Spring Security avec JWT (Json Web Token)

Spring Security avec JWT

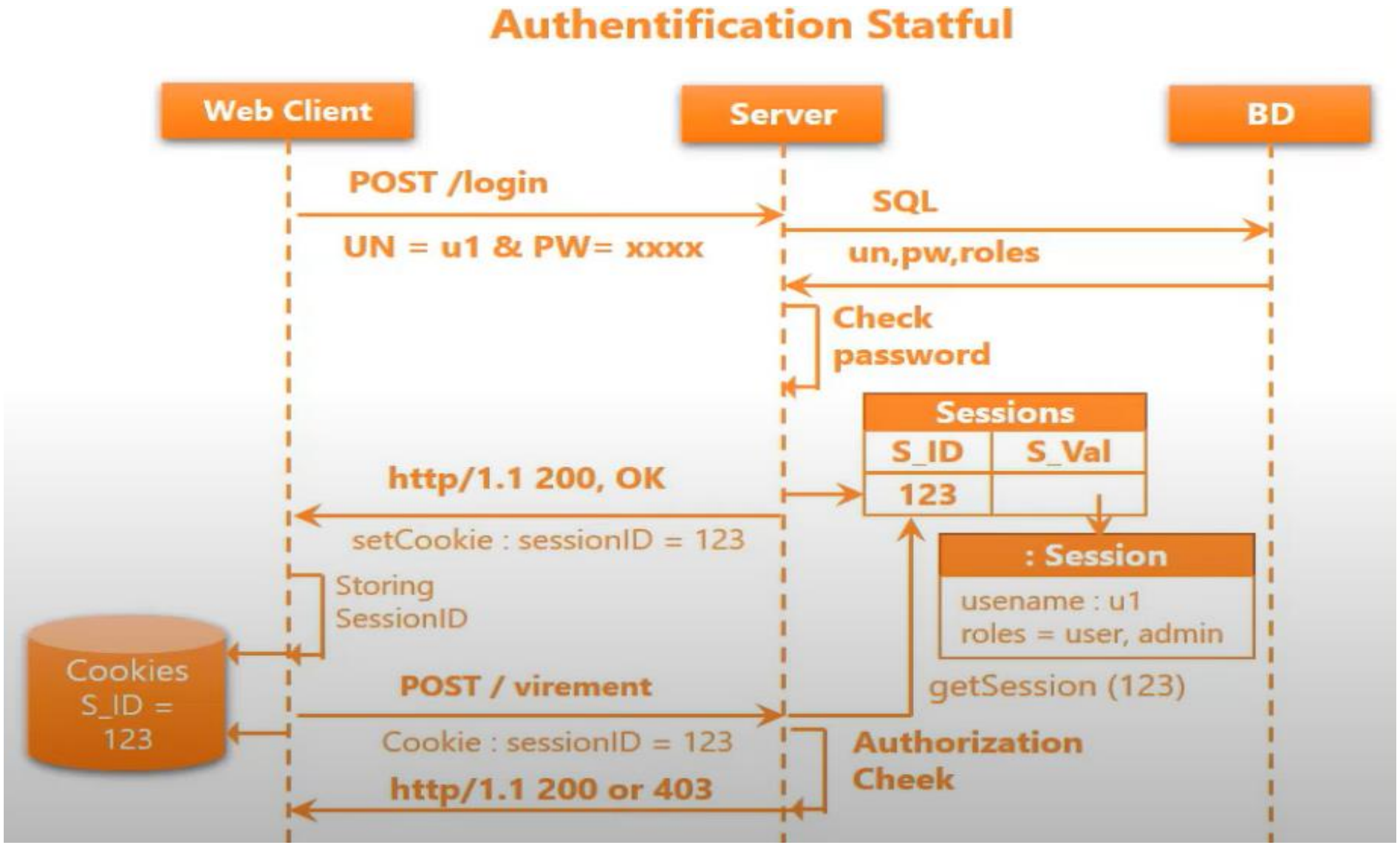
❖ Systèmes d'authentification:

➢ Deux types de modèles d'authentification:

- **Statful:** Les données de la session sont enregistrés coté serveur d'authentification.
- **Statles:** les données de la session sont enregistrés dans un jeton d'authentification délivré au client.

