JWT claims

- "Claims" are pieces of information that can be included in a JWT.
- They represent user attributes, roles, permissions, or other relevant information.
- They allow servers to validate and restrict access to resources based on the user's roles and permissions.
- Claims are included in the body of the JWT token and are protected by a digital signature.
- This ensures that the claims are not manipulated during transmission and that the information contained in the token is reliable and valid.

Types of JWT claims

- **Registered claims:**
  - Defined in the JWT specification (iss, sub, aud, iat, exp, nbf...)
  - Used to provide standard and necessary information for authentication and authorization.
- **Public claims:**
  - Not defined in the JWT specification but commonly used.
  - Examples: name, email, specific application roles...
  - Customizable and specific to each application.
- **Private claims:**
  - Customized and specific to an application or service.
  - Not defined in the JWT specification and not commonly used in other applications.
  - Used for specific and sensitive information that does not need to be shared with other systems.

Singularity Hackers 0xWORD My Public Inbox

Registered JWT claims

- **Issuer (iss):**
  - Indicates the entity that issued the JWT token.
  - Example: "*https://myapp.com*".
- **Subject (sub):**
  - Identifies the subject of the JWT token.
  - Can be a unique user identifier.
  - Example: "*1234567890*".
- **Audience (aud):**
  - Indicates the audience for which the JWT token is intended.
  - Can be an array of values.
  - Example: *["https://myapp.com", "https:/myapp2.com"]*.
- **Expiration Time (exp):**
  - Indicates the time at which the JWT token's validity expires.
  - Represented in seconds since the Unix epoch.
  - Example: *1615967200*.
- **Not Before (nbf):**
  - Indicates the time from which the JWT token is valid.
  - Represented in seconds since the Unix epoch.
  - Example: *1615963600*.
- **Issued At (iat):**
  - Indicates the time at which the JWT token was issued.
  - Represented in seconds since the Unix epoch.
  - Example: *1615963600*.
- **JWT ID (jti):**
  - Provides a unique identifier for the JWT token.
  - Useful for avoiding token repetition and for tracking issued tokens.
  - Example: "*abc123xyz*".

JWT claims exercise

- Install a library to work with JWT (e.g., with Python)
- Generate a JWT token with the library and test its functionality.
- Specific claims must be configured for the expiration and validity of the token:
  - It is not valid until 5 minutes after its issuance.
  - It is not valid after 30 minutes after its issuance.
- Other claims can be explored, such as subject identification or token identification.

Singularity Hackers 0xWORD My Public Inbox