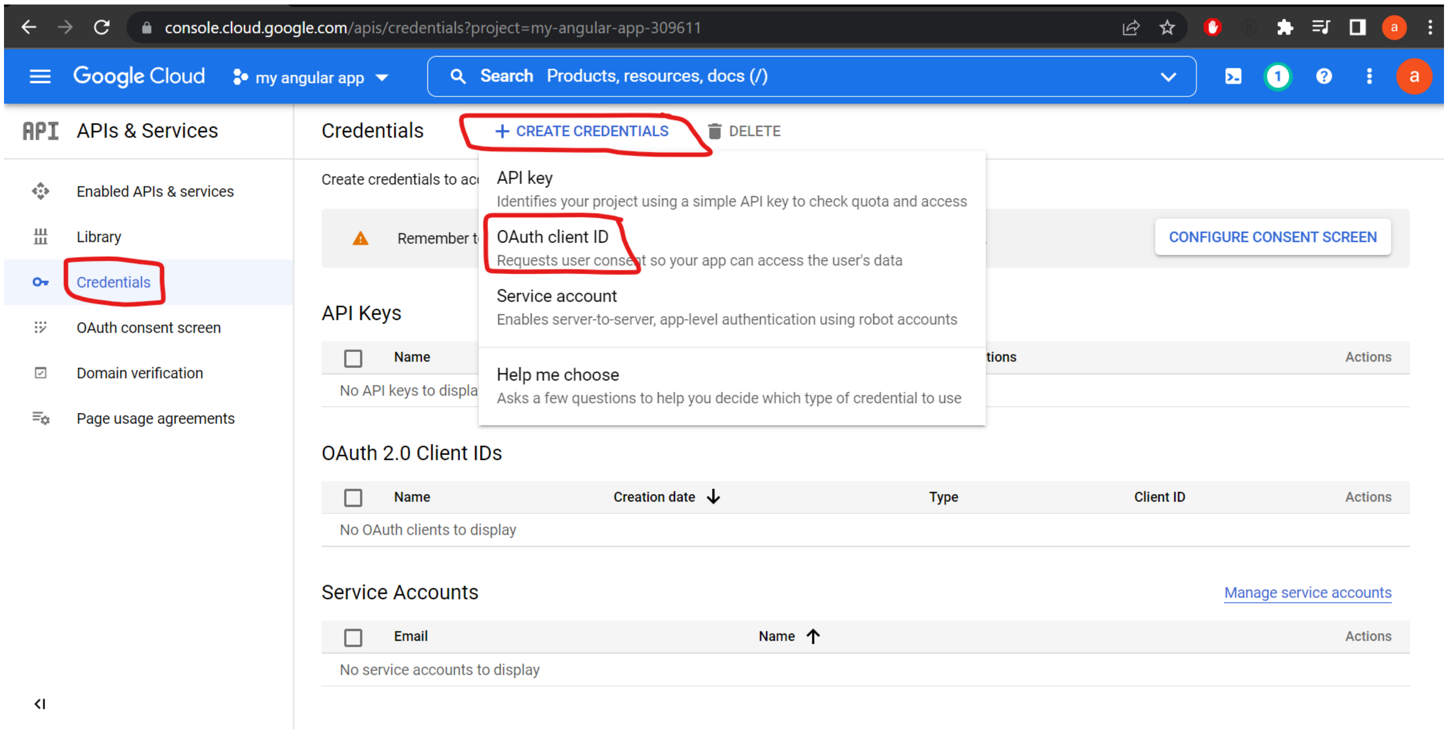
6. Now, client application makes request to resource Server using Access Token.

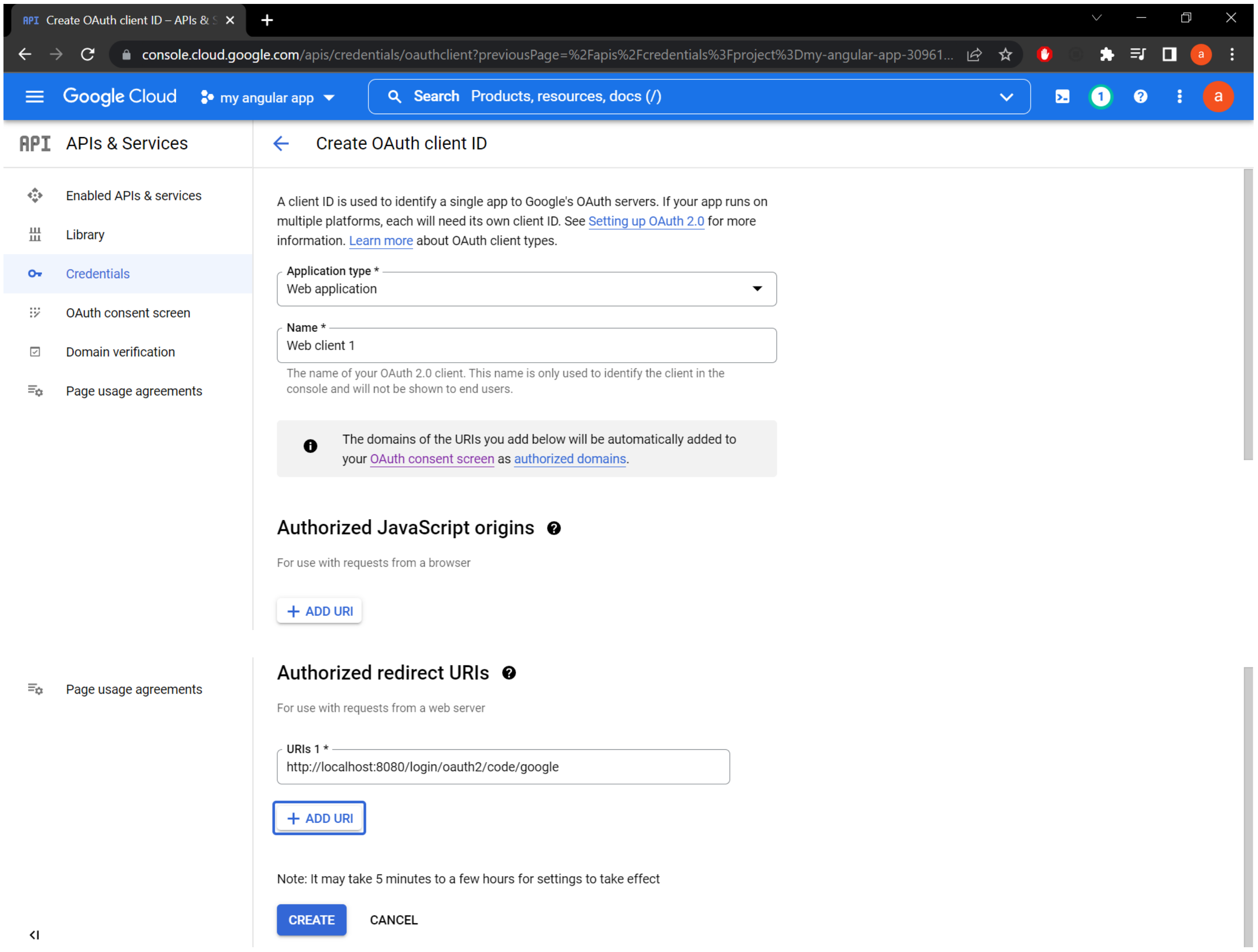
7. Resource server returns end user secure data to client.

8. Finally, Client App process the end user request and gives response.

One Time Setup for Google Oauth;

Steps to generate Client-id and secrete in Google;


console.cloud.google.com/apis/credentials?project=my-angular-app-309611
Google Cloud
my angular app
Search Products, resources, docs (/)
APIs & Services
Enabled APIs & services
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
Credentials
CREATE CREDENTIALS
DELETE
Create credentials to ac
Remember t
CONFIGURE CONSENT SCREEN
API key
Identifies your project using a simple API key to check quota and access
OAuth client ID
Requests user consent so your app can access the user's data
Service account
Enables server-to-server, app-level authentication using robot accounts
Help me choose
Asks a few questions to help you decide which type of credential to use
API Keys
Name
Actions
No API keys to displa
OAuth 2.0 Client IDs
Name
Creation date
Type
Client ID
Actions
No OAuth clients to display
Service Accounts
Manage service accounts
Email
Name
Actions
No service accounts to display



Create OAuth client ID – APIs & S

console.cloud.google.com/apis/credentials/oauthclient?previousPage=%2Fapis%2Fcredentials%3Fproject%3Dmy-angular-app-30961...

Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See Setting up OAuth 2.0 for more information. Learn more about OAuth client types.

Application type *: Web application

Name *: Web client 1

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

The domains of the URIs you add below will be automatically added to your OAuth consent screen as authorized domains.