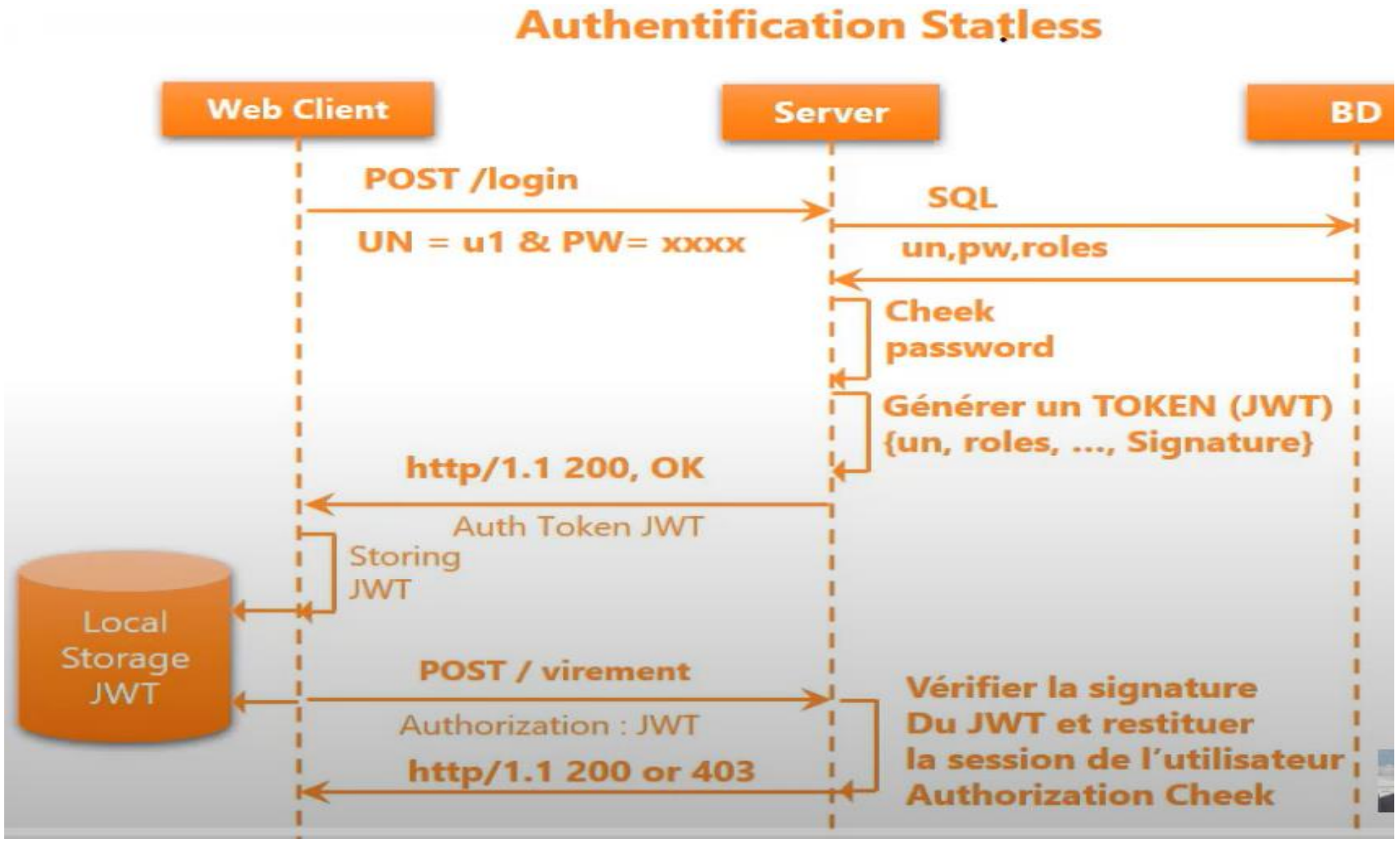
Systèmes d'authentification:

