**OAuth 2:** es un framework de autorización que permite a las aplicaciones obtener acceso (limitado) a las cuentas de determinados servicios, como Facebook, Github, Twitter, Google+ y mucho mas.

Consiste en delegar la autentificación de usuario al servicio que gestiona las cuentas, de modo que sea este quien otorgue el acceso para las aplicaciones de terceros.

Roles Presentes en OAuth:

En el protocolo que define OAuth podemos identificar **4 roles:**

**Cliente:** Es la aplicación Que quiere acceder a la cuenta de un usuario, en un servicio determinado. A fin de conseguir ello, debe contar con una autorización del usuario, y esta autorización se debe validar (a través de la API del servicio.)

**Resource Owner:** El “dueño del recurso” es el usuario que autoriza a una aplicación para que pueda acceder a su cuenta. EL acceso está limitado en función de “Scope” que ha concedido el usuario en la autorización.

**Resource server y Authorization Server:** Resource server es el servidor que almacena las cuetas de usuarios y authorization server es el servidor que verifica la identidad de los usuarios y emite acces tokens a la aplicación cliente.

Flujo de protocolo Oauth

El flujo descrito a continuación es un flujo generico que representa al protocolo Oauth. Sin Embargo, podemos encontrar diferencias en función al authorization grant type (es decir, según las condiciones en que se está implementado Oauth; que vería principalmente si se trata de una aplicación web, movil o de escritorio).

1. La aplicación cliente solicita una autorización para acceder a los recursos de un usuario en un servicio determinado.
2. Si el usuario autoriza la solicitud, la aplicación recibe una authorization grant (concesion de autorizacion).
3. La aplicación solicita un access token al ahutorization server (API) presentando su identidad, y el permiso concedido anteriormente.
4. Si la identidad de la aplicación cliente se reconoce correctamente por el servicio, y la concesion de autorización es valida el authorization server (API) emite un access token a la aplicación. Con esto la autorización está completa.
5. La aplicación solicita un recurso al resource server (API) y presenta el correspondiente access token.
6. Si el access token es valido, el resource server (API) hace entrega del recurso a la aplicación.

EJEMPLO:

Imaginemos que queremos iniciar sesion via Facebook:

Se desarrolla la siguiente secuencia:

* Un usuario entra a Nuestra pagina (digamos que nuestra pagin se llama PYM), y hace click en “Ingresar usando Facebook”.
* Nuestra aplicación lo va a redirigir a una URL como la siguiete: ….
* Esta URL contiene los siguientes parametros: un client\_id, una redirect\_uri y opcionalmente un paramentro scopes (para indicar que informacion queremos acceder).
* Facebook primero va a ver si nuestro xlient-id es valido (comparandolo con la lista de oauth\_cliente permitidos).
* Si todo está correcto, entonces define una variable de sesion que guarda niestro cliente\_id y redirect\_uri Y entonces:
* Redirige al usuario a facebook.com/login ( muestra un formulario de inicio de sesion) si el usuario aun no ha iniciado sesion.
* O avanza directamente al siguiente paso si ya hay una sesion activa en facebook.
* Facebook muestra el logo de PYM y el nombre de la app (lo reconoce a partir del client\_id) indicando al usuario: “esta app quiere acceder a tus datos …”

Si aceptamos entonces:

* Facebook genera un codigo (que tiene un solo uso valido para PYM, el usuario en cuestion y el escope solicitado). Facebook redirige al usuario según la redirect\_uri indicada al inicio.
* PYM toma el codigo que recibe de Facebook y vuelve a hacer una peticion a Facebook incluyendo ahora su client\_secret.

Esta ultima peticion no se trata de una redireccion a nivel de navegador, sino mas bien de una solicitud de servidor a servidor.

* Facebook verifica que el codigo sea valido, y asi mismo lo invalida en ese instante Entonces Facebook responde con un AccessTOken, que pym podra usar (hasta que expire) para hacer peticiones a la API, en nombre del usuario que ha otorgado permiso.