Authorized JavaScript origins

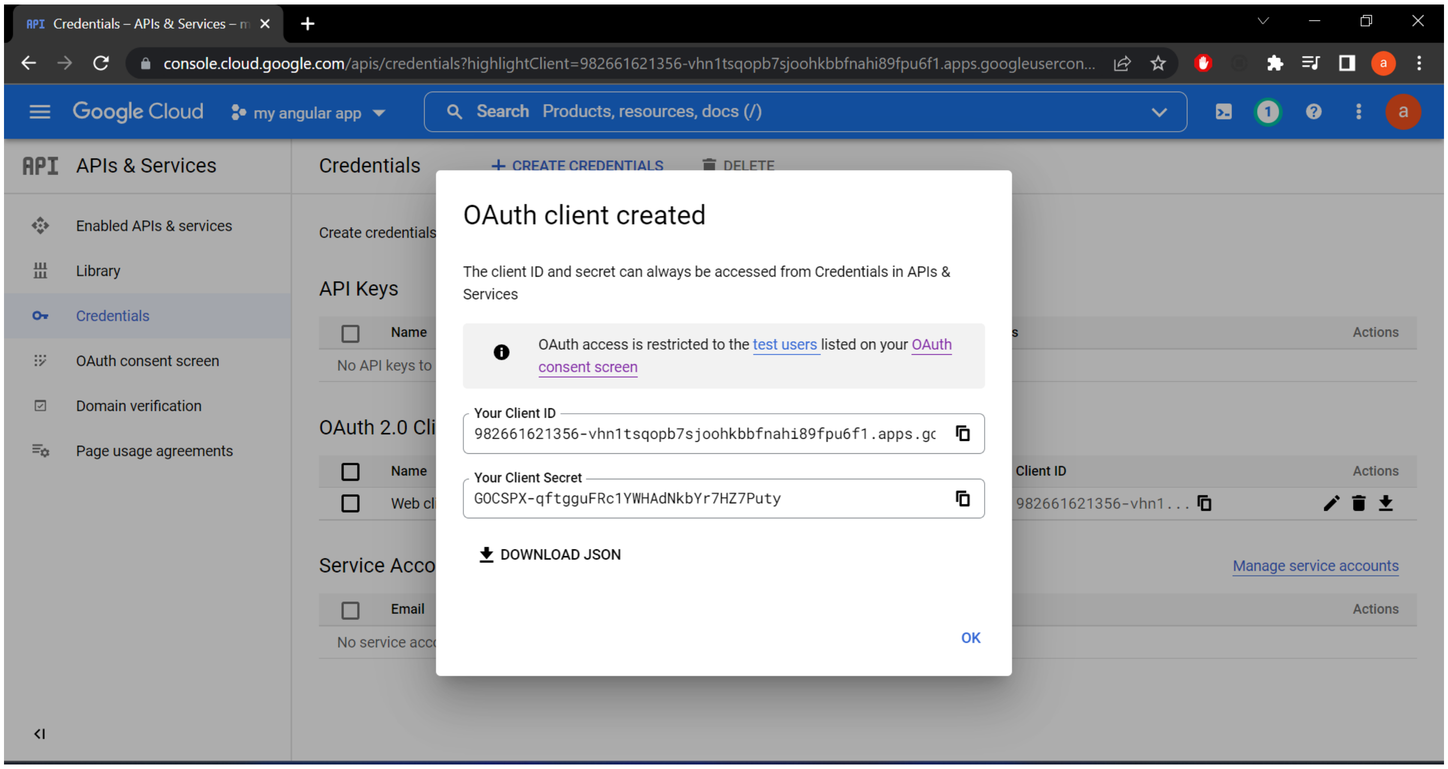
For use with requests from a browser

Authorized redirect URIs

For use with requests from a web server

URIs 1 *: http://localhost:8080/login/oauth2/code/google

Note: It may take 5 minutes to a few hours for settings to take effect



OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

OAuth access is restricted to the test users listed on your OAuth consent screen

Your Client ID
982661621356-vhn1tsqopb7sjoohkbbfnahi89fpu6f1.apps.gc

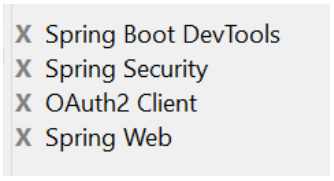
Your Client Secret
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

DOWNLOAD JSON

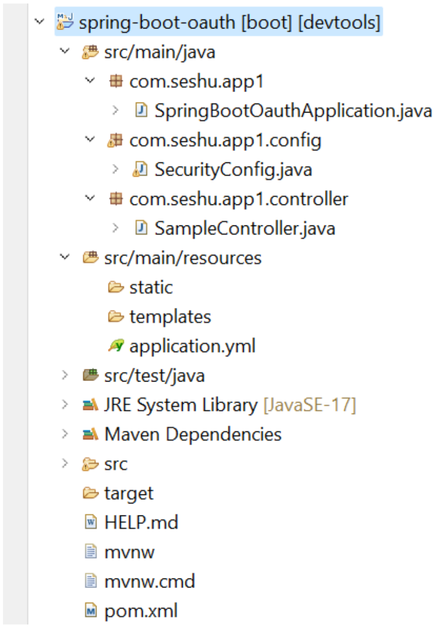
OK

Example: Spring Boot and Google Oauth

Generate a new Spring Boot Project as ***spring-boot-oauth*** with fallowing dependencies;



X Spring Boot DevTools
X Spring Security
X OAuth2 Client
X Spring Web



```
spring-boot-oauth [boot] [devtools]
  src/main/java
    com.seshu.app1
      SpringBootOauthApplication.java
    com.seshu.app1.config
      SecurityConfig.java
    com.seshu.app1.controller
      SampleController.java
  src/main/resources
    static
    templates
    application.yml
  src/test/java
  JRE System Library [JavaSE-17]
  Maven Dependencies
  src
  target
  HELP.md
  mvnw
  mvnw.cmd
  pom.xml
```

application.yml

```
spring:
  security:
    oauth2:
      client:
        registration:
          google:
            client-id: 982661621356-
vhn1tsqopb7sjoohkbbfnahi89fpu6f1.apps.googleusercontent.com
            client-secret: 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
```

SampleController.java

```
package com.seshu.app1.controller;

import java.security.Principal;

import org.springframework.web.bind.annotation.GetMapping;
import org.springframework.web.bind.annotation.RestController;

@RestController
public class SampleController {
	@GetMapping("/")
	public String welcomeView() {
		return "Welcome to sample controller";
	}
	@GetMapping("/profile")
	public String profileView() {
		return "welcome to profile page";
	}
	@GetMapping(value = "/user")
	public Principal user(Principal principal) {
	   return principal;
	}
}
```

SecurityConfig.java

```
package com.seshu.app1.config;

import org.springframework.context.annotation.Configuration;
import
org.springframework.security.config.annotation.web.builders.HttpSecurity;
import
org.springframework.security.config.annotation.web.configuration.~~WebSecur
ityConfigurerAdapter~~;

@Configuration
public class SecurityConfig extends ~~WebSecurityConfigurerAdapter~~ {
	@Override
	public void configure(HttpSecurity http) throws Exception {
		http.antMatcher("/**")
			.authorizeRequests()
			.antMatchers(new String[] { "/" })
			.permitAll()
			.anyRequest()
			.authenticated()
			.and()
			.oauth2Login();
	}
}
```

SpringBootOauthApplication.java

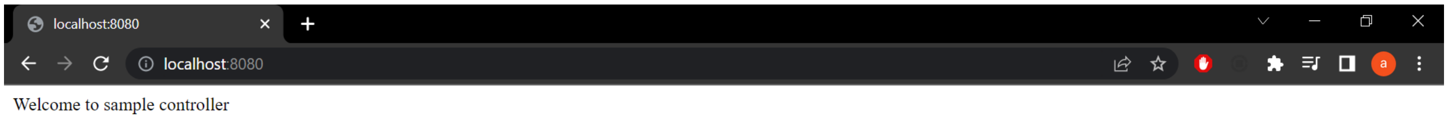
```
package com.seshu.app1;

import org.springframework.boot.SpringApplication;
import org.springframework.boot.autoconfigure.SpringBootApplication;

@SpringBootApplication
public class SpringBootOauthApplication {
	public static void main(String[] args) {
		SpringApplication.run(SpringBootOauthApplication.class, args);
	}
}
```

