

# Intermediate APIs in R: Takeaways

by Dataquest Labs, Inc. - All rights reserved © 2021

## Syntax

- Customizing our function to use query parameters:

```
wb_api_json_get_df <- function(endpoint, queries = list()) {  
  # Preparing the URL  
  url <- modify_url("http://api.worldbank.org", path = endpoint)  
  # API requests  
  response <- GET(url, query = queries)  
  # Tracking errors  
  if ( http_error(response) ){  
    print(status_code(response))  
    stop("Something went wrong.", call. = FALSE)  
  }  
  if (http_type(response) != "application/json") {  
    stop("API did not return json", call. = FALSE)  
  }  
  # Extracting content  
  json_text <- content(response, "text")  
  # Converting content into Dataframe  
  dataframe <- jsonlite::fromJSON(json_text)  
  # Return the dataframe  
  dataframe[[2]]  
}
```

- Adding a query parameter:

```
query = list(format = "json")
```

- Defining pagination query parameters:

```
query = list(page = 2, per_page = 100)
```

- Passing in a token to authorize API access:

```
query = list(api_key = "1f36137fbbe1602f779300dad26e4c1b7fbab631")
```

- Using a POST request to create a repository:

```
body = list(message = "this message", name = "authordq")
```

## Concepts

- Pagination allows for a certain number of records per page.
- APIs use authentication to perform rate limiting. Rate limiting ensures the user can't overload the API server by making too many requests too quickly. It keeps the API server available and responsive for all users.
- Rate limiting ensures the user can't overload the API server by making too many requests too quickly.

- APIs requiring authentication use an access token. An access token is a string the API can read and associate with our account. Tokens are better than a username and password for the following security reasons:
  - Typically someone accesses an API from a script. If we put our username and password in a script and someone finds it, they can take over our account. If someone manages to get the access token, we can revoke the access token.
  - Access tokens can also have scopes in specific permissions. We can generate multiple tokens that give different permissions for more control over security.
- Different API endpoints choose what types of requests they will accept.
  - We use POST requests to send information and to create objects on the API's server. POST requests almost always include data so the server can create the new object. A successful POST request will return a 200 status code.

## Resources

- [Data Gov API documentation](#)
- [Understanding REST](#)