Statful:



Systèmes d'authentification:

Statles:

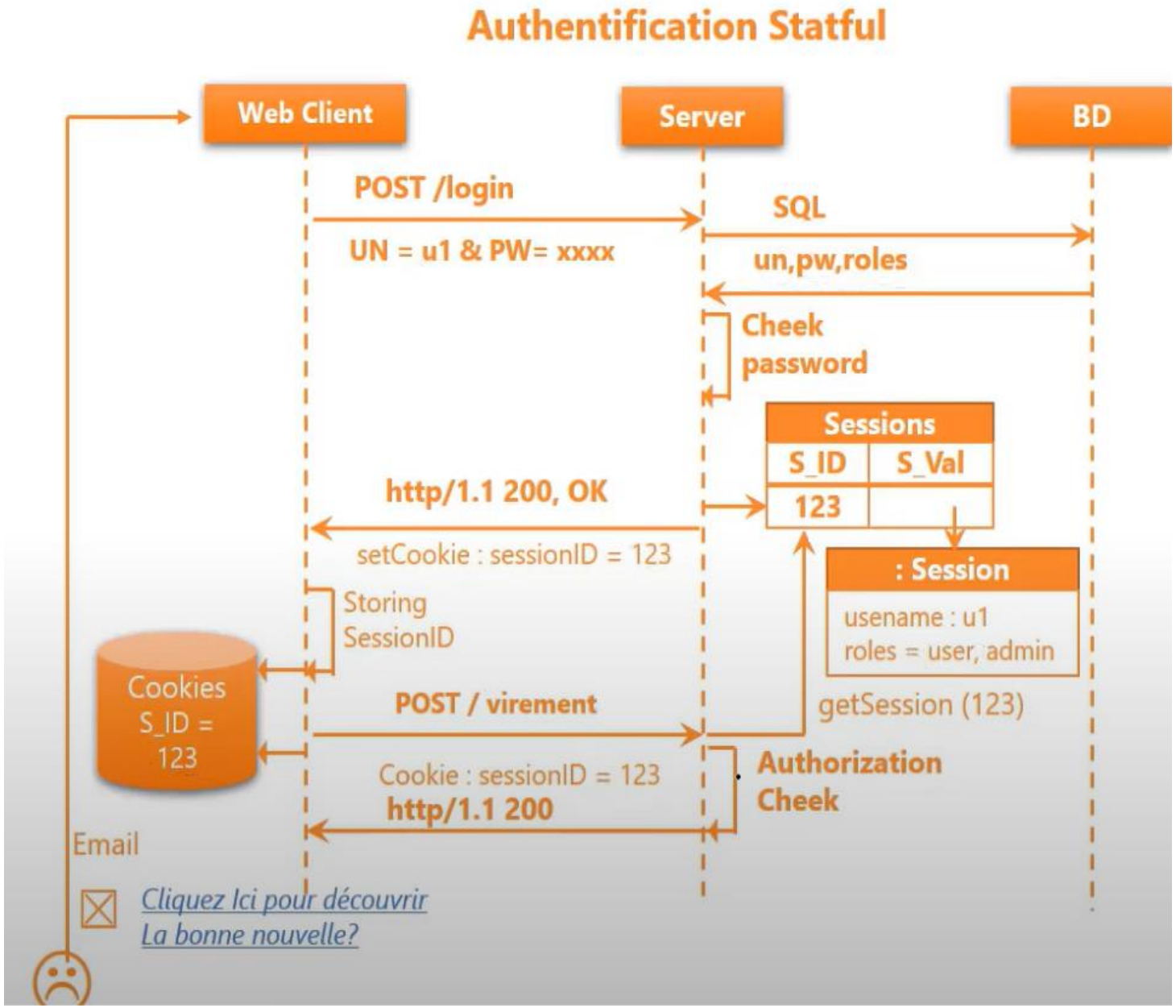


Systèmes d'authentification:

Statful:

Cross Site Request Forgery (CSRF):

- Une requête http falsifiée qui pointe sur une action interne au site.
- Afin qu'il l'exécute sans en avoir conscience et en utilisant ses propres droits.