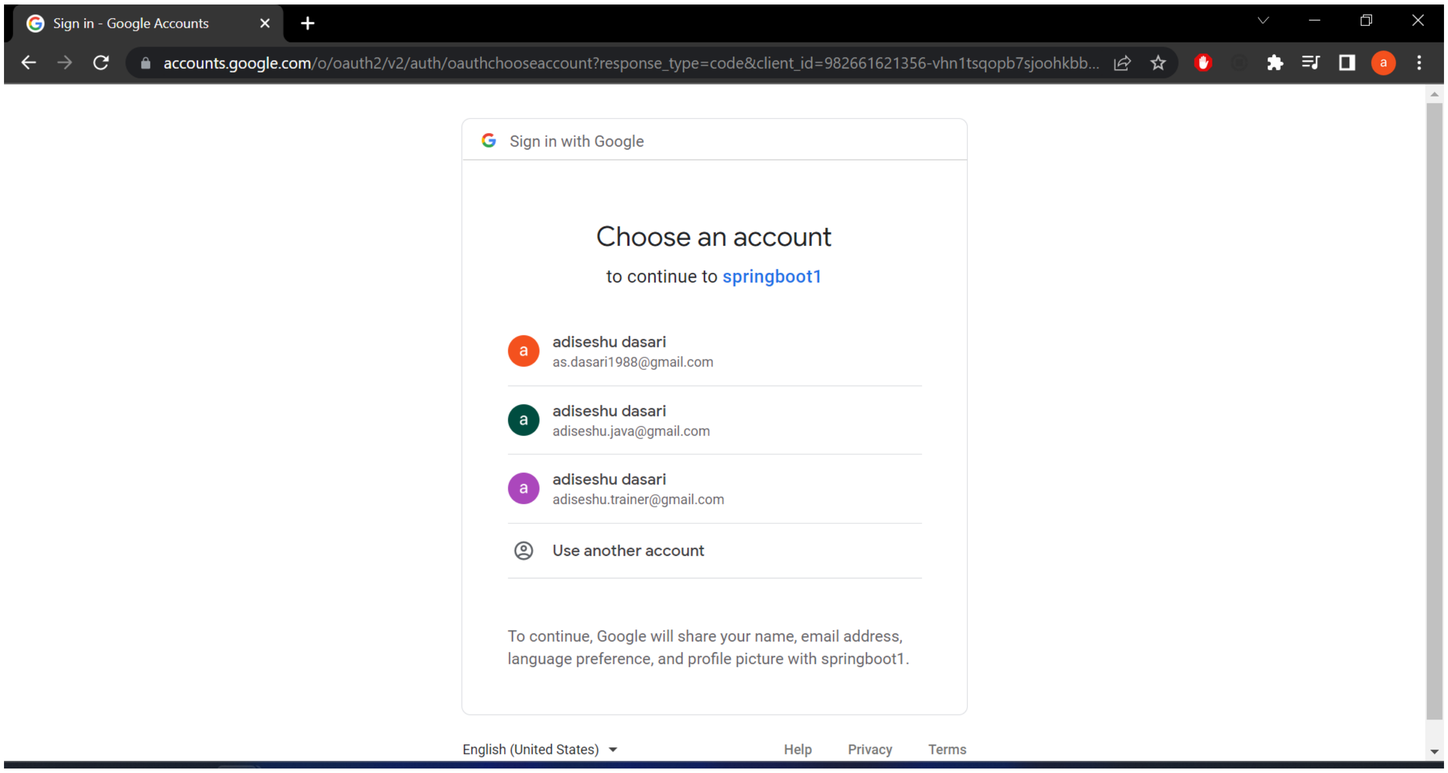
Test the application

http://localhost:8080/



```
Welcome to sample controller
```

http://localhost:8080/profile


Sign in - Google Accounts

accounts.google.com/o/oauth2/v2/auth/oauthchooseaccount?response_type=code&client_id=982661621356-vhn1tsqopb7sjoohkbb...

Sign in with Google

Choose an account

to continue to springboot1

adiseshu dasari
as.dasari1988@gmail.com

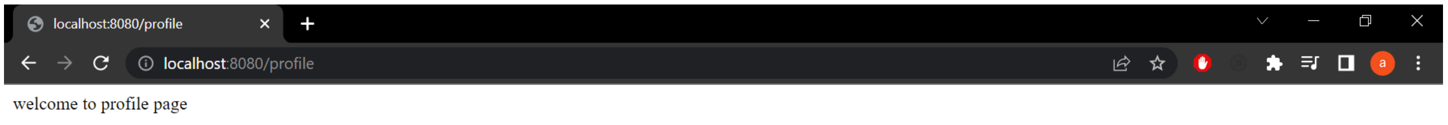
adiseshu dasari
adiseshu.java@gmail.com

adiseshu dasari
adiseshu.trainer@gmail.com

Use another account

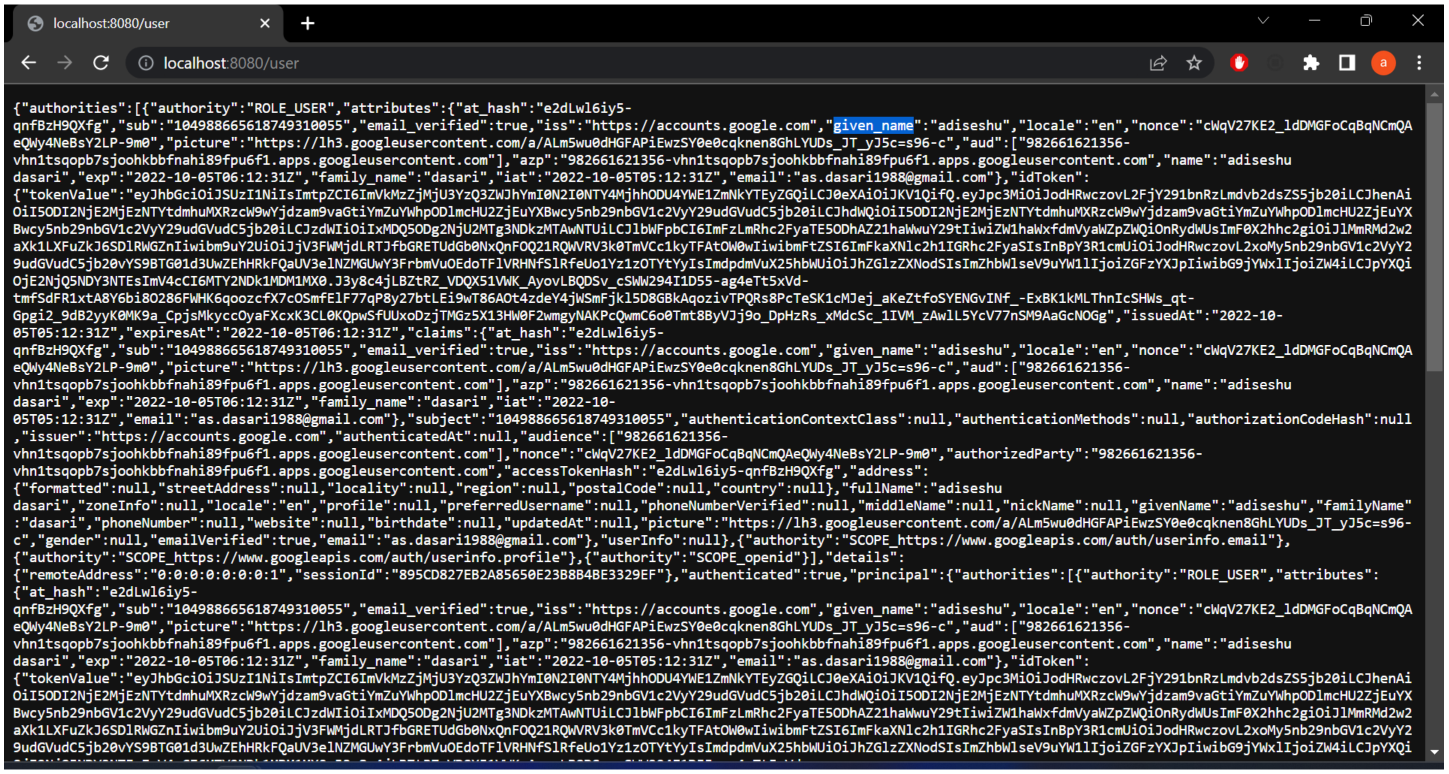
To continue, Google will share your name, email address, language preference, and profile picture with springboot1.

