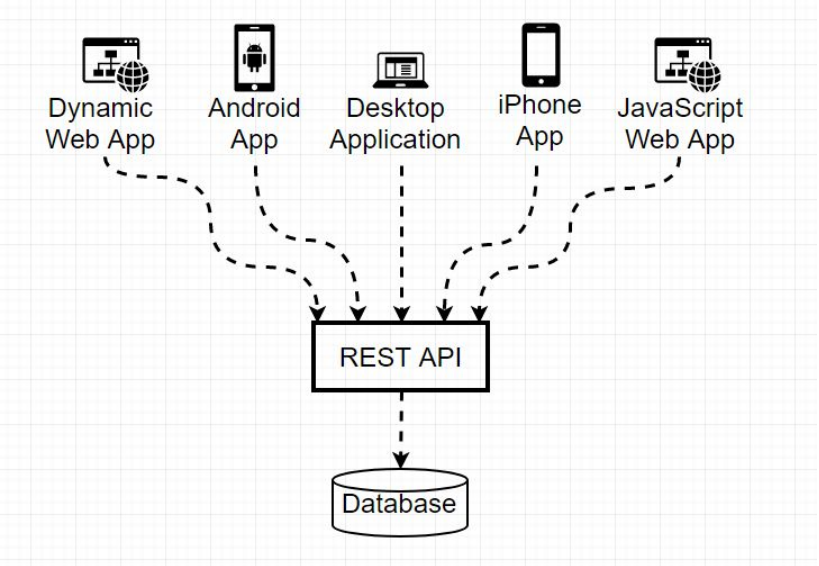
API. Authentication. Authorization

APIs - Application Programming Interface

- Giúp các hệ thống không liên quan tới nhau vẫn có thể giao tiếp được với nhau
- Đồng bộ dữ liệu giữa các nền tảng

  - REST API - API theo **nguyên lý** REST - representational state transfer
  - SOAP API - API theo **giao thức** SOAP - Simple Object Access Protocol



SOAP vs REST

SOAP	REST
SOAP dựa hoàn toàn vào XML để cung cấp các services truyền tin.	Dùng HTTP Method + Url để truyền tin
Sử dụng được nhiều protocols HTTP, SMTP	Chỉ sử dụng HTTP
Phức tạp	Đơn giản, gọn gàng, dễ tiếp cận
Tích hợp xử lý lỗi	

Authentication - Xác thực

- Authentication là về việc xác thực thông tin đăng nhập của bạn như Tên người dùng / ID người dùng và mật khẩu để xác minh danh tính của bạn.
- Single-Factor Authentication
- Two-Factor Authentication
- Multi-Factor Authentication

Authentication - Authorization

- **Authentication** là về việc xác thực thông tin đăng nhập của bạn như Tên người dùng / ID người dùng và mật khẩu để xác minh danh tính của bạn.
- Single-Factor Authentication
- Two-Factor Authentication
- Multi-Factor Authentication

- **Authorization** Xảy ra sau khi hệ thống được Authentication thành công. xác định quyền của bạn với các tài nguyên trong hệ thống.

