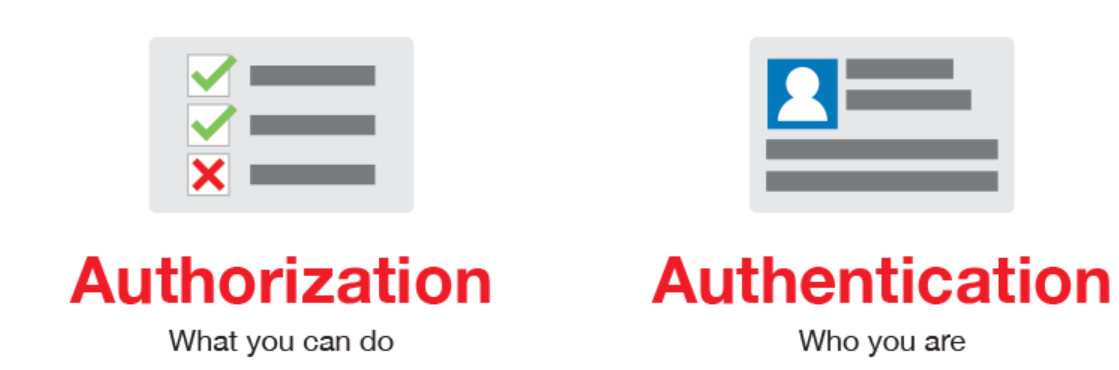
**Request Authentication/ Authorization**



Authentication: used to check whether you are valid user or not?

Authorization: used to check your permission / accesses to the resource

* Almost every REST API must have authorization to check whether you are authorized client or not? before allowing access to the resource
* Authentication is present in header of the request.

**There are 4 types of authorisation:**

1. **Bearer token** : Required “TokenID” to access an API
2. **Basic auth**: Required “Username & Password “ for to access an API

**3**. **OAuth 1.0** : Two level authentication

1. **OAuth 2.0** : One level authentication

**OAuth** : is an Open Standard for Authorization protocol, widely used in web application , which allows API services to accesses user data without sharing is password.

**Basic Auth** : used to access the resource via username / password

**public** **class** BasicAuthTest {

@Test

**public** **void** loginCheck() {

*given*()

.auth().basic("rmgyantra", "rmgy@9999")

.when()

.get("http://localhost:8084/login")

.then()

//.assertThat().statusCode(202)

.log().all();

}

}

Disadvantages: sharing the username /password is not advisable via API , some body can hack your Data

**Bearer Token** : used to access the resource via bearer token ID , that is unique Id to access all the API recourse

**public** **class** BearerTokenTest {

@Test

**public** **void** loginCheck() {

HashMap map = **new** HashMap();

map.put("name", "SDET-17");

*given*()

.auth().oauth2("ghp\_SZaViG7x70Wg3ZIgLKQAGr2Av722Ta2PMFfz")

.contentType(ContentType.***JSON***)

.body(map)

.when()

.post("https://api.github.com/user/repos")

.then()

//.assertThat().statusCode(202)

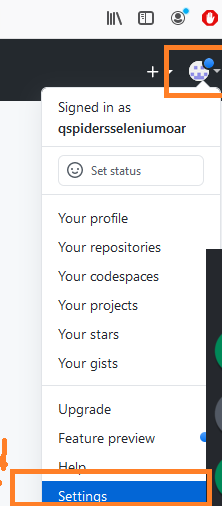
.log().all();

}

}

How to create Bearer Token in GITHUB?

1. Go to gitHUB URL <http://github.com>
2. Create an Account with GitHUB
3. Login to Git HUB
4. Go to user Menu 🡺 click Settings



5.click on “Developers settings”

6. Click on “personal Access token”

7. Click on “Generate new Token” button

8. Enter the name & select “Repo” CheckBox

9. Click on “Generate a Token”

10 . Copy the Token ID

How to get REST-API to Create Repository in GITHUB

1. Go to GIT API Functional Spec Document

<https://docs.github.com/en>

1. Copy the Base URI

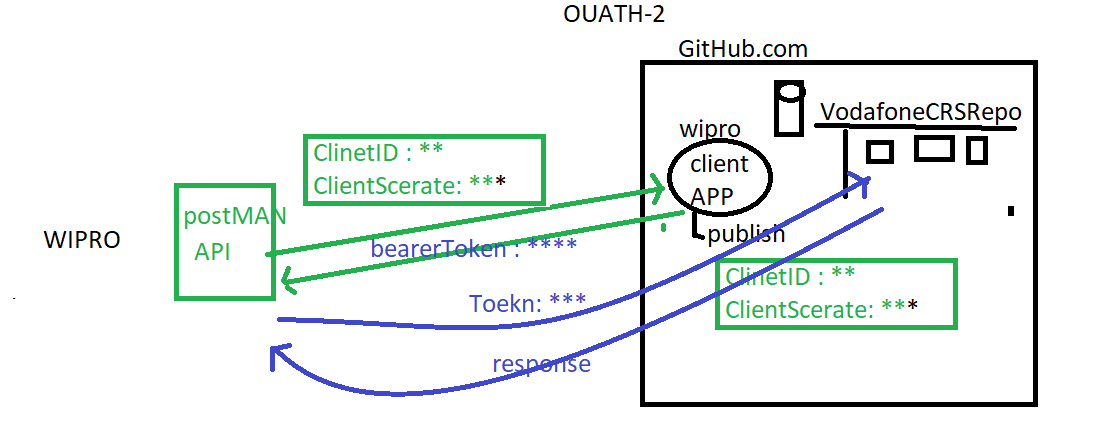
<https://docs.github.com/en/rest/overview/resources-in-the-rest-api>

1. Copy the End PONT & get the JSON BODY structure

<https://docs.github.com/en/rest/reference/repos#create-a-repository-for-the-authenticated-user>

Disadvantages of Bearer Token :

**OAUTH**-2 :

* Whenever your application requests private user data, it must send an OAuth 2.0 token along with the request. Your application first sends a client ID and, client secret to obtain a token. You can generate OAuth 2.0 credentials for web applications, service accounts, or installed applications.
* One level of Authentication
* Client application includes “client secret” with every request.
* 

**package** com.rmgyantra.Authentication;

**import** org.testng.annotations.Test;

**import** io.restassured.response.Response;

**import** **static** io.restassured.RestAssured.\*;

**public** **class** OAuthTest {

@Test

**public** **void** oAuthTest()

{

Response rsps = *given*()

.formParam("client\_id", "SDET5")

.formParam("client\_secret", "893e26cfe9558facd18892231e7f1eb5")

.formParam("grant\_type", "client\_credentials")

.formParam("redirect\_uri", "https://example.com")

.when()

.post("http://coop.apps.symfonycasts.com/token");

String token=rsps.jsonPath().get("access\_token");

System.***out***.println(token);

*given*()

.auth().oauth2(token)

.pathParam("USER\_ID", "2527")

.when()

.post("http://coop.apps.symfonycasts.com/api/{USER\_ID}/eggs-collect")

.then()

.log()

.all();

}

}

**OAUTH-1 :**

* **Consumer key and secret & Access Token / Access Secret**: These two strings are used to identify and authenticate the client application
* **Two level of Authetication**
* 