English (United States) Help Privacy Terms

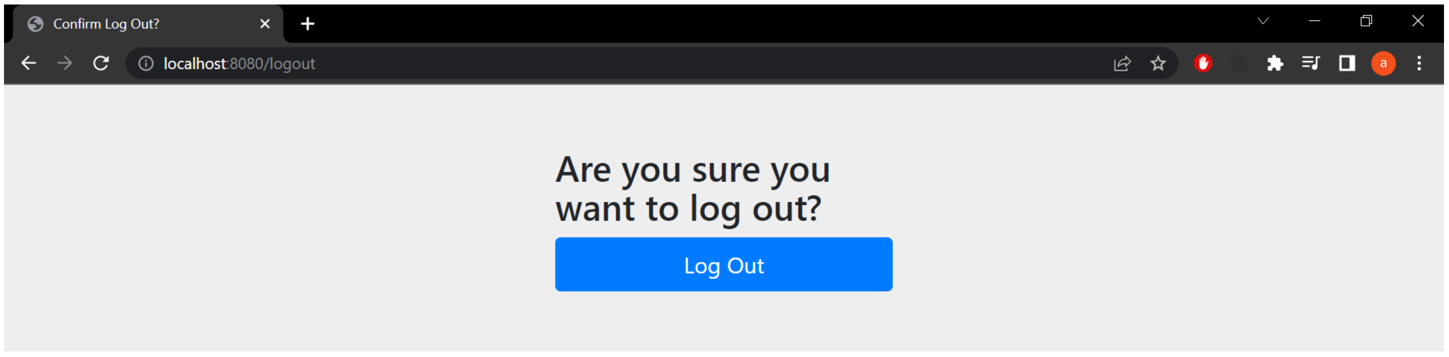

localhost:8080/profile

welcome to profile page

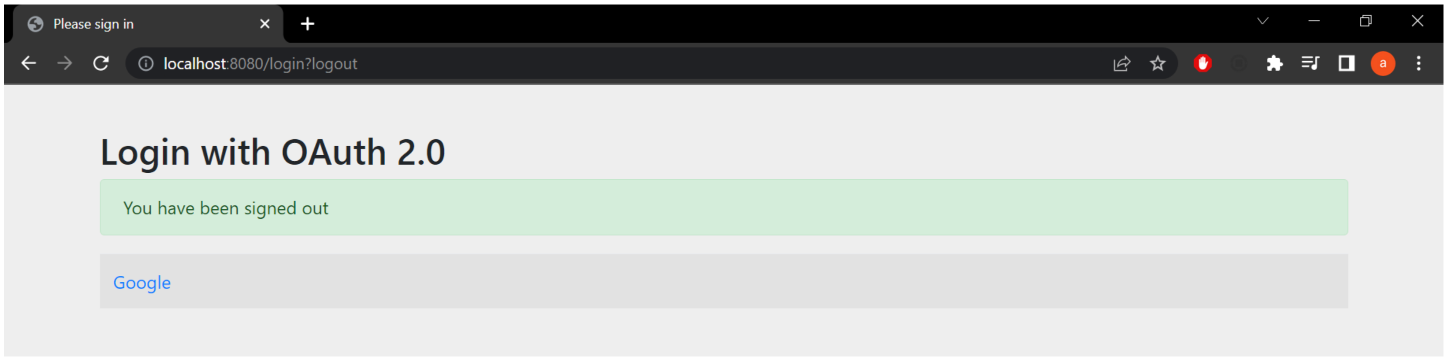
http://localhost:8080/user



```
{"authorities":[{"authority":"ROLE_USER","attributes":{"at_hash":"e2dLwl6iy5-
qnfBzH9QXfg","sub":"104988665618749310055","email_verified":true,"iss":"https://accounts.google.com","given_name":"adiseshu","locale":"en","nonce":"cWqV27KE2_ldDMGFoCqBqNCmQA
eQWy4NeBsY2LP-9m0","picture":"https://lh3.googleusercontent.com/a/ALm5wu0dHGFAPiEwzSY0e0cqknen8GhLYUDs_JT_yJ5c=s96-c","aud":["982661621356-
vhn1tsqopb7sjoohkbbfnahi89fpu6f1.apps.googleusercontent.com"],"azp":"982661621356-vhn1tsqopb7sjoohkbbfnahi89fpu6f1.apps.googleusercontent.com","name":"adiseshu
dasari","exp":"2022-10-05T06:12:31Z","family_name":"dasari","iat":"2022-10-05T05:12:31Z","email":"as.dasari1988@gmail.com"},"idToken":
{"tokenValue":"eyJhbGciOiJSUzI1NiIsImtpZCI6ImVkMzZjMjU3YzQ3ZWJhYmI0N2I0NTY4MjhhODU4YWE1ZmNkYTEyZGQiLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodHRwczovL2FjY291bnRzLmdvb2dsZS5jb20iLCJhenAi
OiI5ODI2NjE2MjEzNTYtdmhuMXRzcW9wYjdzam9vaGtiYmZuYWhpODlmcHU2ZjEuYXBwcy5nb29nbGV1c2VyY29udGVudC5jb20iLCJhdWQiOiI5ODI2NjE2MjEzNTYtdmhuMXRzcW9wYjdzam9vaGtiYmZuYWhpODlmcHU2ZjEuYX
Bwcy5nb29nbGV1c2VyY29udGVudC5jb20iLCJzdWIiOiIxMDQ5ODg2NjU2MTg3NDkzMTAwNTUiLCJlbWFpbCI6ImFzLmRhc2FyaTE5ODhAZ21haWwuY29tIiwiZW1haWxfdmVyaWZpZWQiOnRydWUsImF0X2hhc2giOiJlMmRMd2w2
aXk1LXFuZkJ6SDlRWGZnIiwibm9uY2UiOiJjV3FWMjdLRTJfbGRETUdGb0NxQnFOQ21RQWVRV3k0TmVCc1kyTFAtOW0wIiwibmFtZSI6ImFkaXNlc2h1IGRhc2FyaSIsInBpY3R1cmUiOiJodHRwczovL2xoMy5nb29nbGV1c2VyY2
9udGVudC5jb20vYS9BTG01d3UwZEhHRkFQaUV3elNZMGUwY3FrbmVuOEdoTFlVRHNfSlRfeUo1Yz1zOTYtYyIsImdpdmVuX25hbWUiOiJhZGlzZXNodSIsImZhbWlseV9uYW1lIjoiZGFzYXJpIiwibG9jYWxlIjoiZW4iLCJpYXQi
OjE2NjQ5NDY3NTEsImV4cCI6MTY2NDk1MDM1MX0.J3y8c4jLBZtRZ_VDQX51VWK_AyovLBQDSv_cSWW294I1D55-ag4eTt5xVd-
tmfSdFR1xtA8Y6bi8O286FWHK6qoozcfX7cOSmfElF77qP8y27btLEi9wT86AOt4zdeY4jWSmFjkl5D8GBkAqozivTPQRs8PcTeSK1cMJej_aKeZtfoSYENGvINf_-ExBK1kMLThnIcSHWs_qt-
Gpgi2_9dB2yyK0MK9a_CpjsMkyccOyaFXcxK3CL0KQpwSfUUxoDzjTMGz5X13HW0F2wmgyNAKPcQwmC6o0Tmt8ByVJj9o_DpHzRs_xMdcSc_1IVM_zAwlL5YcV77nSM9AaGcNOGg","issuedAt":"2022-10-
05T05:12:31Z","expiresAt":"2022-10-05T06:12:31Z","claims":{"at_hash":"e2dLwl6iy5-
qnfBzH9QXfg","sub":"104988665618749310055","email_verified":true,"iss":"https://accounts.google.com","given_name":"adiseshu","locale":"en","nonce":"cWqV27KE2_ldDMGFoCqBqNCmQA
eQWy4NeBsY2LP-9m0","picture":"https://lh3.googleusercontent.com/a/ALm5wu0dHGFAPiEwzSY0e0cqknen8GhLYUDs_JT_yJ5c=s96-c","aud":["982661621356-
vhn1tsqopb7sjoohkbbfnahi89fpu6f1.apps.googleusercontent.com"],"azp":"982661621356-vhn1tsqopb7sjoohkbbfnahi89fpu6f1.apps.googleusercontent.com","name":"adiseshu
dasari","exp":"2022-10-05T06:12:31Z","family_name":"dasari","iat":"2022-10-
05T05:12:31Z","email":"as.dasari1988@gmail.com"},"subject":"104988665618749310055","authenticationContextClass":null,"authenticationMethods":null,"authorizationCodeHash":null
,"issuer":"https://accounts.google.com","authenticatedAt":null,"audience":["982661621356-
vhn1tsqopb7sjoohkbbfnahi89fpu6f1.apps.googleusercontent.com"],"nonce":"cWqV27KE2_ldDMGFoCqBqNCmQAeQWy4NeBsY2LP-9m0","authorizedParty":"982661621356-
vhn1tsqopb7sjoohkbbfnahi89fpu6f1.apps.googleusercontent.com","accessTokenHash":"e2dLwl6iy5-qnfBzH9QXfg","address":
{"formatted":null,"streetAddress":null,"locality":null,"region":null,"postalCode":null,"country":null},"fullName":"adiseshu
dasari","zoneInfo":null,"locale":"en","profile":null,"preferredUsername":null,"phoneNumberVerified":null,"middleName":null,"nickName":null,"givenName":"adiseshu","familyName"
:"dasari","phoneNumber":null,"website":null,"birthdate":null,"updatedAt":null,"picture":"https://lh3.googleusercontent.com/a/ALm5wu0dHGFAPiEwzSY0e0cqknen8GhLYUDs_JT_yJ5c=s96-
c","gender":null,"emailVerified":true,"email":"as.dasari1988@gmail.com"},"userInfo":null},{"authority":"SCOPE_https://www.googleapis.com/auth/userinfo.email"},
{"authority":"SCOPE_https://www.googleapis.com/auth/userinfo.profile"},{"authority":"SCOPE_openid"}],"details":
{"remoteAddress":"0:0:0:0:0:0:0:1","sessionId":"895CD827EB2A85650E23B8B4BE3329EF"},"authenticated":true,"principal":{"authorities":[{"authority":"ROLE_USER","attributes":
{"at_hash":"e2dLwl6iy5-
qnfBzH9QXfg","sub":"104988665618749310055","email_verified":true,"iss":"https://accounts.google.com","given_name":"adiseshu","locale":"en","nonce":"cWqV27KE2_ldDMGFoCqBqNCmQA
eQWy4NeBsY2LP-9m0","picture":"https://lh3.googleusercontent.com/a/ALm5wu0dHGFAPiEwzSY0e0cqknen8GhLYUDs_JT_yJ5c=s96-c","aud":["982661621356-
vhn1tsqopb7sjoohkbbfnahi89fpu6f1.apps.googleusercontent.com"],"azp":"982661621356-vhn1tsqopb7sjoohkbbfnahi89fpu6f1.apps.googleusercontent.com","name":"adiseshu
dasari","exp":"2022-10-05T06:12:31Z","family_name":"dasari","iat":"2022-10-05T05:12:31Z","email":"as.dasari1988@gmail.com"},"idToken":
{"tokenValue":"eyJhbGciOiJSUzI1NiIsImtpZCI6ImVkMzZjMjU3YzQ3ZWJhYmI0N2I0NTY4MjhhODU4YWE1ZmNkYTEyZGQiLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodHRwczovL2FjY291bnRzLmdvb2dsZS5jb20iLCJhenAi
OiI5ODI2NjE2MjEzNTYtdmhuMXRzcW9wYjdzam9vaGtiYmZuYWhpODlmcHU2ZjEuYXBwcy5nb29nbGV1c2VyY29udGVudC5jb20iLCJhdWQiOiI5ODI2NjE2MjEzNTYtdmhuMXRzcW9wYjdzam9vaGtiYmZuYWhpODlmcHU2ZjEuYX
Bwcy5nb29nbGV1c2VyY29udGVudC5jb20iLCJzdWIiOiIxMDQ5ODg2NjU2MTg3NDkzMTAwNTUiLCJlbWFpbCI6ImFzLmRhc2FyaTE5ODhAZ21haWwuY29tIiwiZW1haWxfdmVyaWZpZWQiOnRydWUsImF0X2hhc2giOiJlMmRMd2w2
aXk1LXFuZkJ6SDlRWGZnIiwibm9uY2UiOiJjV3FWMjdLRTJfbGRETUdGb0NxQnFOQ21RQWVRV3k0TmVCc1kyTFAtOW0wIiwibmFtZSI6ImFkaXNlc2h1IGRhc2FyaSIsInBpY3R1cmUiOiJodHRwczovL2xoMy5nb29nbGV1c2VyY2
9udGVudC5jb20vYS9BTG01d3UwZEhHRkFQaUV3elNZMGUwY3FrbmVuOEdoTFlVRHNfSlRfeUo1Yz1zOTYtYyIsImdpdmVuX25hbWUiOiJhZGlzZXNodSIsImZhbWlseV9uYW1lIjoiZGFzYXJpIiwibG9jYWxlIjoiZW4iLCJpYXQi
```



Are you sure you want to log out?



