[**https://stackoverflow.com/questions/71179660/spring-boot-3-jakarta-and-javax**](https://stackoverflow.com/questions/71179660/spring-boot-3-jakarta-and-javax)

**Từ Spring Boot ver 3.x trở đi, sẽ dùng thư viện jakarta của Jakarta EE 9 thay vì javax. Và sẽ dùng Java 17.**

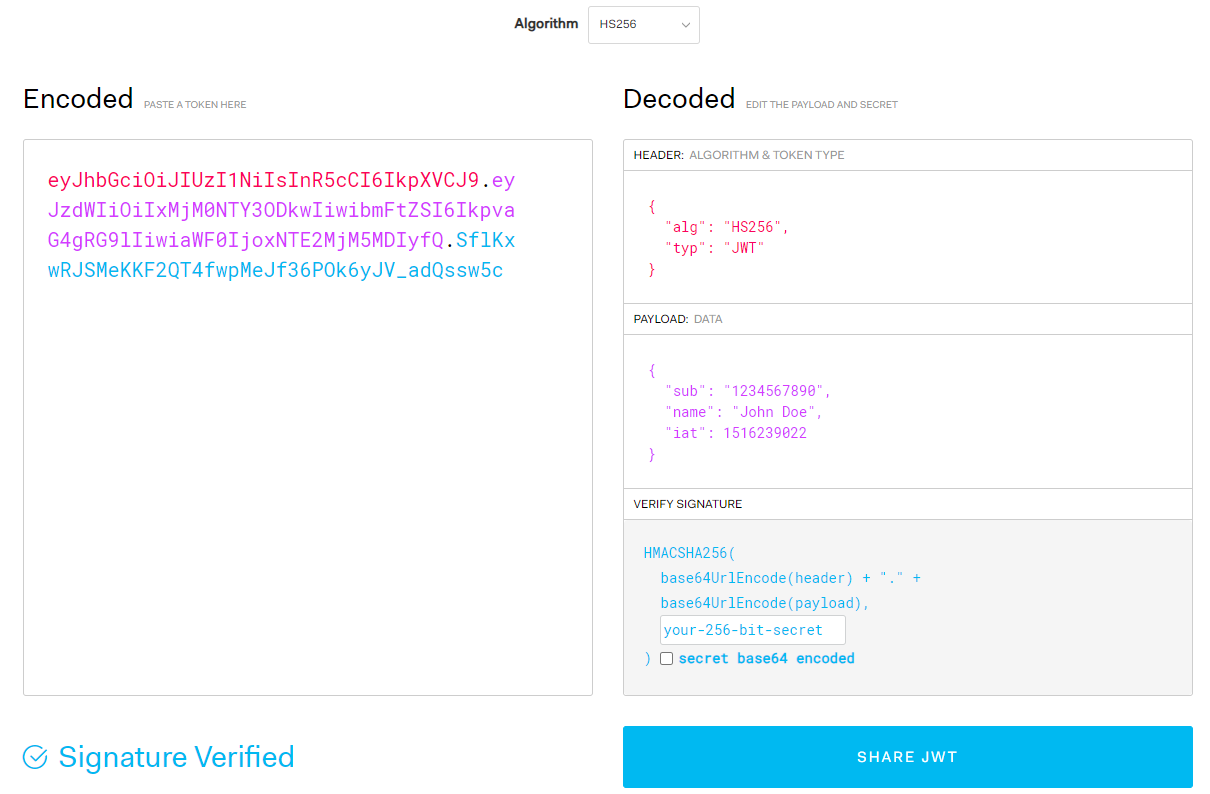
**-> khi import các thư viện vẫn xài thư viện của javax, thì down parent version của Spring Boot xuống ver 2.x.**

**Hoặc đơn giản hơn là cứ vào luôn solution copy file pom.xml cho nhanh.**

1. **Authentication? Authorization**
2. **Encoding? Encrypting? Hashing? Salting?**
   * **Encoding** đơn giảnlà mã hoá 1 input chuỗi kí tự thành một output bằng một thuật thoán. Output này có thể dễ dàng dịch ngược lại được bằng cách sử dụng lại chính thuật toán đã encode trước đó.
   * **Encrypting** nôm na giống như encoding, nhưng chúng sẽ đi kèm theo secret key. Khi encrypt 1 input thì sẽ đi kèm theo một secret key để cho ra output, muốn dịch ngược lại output thì ta chỉ cần thuật toán ban đầu kèm theo secret key là được
   * **Hashing** là mã hoá 1 chuỗi kí tự nhưng không thể dịch ngược lại được (hoặc rất rất khó có thể dịch ngược lại vì bản chất thuận toán hash là hash đi hash lại nhiều lần output đó sau mỗi lần hash rồi mới ra output cuối cùng)
     + Thuật toán hashing ko hoàn hảo, chúng vẫn có tỉ lệ hash ra 2 output giống nhau từ 2 input ban đầu khác nhau. Việc hash 2 input ban đầu khác nhau ra output giống nhau đó gọi là đụng độ giá trị băm (**collision)**
     + Điều này sẽ sinh ra vấn đề khi 2 user có password giống nhau sẽ hash ra cùng output giống nhau. Điều này là nên tránh vì khi ta lưu password trên hệ thống, mọi hashing value nên là unique (hashing value rất khó có thể dịch ngược lại nhưng ko có nghĩa là ko thể). **Salt** sinh ra để khắc phục vấn đề này.
   * **Salting** là hành động thêm 1 chuỗi kí tự bất kì vào cuối password trước khi hashing. Với việc ta định nghĩa trước mỗi user sẽ có một **salt** riêng biệt, ta sẽ đảm bảo rằng password của từng user nếu kết hợp với salt sẽ luôn hash ra output ko trùng nhau. Việc này sẽ làm tăng độ phức tạp của hashing value nên rất nhiều lần và việc dịch ngược lại gần như là ko thể.
3. **Basic auth? Session-based auth? Token-based auth?**
   * <https://kipalog.com/posts/Authentication-story-part-2--Authentication-co-ban>
   * **Basic** **auth** 
     + là cơ chế authen cổ điển nhất, đơn giản là gửi username và password kèm theo mỗi lần gửi request.
     + Dấu hiệu nhận biết là ở những website cũ, khi truy cập lần đầu sẽ hiện lên dialog của browser yêu cầu nhập username và password.
     + Cơ chế: Sau khi đã nhập username và password và xác thực thành công thì browser sẽ lưu lại username và pasword này và sẽ tự động gửi kèm nó trong phần header (**Authorization**) cho mỗi lần gửi request sau. Server mỗi lần nhận request thì sẽ kiểm tra lại username và password trong database.
     + Nhược điểm: Điều này có nghĩa là trong mỗi request đó sẽ luôn bao gồm thông tin của username và password

