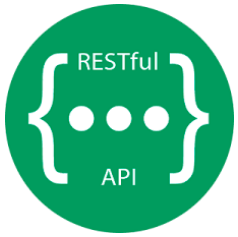
Writing Beautiful RESTful APIs

Ethan Ballinger



Advanced Topics: Authentication

Advanced Topics: Authentication

- What makes authentication important?
- Basic authentication
- OAuth 2.0 authentication

What makes authentication important?

- There are several lines of thought on how to handle authentication for an API
- Some APIs don't need authentication, but unless they are trivial they will at some point
- Authentication can provide the following benefits:

1) Protects the system from unwanted access
2) Allows developers to control level of access (RBAC)
3) Allows developers to gather additional information about how users interact with their system

Basic authentication

- Basic authentication allows you to provide a username and password to access the API
- This is the easiest of the 2 to implement as it is a simple validation against the identity provider
- The downside to basic authentication is if SSL is not used, the username/password can be exposed over the request
- Developers should always implement their API using SSL as it provides an additional layer of security for the user
- If implementing basic authentication, the username/password should be provided as part of an Authorization header

OAuth 2.0 authentication

- OAuth is a type of token authentication allows you to provide a username and password to gain a token that provides you access to the API

- The general flow is as follows:

1) Client requests authorization from user
2) User provides authorization to client
3) Client provides authorization to authentication server
4) Authentication server provides token to client
5) Client provides token to API
6) API provides response to client

OAuth 2.0 authentication (cont.)

- OAuth requires a more complex setup and management, but provides additional security as the client never has to provide their password to the API
- This also gives developers tighter control over access to their API
- The authorization grant can be configured to provide partial access or access for a certain period of time