Login with OAuth 2.0

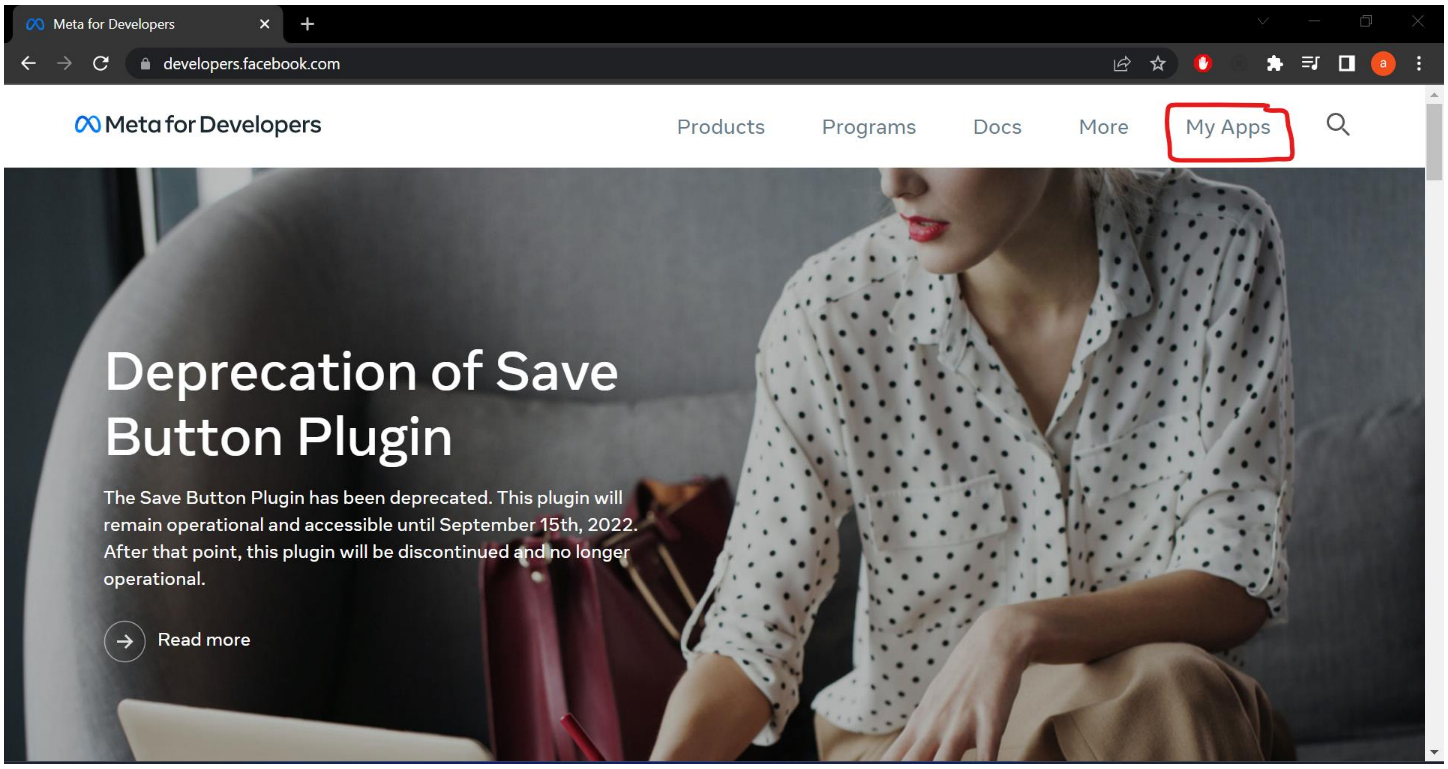
You have been signed out

One Time setup for Facebook OAuth2:

Step 1: Go to the fallowing url;

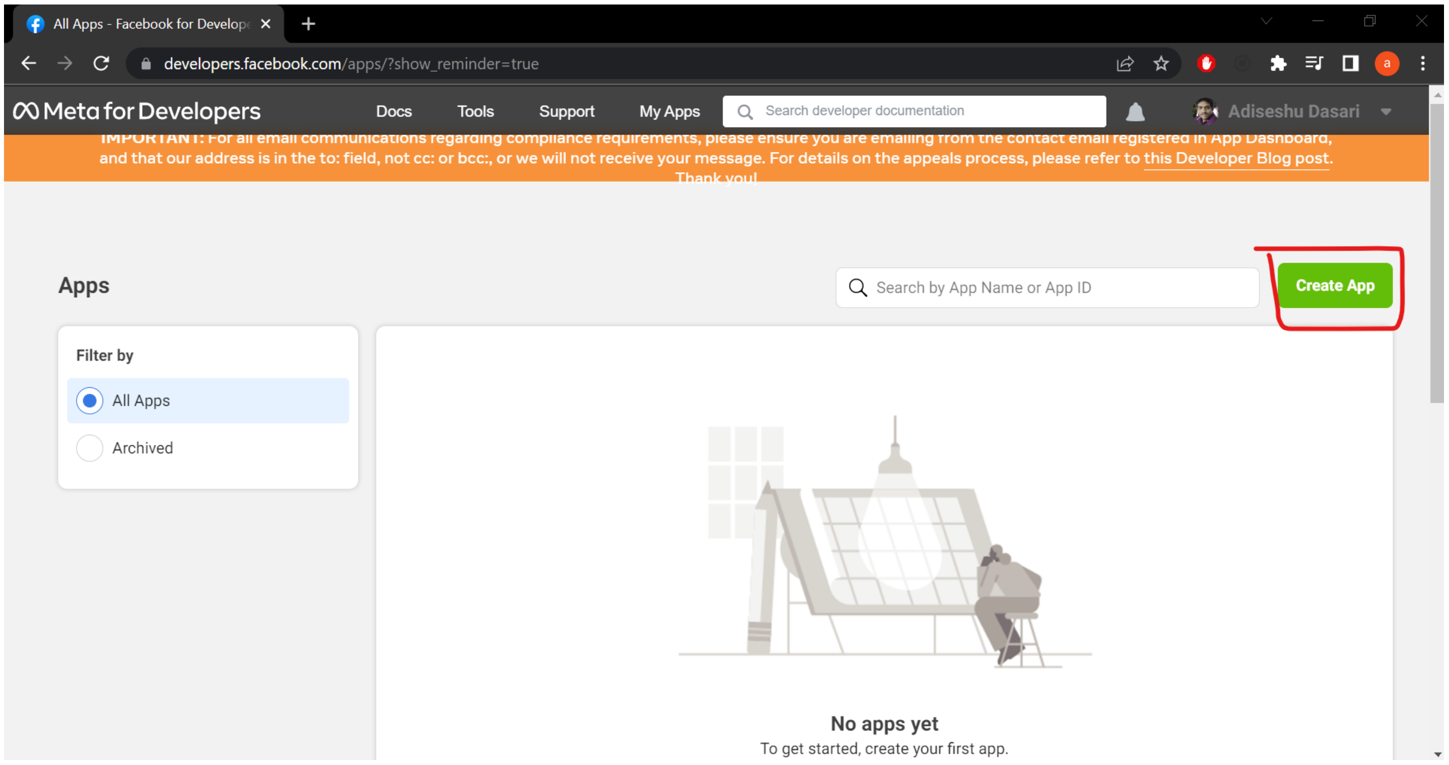
https://developers.facebook.com/

Select My Apps



Deprecation of Save Button Plugin

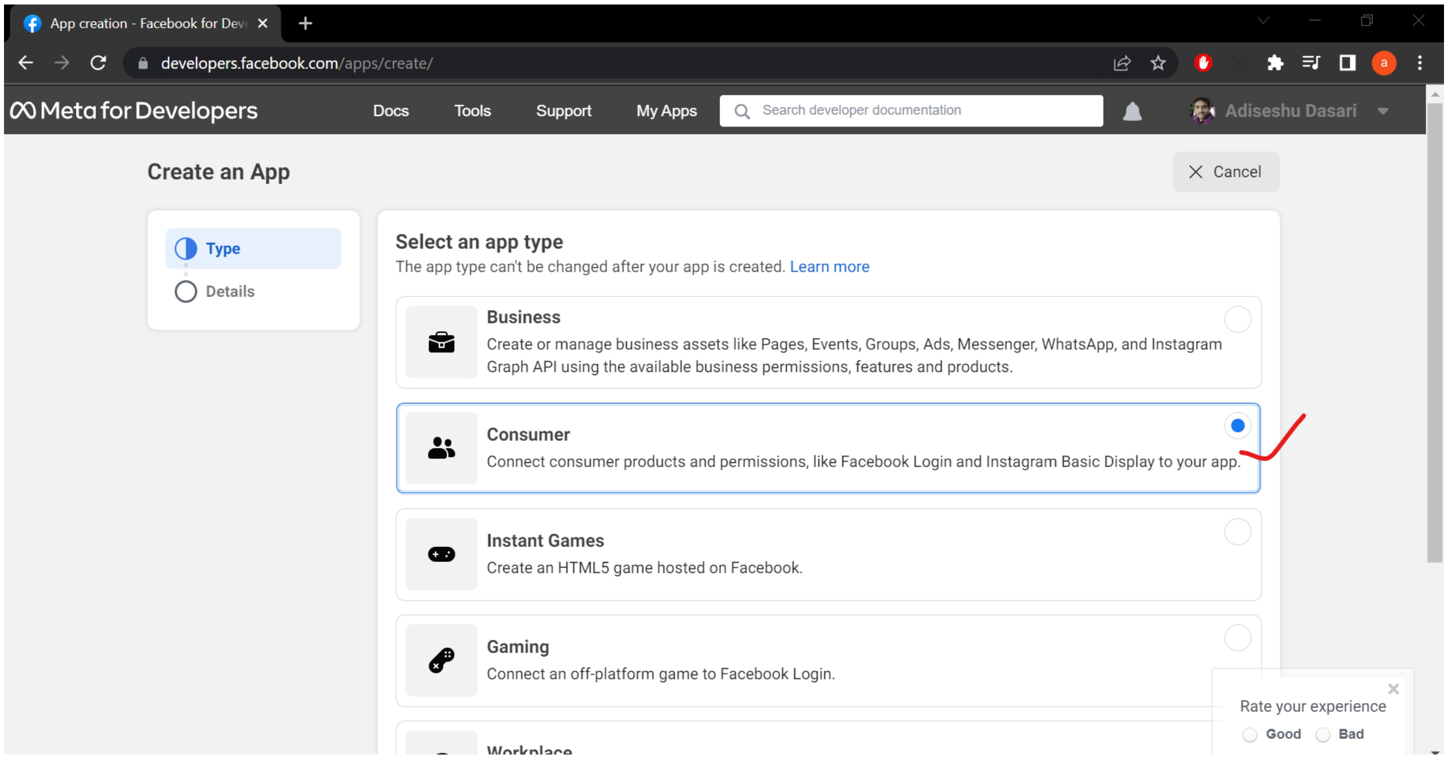
The Save Button Plugin has been deprecated. This plugin will remain operational and accessible until September 15th, 2022. After that point, this plugin will be discontinued and no longer operational.