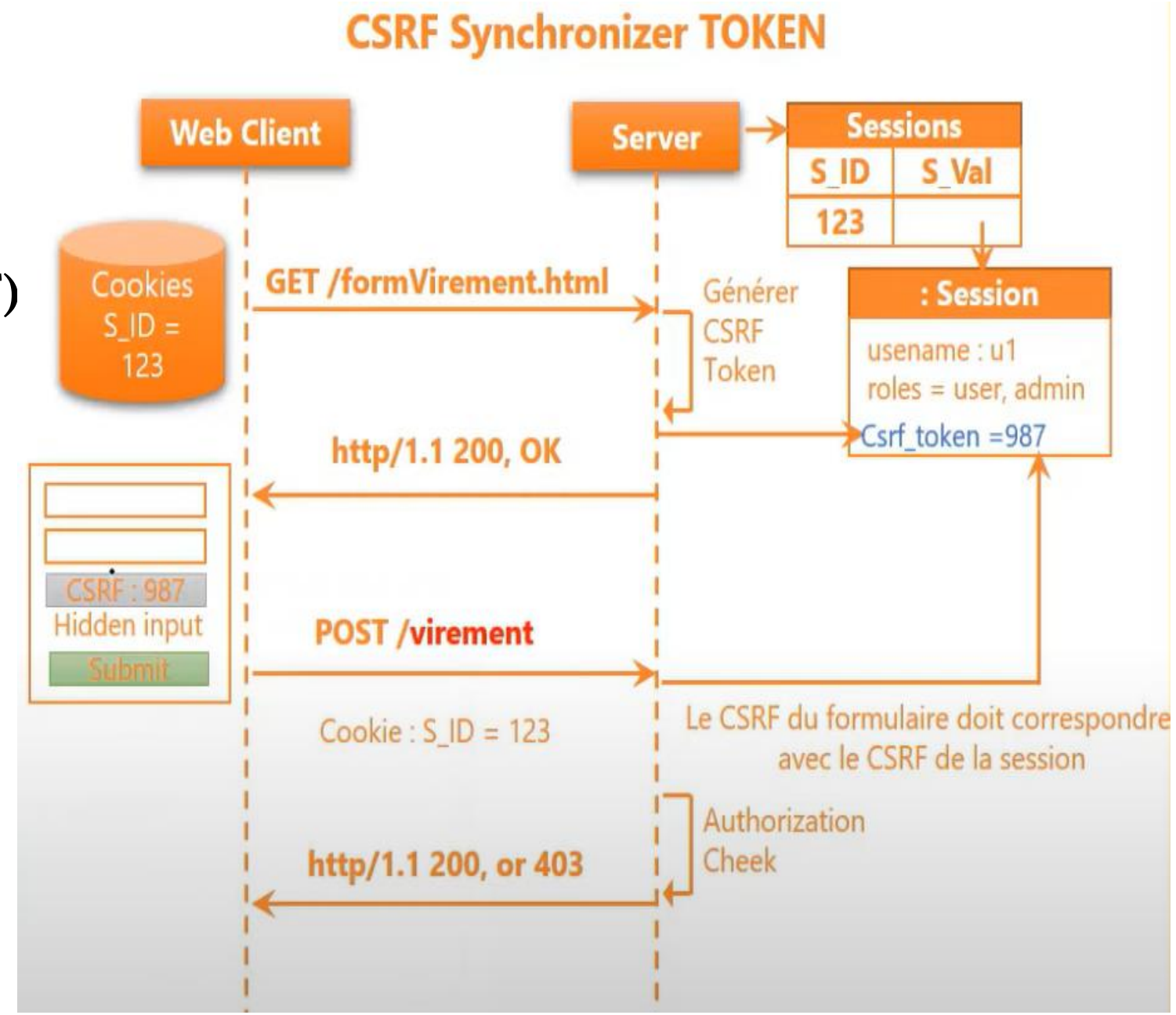


Systèmes d'authentification:

Statful:

Prévention contre les attaques(CSRF)

- Utiliser des jetons de validation **(CSRF Synchronizer Token)** dans les formulaires



Systèmes d'authentification:

JSON Web Token (JWT) : est un standard (RFC 7519) qui définit une solution **compacte** et **autonome** pour transmettre de manière sécurisée des informations entre des applications en tant qu'objet structuré au format JSON.

