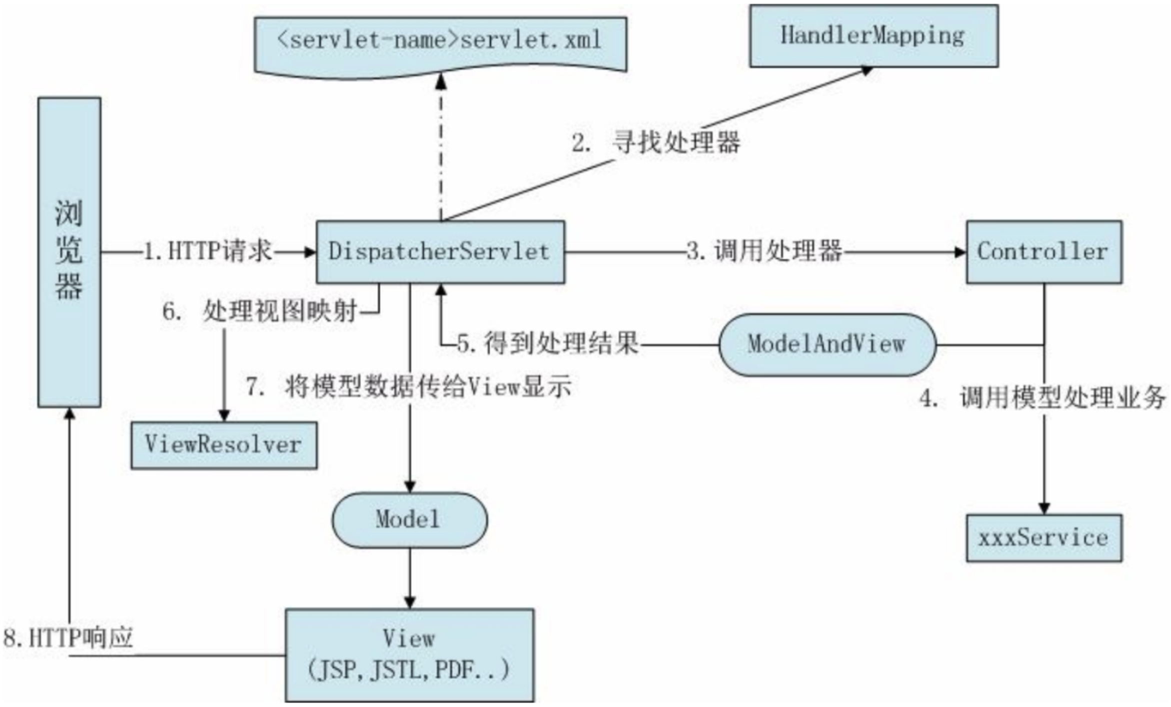
Spring - Mar 4



what is the difference between authentication and authorization?

Simply put, authentication is the process of verifying who someone is, whereas authorization is the process of verifying what specific applications, files, and data a user has access to.

What is Spring Security?