All Apps - Facebook for Develope
developers.facebook.com/apps/?show_reminder=true
Meta for Developers
Docs
Tools
Support
My Apps
Search developer documentation
Adiseshu Dasari
Create App
Search by App Name or App ID
Filter by
All Apps
Archived

IMPORTANT: For all email communications regarding compliance requirements, please ensure you are emailing from the contact email registered in App Dashboard, and that our address is in the to: field, not cc: or bcc:, or we will not receive your message. For details on the appeals process, please refer to this Developer Blog post. Thank you!

Apps

No apps yet
To get started, create your first app.



Create an App

Select an app type
The app type can't be changed after your app is created. Learn more

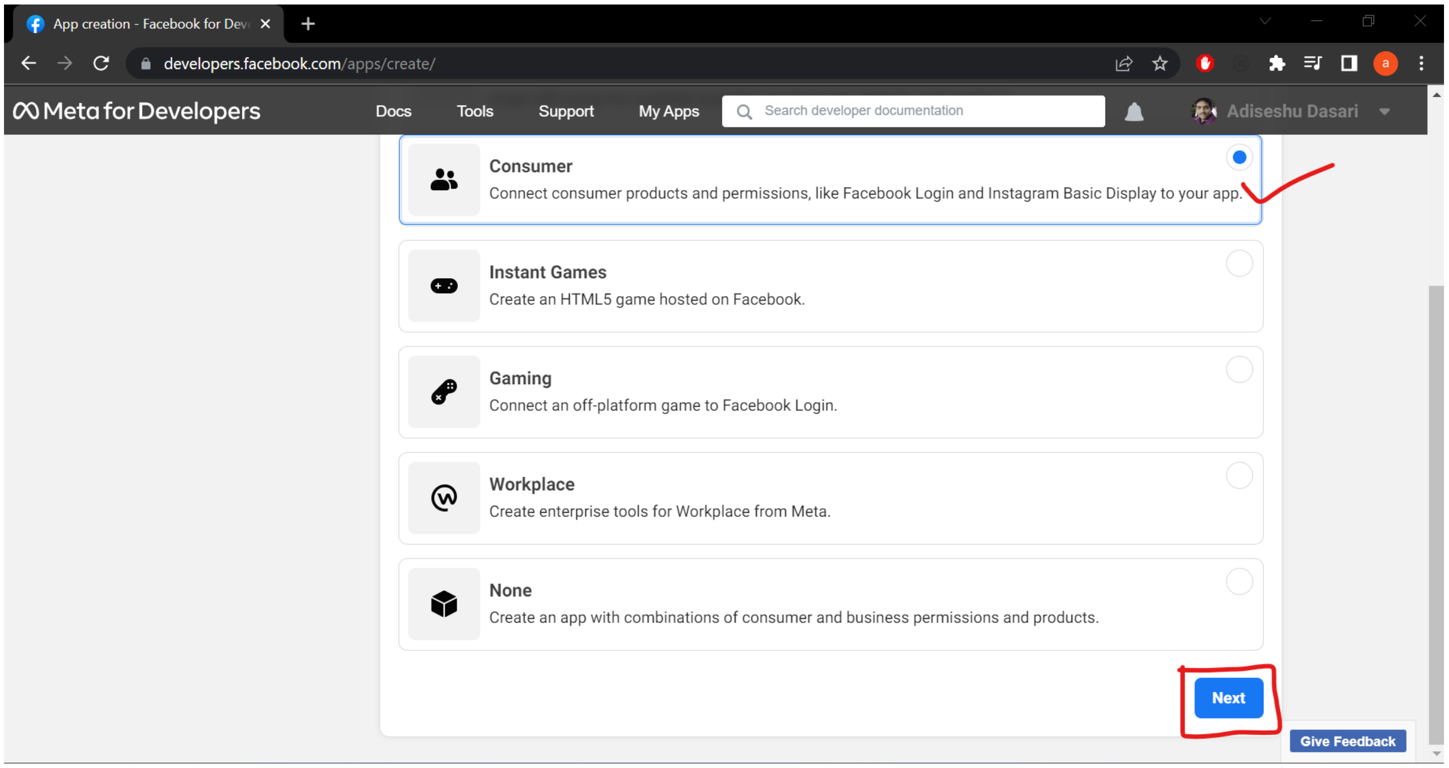
Business
Create or manage business assets like Pages, Events, Groups, Ads, Messenger, WhatsApp, and Instagram Graph API using the available business permissions, features and products.

[✓ Consumer]
Connect consumer products and permissions, like Facebook Login and Instagram Basic Display to your app.

Instant Games
Create an HTML5 game hosted on Facebook.

Gaming
Connect an off-platform game to Facebook Login.

Workplace


App creation - Facebook for Deve
developers.facebook.com/apps/create/
Meta for Developers
Docs
Tools
Support
My Apps
Search developer documentation
Adiseshu Dasari
Next
Give Feedback

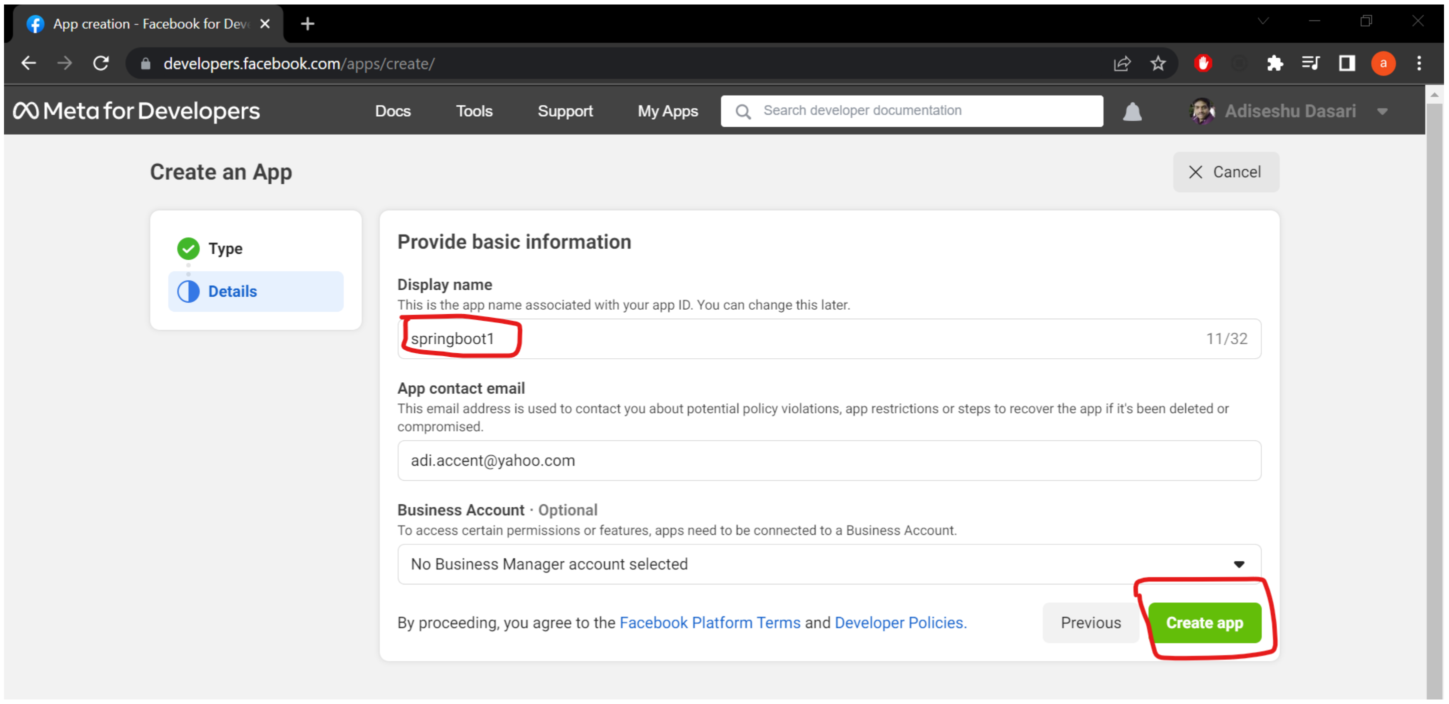
Consumer [✓]
Connect consumer products and permissions, like Facebook Login and Instagram Basic Display to your app.