Compact : Dans la représentation compacte, le JWT est représenté par une chaîne de caractères contenant trois parties séparées par des points. Cette représentation permet d'économiser de l'espace et de faciliter la transmission du JWT, notamment dans les en-têtes HTTP.

Autonome : Un JWT est dit autonome car il contient toutes les informations nécessaires pour être vérifié par le destinataire sans avoir besoin de recourir à des sources externes. La signature du JWT garantit que les informations du payload n'ont pas été modifiées et provient d'une source fiable.

➔ JWT **fiable** car il est **signé numériquement**.

➢ JWT compose de trois parties:

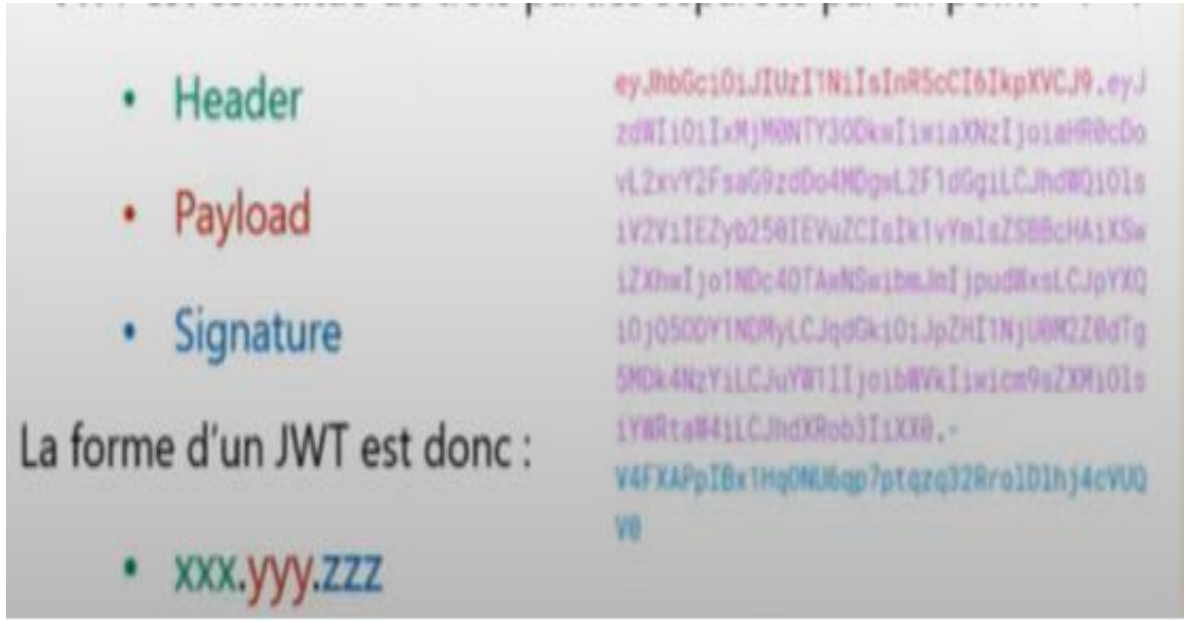
- **Header :** Il s'agit de l'en-tête du JWT qui contient les informations sur l'algorithme utilisé pour la signature et le type de JWT.