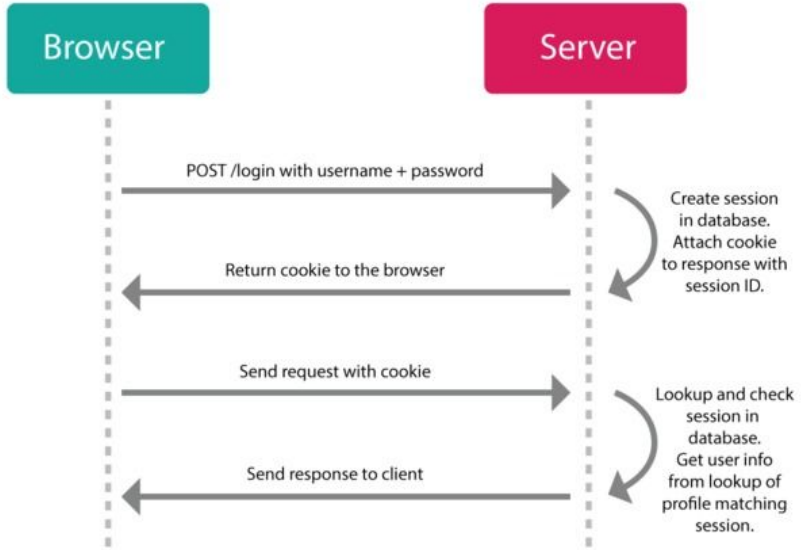
RESTful API Authentication

- **Cookied Base**
- Basic Authentication
- HMAC
- ***OAuth 2.0***

https://blog.restcase.com/restful-api-authentication-basics/

Session - Cookies

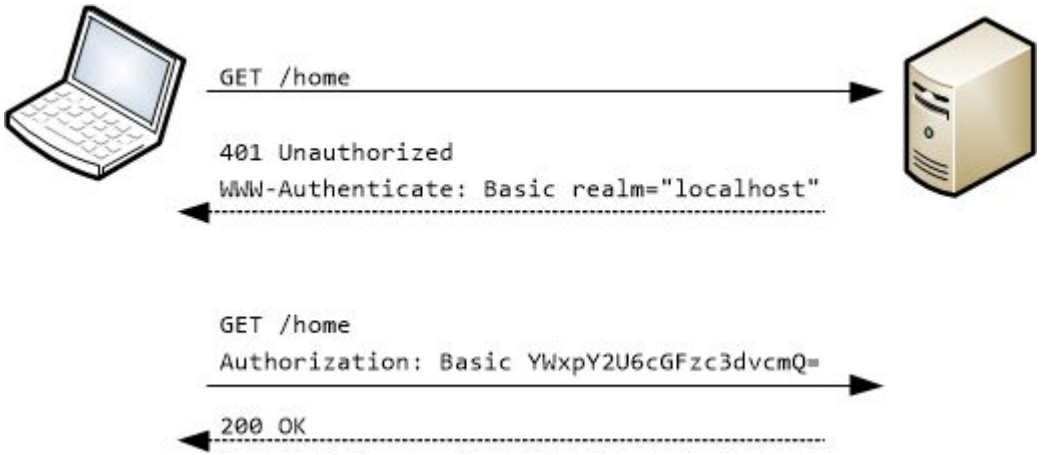
Cookie	Session
Cookie được lưu trữ trên trình duyệt của người dùng.	Dữ liệu **session** được lưu trữ ở phía server.
Dữ liệu **cookie** được lưu trữ ở phía client.	Dữ liệu **session** không dễ dàng sửa đổi vì chúng được lưu trữ ở phía máy chủ.
Dữ liệu cookie dễ dàng sửa đổi hoặc đánh cắp khi chúng được lưu trữ ở phía client.	Sau khi đóng trình duyệt sẽ hết phiên làm việc (session)
Dữ liệu **cookie** có sẵn trong trình duyệt đến khi expired.	



Basic Authentication

The most simple way to deal with authentication is to use HTTP basic authentication. We use a special HTTP header where we add 'username:password' encoded in base64.

```
GET / HTTP/1.1
Host: example.org
Authorization: Basic Zm9vOmJhcg==
```



https://blog.restcase.com/restful-api-authentication-basics/

OAuth 2.0

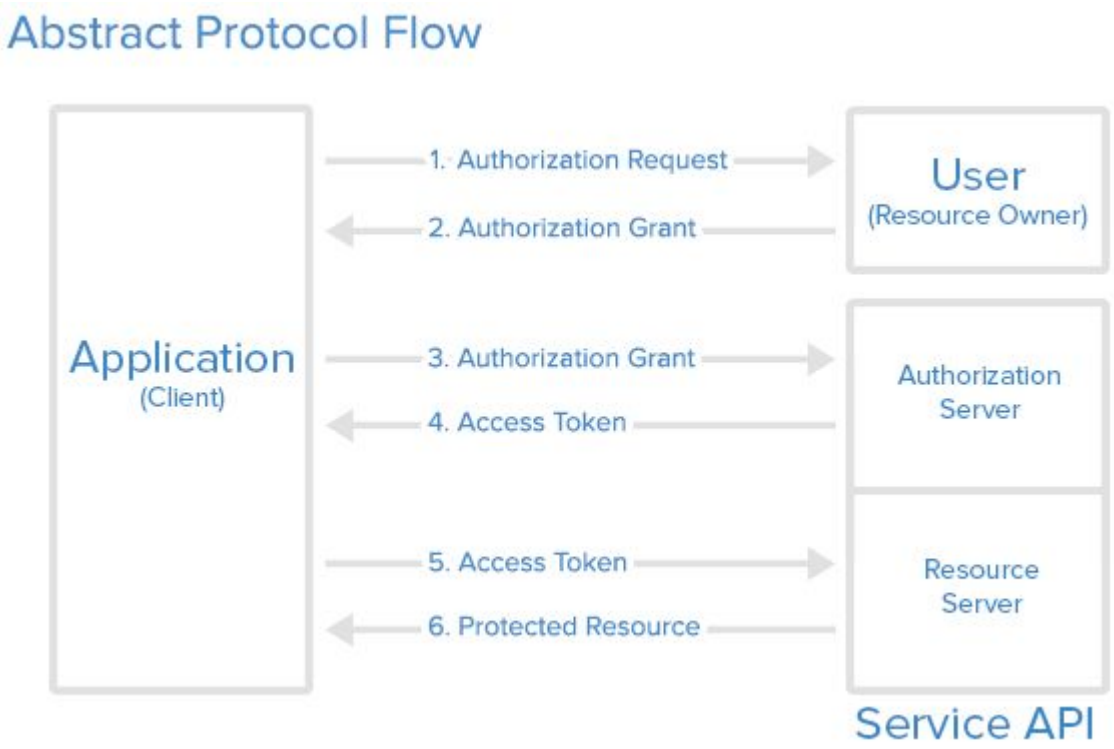
OAuth là một *phương thức chứng thực* giúp các ứng dụng có thể chia sẻ tài nguyên với nhau mà không cần chia sẻ thông tin **username** và **password**.