Instant Games
Create an HTML5 game hosted on Facebook.

Gaming
Connect an off-platform game to Facebook Login.

Workplace
Create enterprise tools for Workplace from Meta.

None
Create an app with combinations of consumer and business permissions and products.


App creation - Facebook for Deve
developers.facebook.com/apps/create/
Meta for Developers
Docs
Tools
Support
My Apps
Search developer documentation
Adiseshu Dasari
Cancel
Type
Details
Previous
Create app

Create an App

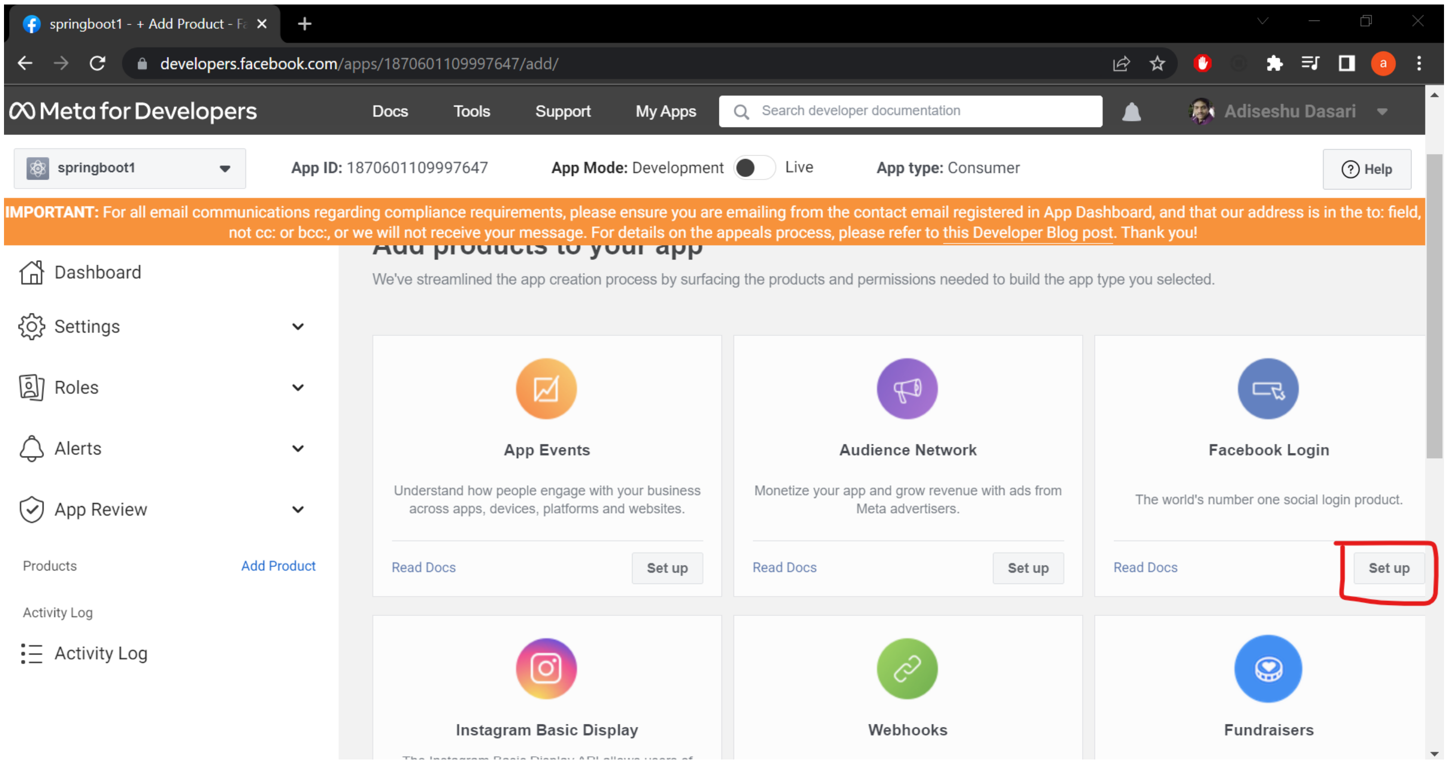
Provide basic information

Display name
This is the app name associated with your app ID. You can change this later.
springboot1 11/32

App contact email
This email address is used to contact you about potential policy violations, app restrictions or steps to recover the app if it's been deleted or compromised.
adi.accent@yahoo.com

Business Account · Optional
To access certain permissions or features, apps need to be connected to a Business Account.
No Business Manager account selected

By proceeding, you agree to the Facebook Platform Terms and Developer Policies.



springboot1 - + Add Product - F

developers.facebook.com/apps/1870601109997647/add/

Meta for Developers | Docs | Tools | Support | My Apps | Search developer documentation | Adiseshu Dasari

springboot1 | App ID: 1870601109997647 | App Mode: Development | Live | App type: Consumer | Help

IMPORTANT: For all email communications regarding compliance requirements, please ensure you are emailing from the contact email registered in App Dashboard, and that our address is in the to: field, not cc: or bcc:, or we will not receive your message. For details on the appeals process, please refer to this Developer Blog post. Thank you!

Add products to your app

We've streamlined the app creation process by surfacing the products and permissions needed to build the app type you selected.

App Events — Understand how people engage with your business across apps, devices, platforms and websites. Read Docs | Set up

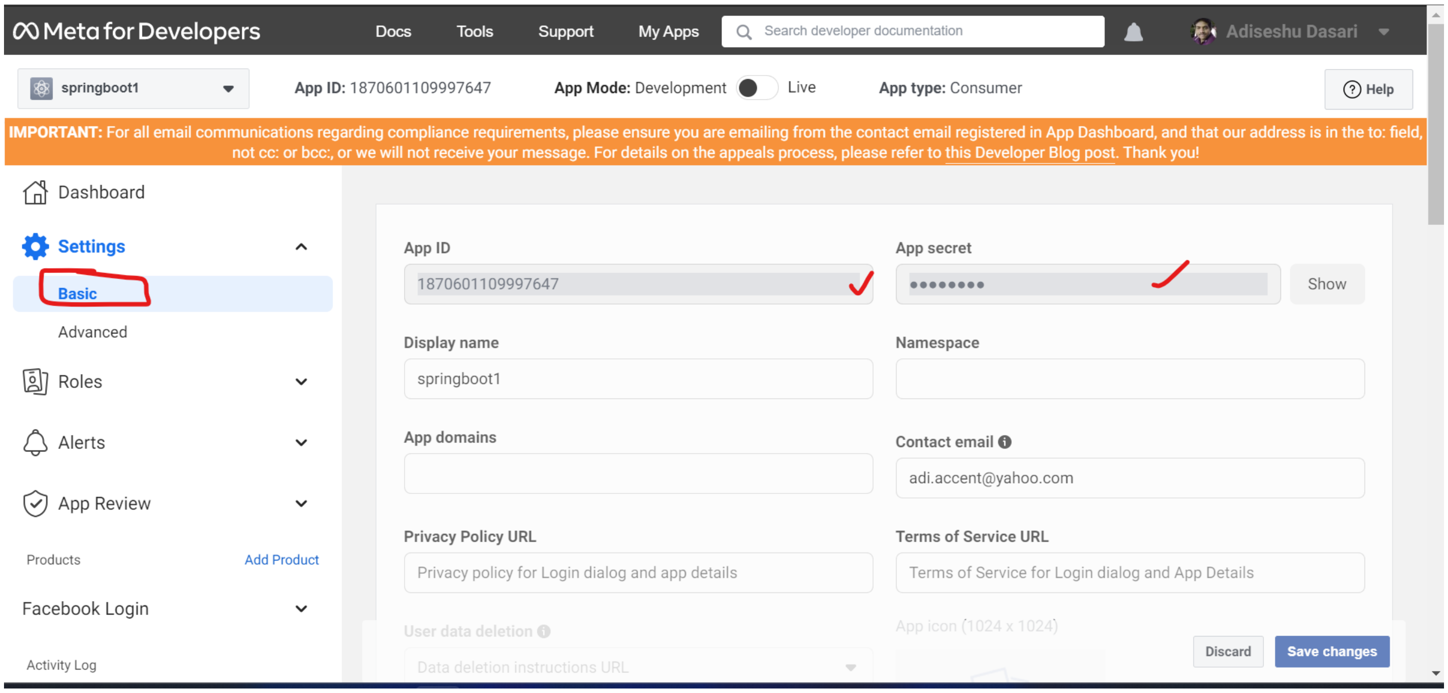
Audience Network — Monetize your app and grow revenue with ads from Meta advertisers. Read Docs | Set up

Facebook Login — The world's number one social login product. Read Docs | Set up

Instagram Basic Display

Webhooks

Fundraisers



Meta for Developers | Docs | Tools | Support | My Apps | Search developer documentation | Adiseshu Dasari

springboot1 | App ID: 1870601109997647 | App Mode: Development | Live | App type: Consumer | Help

IMPORTANT: For all email communications regarding compliance requirements, please ensure you are emailing from the contact email registered in App Dashboard, and that our address is in the to: field, not cc: or bcc:, or we will not receive your message. For details on the appeals process, please refer to this Developer Blog post. Thank you!