=> Lỗi thời, kém bảo mật và ko thể logout vì việc username và password được lưu là do trình duyệt làm và server ko thể can thiệp được, muốn logout chỉ có cách là xoá lịch sử duyệt web hoặc đợi thời gian lưu của browser này kết thúc.

* + **Session-base auth**
    - là cơ chế đăng nhập người dùng dựa trên việc tạo ra session của người dùng ở phía server. Sau quá trình xác thực người dùng thành công (username/password,...) thì phía server sẽ tạo và lưu ra một session chứa thông tin của người dùng đang đăng nhập và trả lại cho client session ID ngẫu nhiên để truy cập session cho những request sau.
    - Cơ chế: Sau khi đã nhập username và password và xác thực thành công thì server sẽ tạo ra SessionID và lưu lại trên server, sau đó gửi SessionID này về phía client. Mỗi lần user gửi request sẽ kèm theo SessionID này trong phần header (**Cookie**). Server mỗi lần nhận request thì sẽ so sánh SessionID này và SessionID do server đã tạo ra trước đó.
    - Ưu điểm:
      * vì SessionID do server gửi về là 1 chuỗi ngẫu nhiên, ko bao gồm thông tin gì nên quá trình truyển tải dữ liệu sẽ giấu thông tin về username và password.
  + **Token-base auth**
    - là cơ chế đăng nhập người dùng dựa trên việc tạo ra **token** - một chuỗi ký tự mang thông tin xác định người dùng được server tạo ra và lưu ở client. Server sau đó có thể không lưu lại token này.
    - Cơ chế: Sau khi đã nhập username và password và xác thực thành công thì server sẽ tạo ra token bao gồm những thông tin cơ bản của user, encode nó, sau đó gửi token này về phía client. Mỗi lần user gửi request sẽ kèm theo token này trong phần header (thường là **Authorization**). Server mỗi lần nhận request thì sẽ decode token này và sẽ có thông tin cơ bản của user.
    - Token này bản chất đã được verify khi tạo ra rồi vậy nên chúng sẽ ko cần kèm theo thông tin password nữa. Và server cũng ko cần lưu lại chúng.
    - Token này đã được encode cùng với secret key. Và chúng sẽ ko thể dịch ngược lại được nếu như ko biết secret key, và secret key này chỉ có server biết => chỉ server mới biết được trong token này chứa thông tin gì.

1. **JWT**
   * <https://viblo.asia/p/jwt-va-ung-dung-cua-no-vyDZOMRk5wj>
   * <https://viblo.asia/p/jwt-tu-co-ban-den-chi-tiet-LzD5dXwe5jY>
   * ****
   * <base64-encoded header>.<base64-encoded payload>.<HMACSHA256(base64-encoded signature)>
   * 
     + **Header:** bao gồm thuật toán encode chuỗi JWT này, và loại token (ở đây là JWT)
     + **Payload:** chứa các claims, chứa thông tin của user và vài thông tin về token như issue at,…
     + **Signature:** bao gồm header và payload đã được encode theo kiểu base64, secret key, và thuật toán encode được chỉ định trong header => nếu thay đổi payload thì signature cũng sẽ thay đổi theo.
   * Payload trong JWT thường ko bao gồm password (và cũng ko cần thiết) vì bản chất JWT được tạo ra từ việc encoding và decoding, ta hoàn toàn có thể đọc được nội dung bên trong nếu như biết được thuật toán encoding và chuỗi secret key.
2. **Testing**
   * **JUnit**
   * **Selenium**
3. **Mockito**
   * **Mockito** là một framework cho phép ta tạo các đối tượng giả (mock object) để có thể tập trung vào việc test những thứ khác bằng cách bỏ qua việc khởi tạo các object (nếu object đó có nhiều sự phụ thuộc khác). Bằng cách này ta có thể giả lập hành vi của các object đó.
     + **@Mock/mock():** dùng để tạo một mock object **hoàn toàn giả** -> những method được gọi từ object này sẽ ko thực hiện code gì trong method cả nếu chúng ta ko giả hành vi của chúng.
     + **when()/given():** dùng để định nghĩa hành vi của object đó, có arg là một method cụ thể.
     + **thenReturn():** để giả hành vi rằng method đó sẽ return về value gì.
     + **thenThrow():** để giả hành vi rằng method đó sẽ throw exception gì.
     + **@Spy/spy():** dùng để tạo một object **thật** nhưng ta vẫn có thể giả hành vi của chúng -> những method được gọi từ object này sẽ thực sự thực hiện code bên trong các method đó.
     + **@InjectMock:**
   * Mockito ko thể mock method private. Mockito ngầm định rằng method private ko tồn tại trong viewpoint của việc test.
   * .