Resource Owner (User)

Client (Application)

Resource Server (API)

Authorization Server (API)



HMAC

Hash based Message Authentication. Instead of having passwords that need to be sent over, we actually send a hashed version of the password, together with more information. Let's assume we have the following credentials: username "username", password "secret".

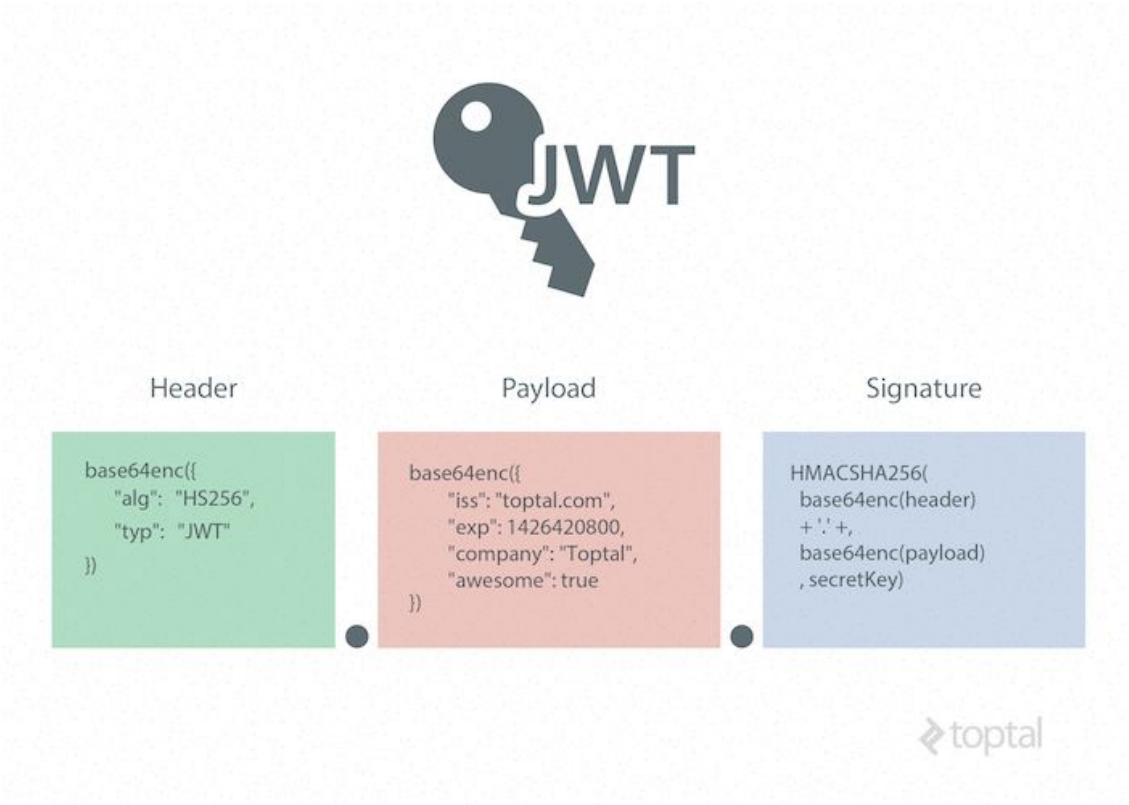
```
digest = base64encode(hmac("sha256", "secret",      "GET+/users/username/account"))
```

```
GET /users/username/account HTTP/1.1
Host: example.org
Authentication: hmac username:[digest]
```

JWT - JSON Web token

JWT là một phương tiện đại diện cho các yêu cầu chuyển giao giữa hai bên Client – Server , các thông tin trong chuỗi **JWT** được định dạng bằng JSON . Trong đó chuỗi Token phải có 3 phần là header , phần payload và phần signature được ngăn bằng dấu “.”

Authentication: Đây là trường hợp phổ biến nhất thường sử dụng JWT. Khi người dùng đã đăng nhập vào hệ thống thì những request tiếp theo từ phía người dùng sẽ chứa thêm mã JWT.



Bài tập