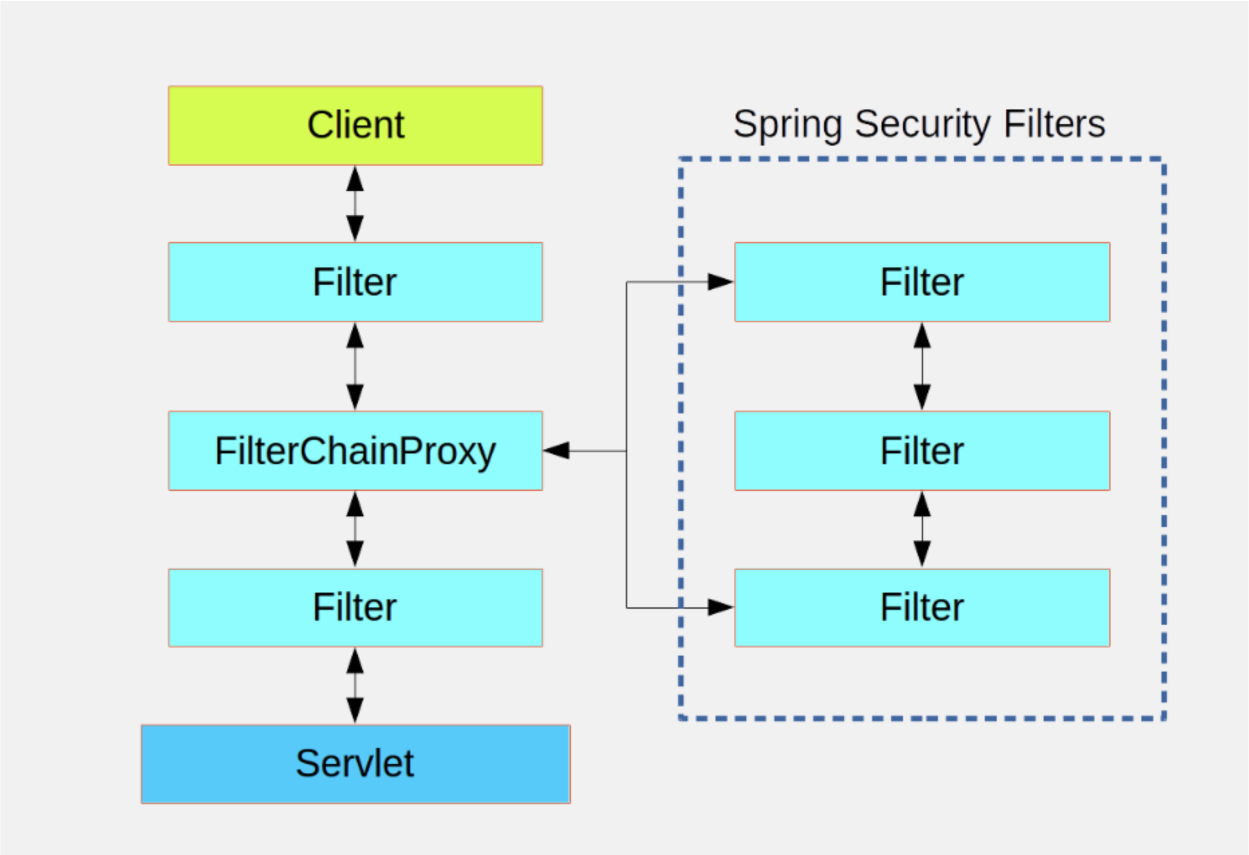
Spring Security provides security services for Java EE-based enterprise software applications. There is a particular emphasis on Spring based applications.

Authentication

- The process of checking credentials and making sure the current logged user is who they claim to be.

Authorization

- The process of deciding whether a current logged user is allowed to perform an action within your application.



Session-Based Authentication

How it works

1. A user enters their login credentials (username + password).
2. The server verifies the credentials are correct and creates a session which is then stored in a database.
3. The client-side stores the session ID returned from the server.

4. On subsequent requests, the session ID is verified against the database and if valid the request is processed.
5. Once a user logs out of the app, the session is destroyed on the server-side.

Token-Based Authentication

How it works

1. A user enters their login credentials (=username + password).
2. The server verifies the credentials are correct and creates an encrypted and signed token with a private key ({ username: “abcd”, exp: “2021/1/1/10:00” }, private key => token).
3. The client-side stores the token returned from the server.
4. On subsequent requests, the token is decoded with the same private key and if valid the request is processed.
5. Once a user logs out, the token is destroyed client-side, no interaction with the server is necessary.

Advantages of Token-Based Authentication

Stateless, Scalable and Decoupled

- Stateless: The back-end does not need to keep a record of tokens.
- Self-contained, containing all the data required to check its validity. No DB lookup is needed.

Mobile Friendly

- Native mobile platforms and cookies do not mix well. With a session-based approach, you simply store the session ID in a cookie.

Disadvantages of Token-Based Authentication

- The size of a token is usually larger than a session id.