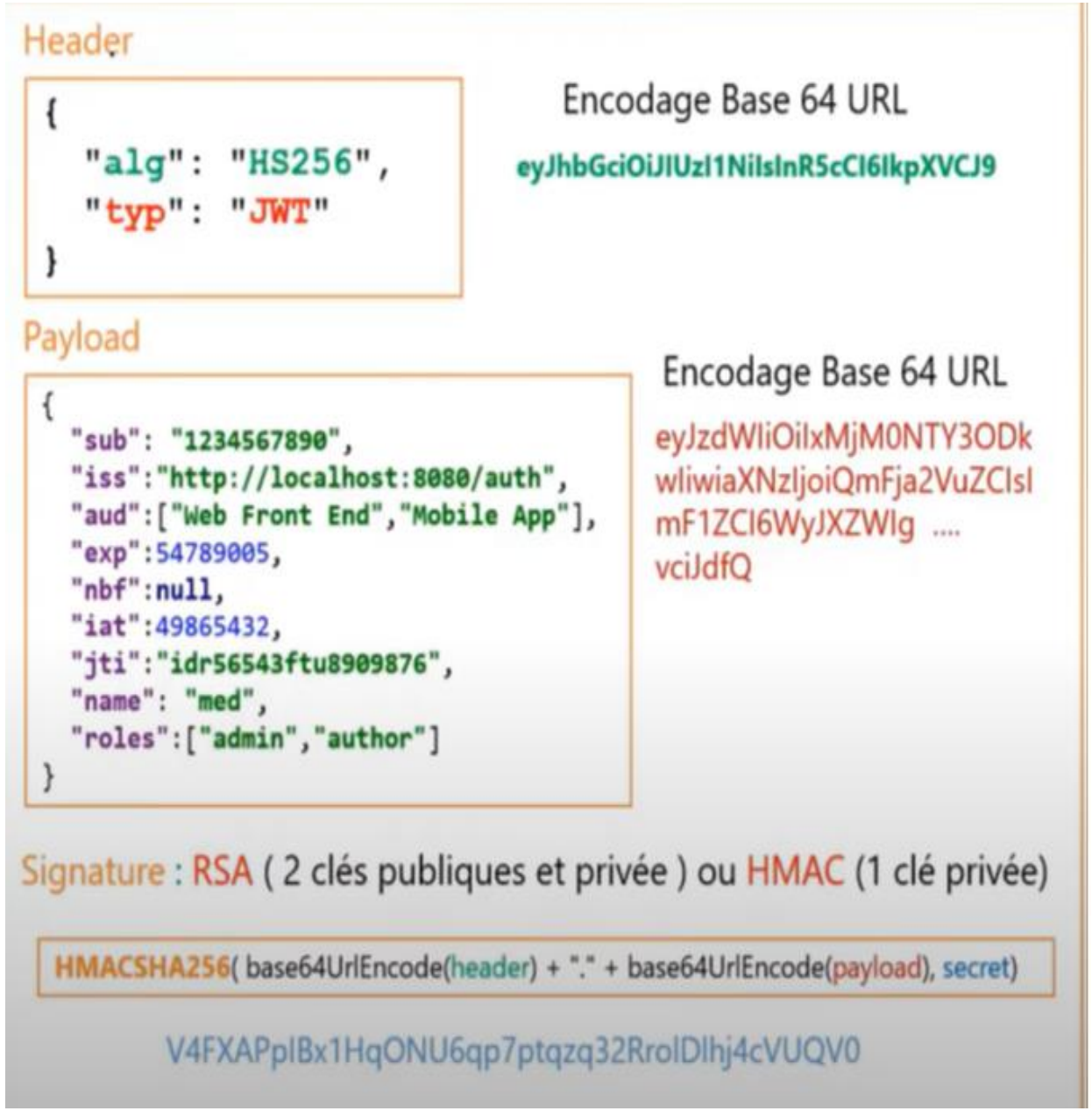
Systèmes d'authentification:

