**6 POMA AGUILAR, DAYSE NICOLE**

**What is OAuth?**

It is an authorization protocol that gives applications the ability to “secure designated access”, which allows you to approve an application that interacts with another on your behalf without revealing your password. Allowing to minimize the risk of data leakage.

The OAuth (Open Authorization) protocol was developed by the Internet Engineering Task Force and enables secure delegated access. Allows an application to access a resource controlled by another person (end user). This type of access requires Tokens, which represent the delegated right of access. This is why applications gain access without impersonating the user who controls the resource.

**Features**

The idea of ​​roles is central to the OAuth framework and defines the essential components of a system:

* Resource Owner: The user or system that owns the protected resources and can grant access to them.
* Client: The client is the system that requires access to the protected resources. To access the resources, the Client must have the appropriate access token.
* Authorization server: This server receives requests for access tokens from the client and issues them upon successful authentication and consent of the resource owner. The authorization server exposes two endpoints: the authorization endpoint, which handles interactive authentication and user consent, and the token endpoint, which is involved in machine-to-machine interaction.
* Resource Server: A server that protects user resources and receives access requests from the Client. Accepts and validates an access token from the client and returns the appropriate resources to it.

Bibliography

*Google Developers OAuth 2.0 Playground. Retrieved June 10, 2022 from https://developers.google.com/oauthplayground/*