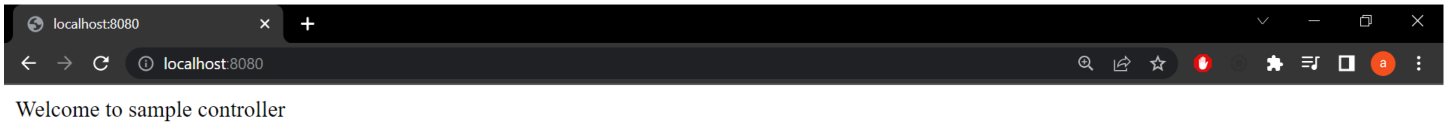
App ID: 1870601109997647	App secret: •••••••• Show
Display name: springboot1	Namespace:
App domains:	Contact email: adi.accent@yahoo.com
Privacy Policy URL: Privacy policy for Login dialog and app details	Terms of Service URL: Terms of Service for Login dialog and App Details
User data deletion: Data deletion instructions URL	App icon (1024 x 1024)

Discard | Save changes

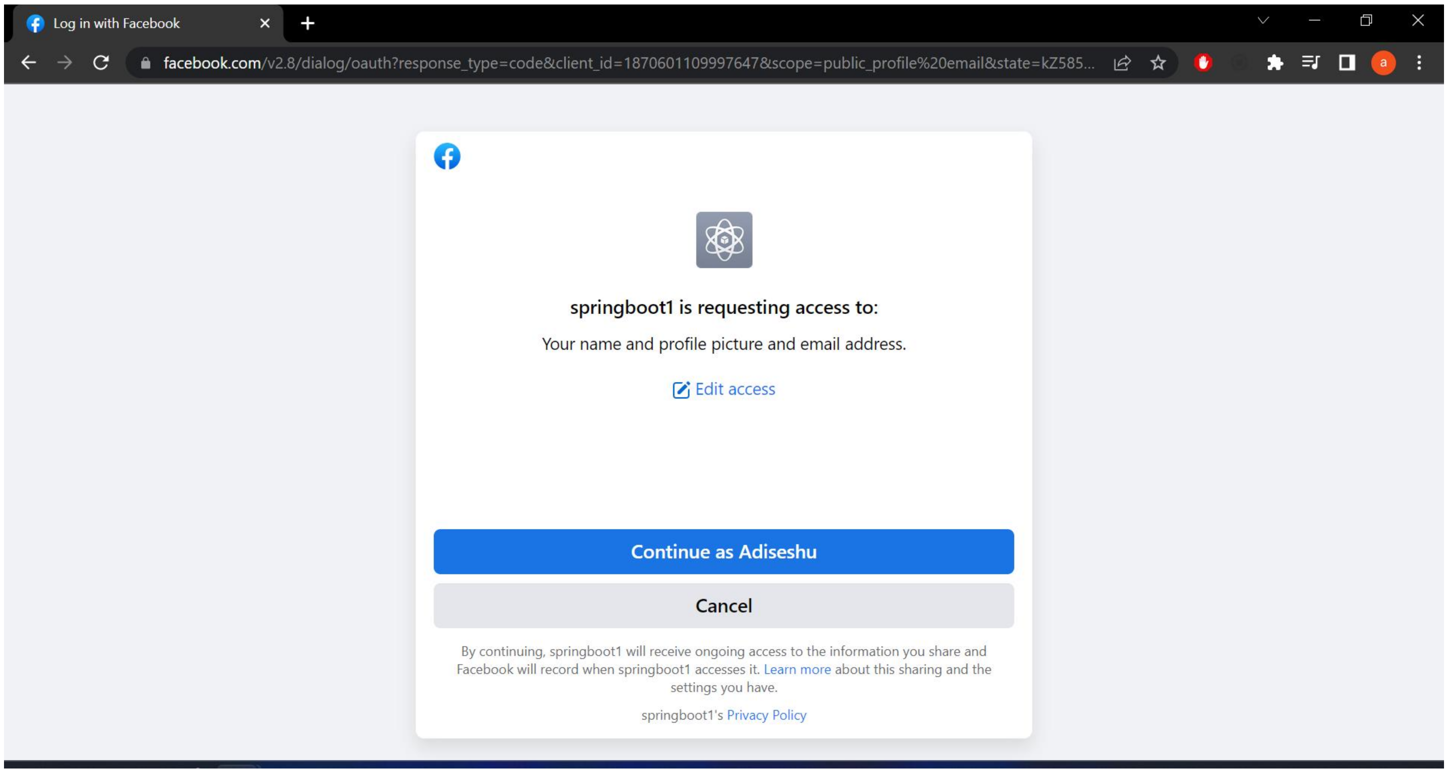
Only update the application.yml file of ***spring-boot-oauth*** project

```
spring:
  security:
    oauth2:
      client:
        registration:
          facebook:
            client-id: 1870601109997647
            client-secret: b1ce3649586841fa018bd3d9d3fa2174
```

Test the application


localhost:8080

Welcome to sample controller

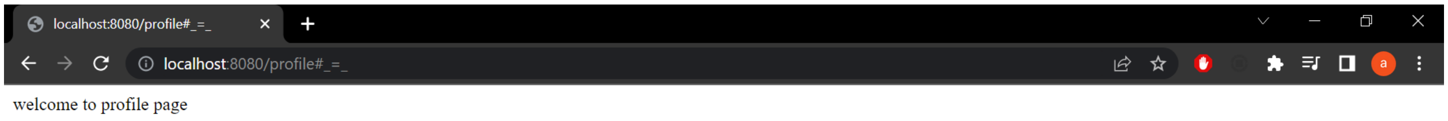

facebook.com/v2.8/dialog/oauth?response_type=code&client_id=1870601109997647&scope=public_profile%20email&state=kZ585...

springboot1 is requesting access to:

Your name and profile picture and email address.

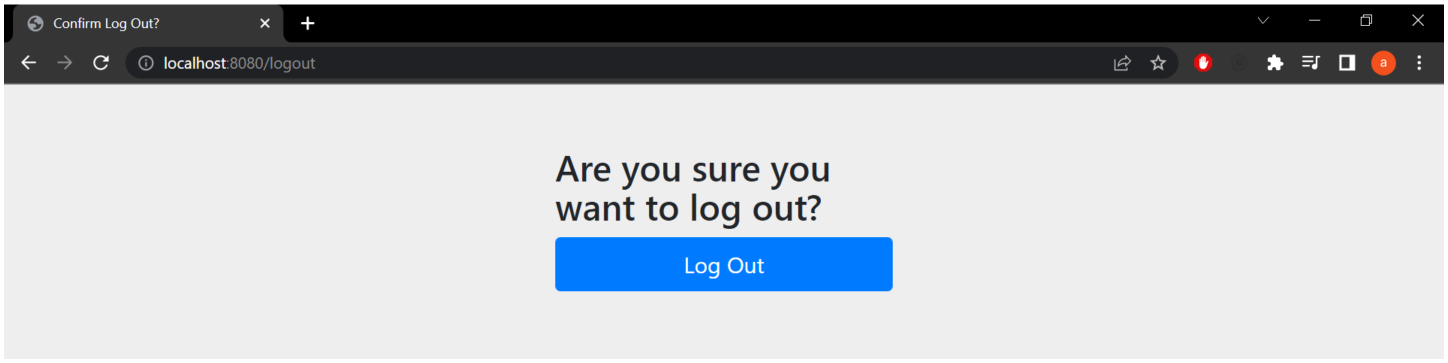
By continuing, springboot1 will receive ongoing access to the information you share and Facebook will record when springboot1 accesses it. Learn more about this sharing and the settings you have.

springboot1's Privacy Policy



localhost:8080/profile#_=_

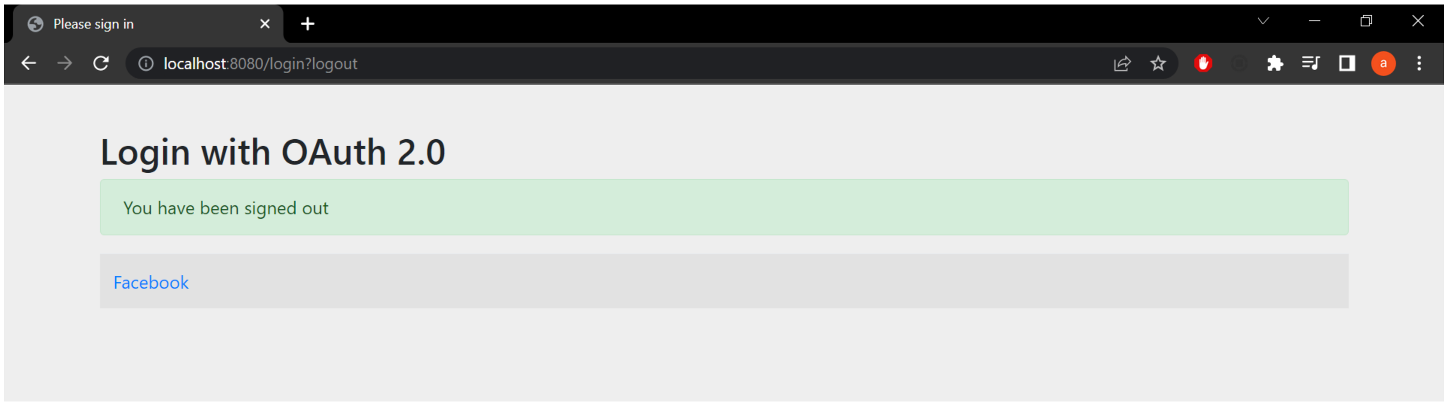
welcome to profile page



Confirm Log Out?

localhost:8080/logout

Are you sure you want to log out?



Please sign in

localhost:8080/login?logout

Login with OAuth 2.0

You have been signed out