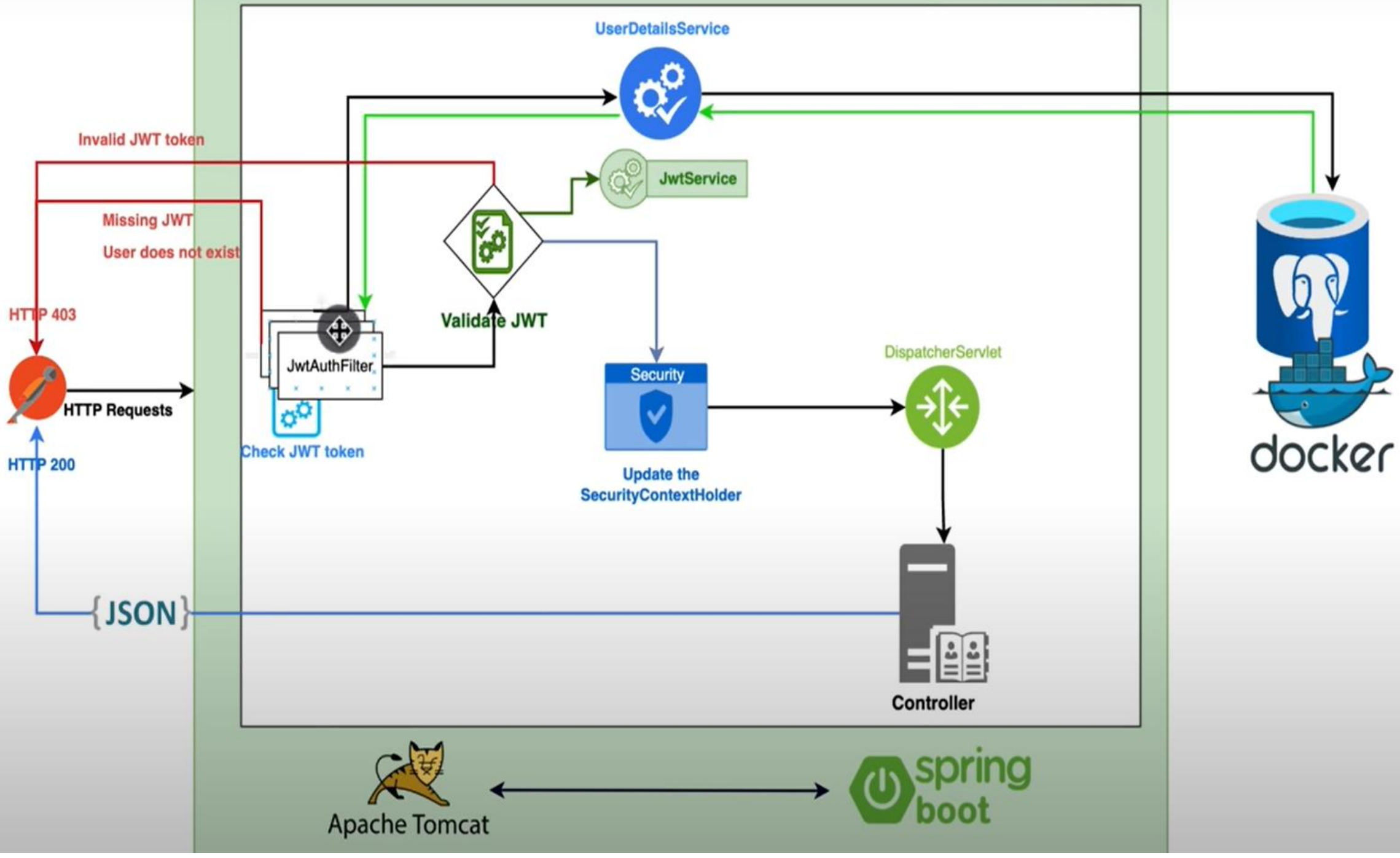
- **Payload :** Le payload contient les revendications ou les informations du JWT.

Il peut inclure des informations sur l'émetteur, l'audience, l'expiration, etc.

- **Signature :** La signature est générée en utilisant la clé secrète et la concaténation des en-têtes et des payloads du JWT. Elle sert à vérifier l'authenticité et l'intégrité du JWT






UserDetailsService
Invalid JWT token
JwtService
Missing JWT
User does not exist
HTTP 403
Validate JWT
JwtAuthFilter
Security
DispatcherServlet
HTTP Requests
Check JWT token
Update the
SecurityContextHolder
HTTP 200
{JSON}
Controller
Apache Tomcat
spring
boot
docker