Adrián Bertos Gómez - PumukyDev

API Testing <https://PumukyDev.github.io/portswigger-websecurity-academy/api-testing.pdf>`_

API recon

> To start API testing, you first need to find out as much information about the API as possible, to discover its attack surface.

To begin, you should identify API endpoints. These are locations where an API receives requests about a specific resource on its server. For example, consider the following GET request: GET /api/books HTTP/1.1 Host: example.com

The API endpoint for this request is /api/books. This results in an interaction with the API to retrieve a list of books from a library. Another API endpoint might be, for example, /api/books/mystery, which would retrieve a list of mystery books.

Once you have identified the endpoints, you need to determine how to interact with them. This enables you to construct valid HTTP requests to test the API. For example, you should find out information about the following:

> The input data the API processes, including both compulsory and optional parameters. The types of requests the API accepts, including supported HTTP methods and media formats. Rate limits and authentication mechanisms.