Desarrollo Web Integrado

Sesión 9

Implementación de autenticación con JWT

Inicio

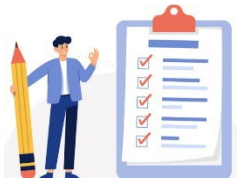
Universidad Tecnológica del Perú

Utilidad

Universidad Tecnológica del Perú

¿Qué vimos la sesión anterior?

- **Spring Security**
  - SecurityFilterChain
  - UserDetailsService
  - PasswordEncoder
  - *Caso de Estudio*: **Consulta RUC**

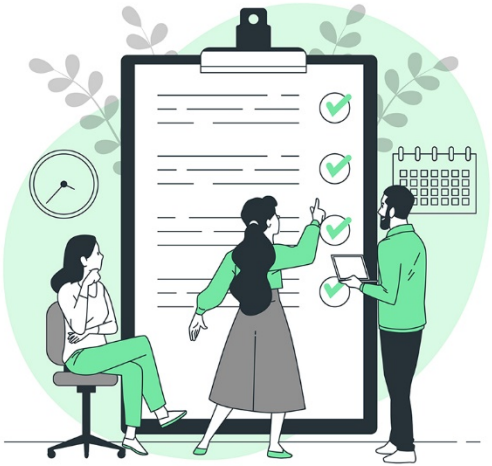


¿Preguntas?

Utilidad

Universidad Tecnológica del Perú

Saberes Previos

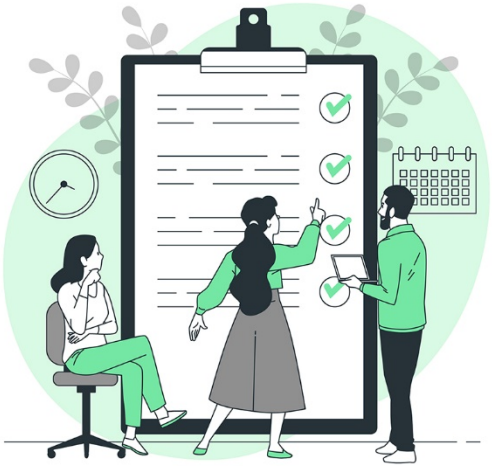


¿JWT?

Utilidad

Universidad Tecnológica del Perú

Saberes Previos

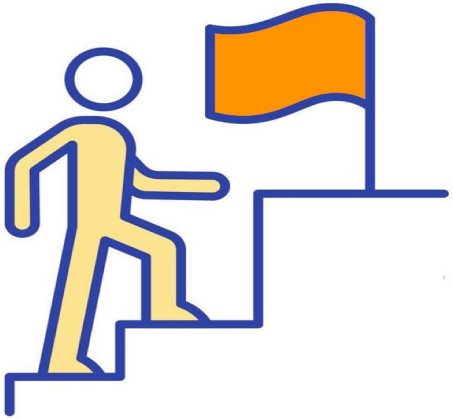


¿TOKEN?

Utilidad

Universidad Tecnológica del Perú

Logro de Aprendizaje



Al finalizar la sesión, el estudiante implementa una API REST segura usando JWT (JSON Web Token)

Universidad Tecnológica del Perú

Importancia

¿Cuál es la importancia de lo que veremos en la sesión de hoy tanto, para su vida académica como profesional?

Universidad Tecnológica del Perú

¿Qué vamos a ver en la sesión de hoy?

- **Implementación de autenticación con JWT**
  - Dependencias
  - Clave secreta
  - Servicio de JWT
  - Controlador de autenticación
  - Filtro JWT para proteger endpoints
  - Configuración de seguridad
  - Endpoint protegido
  - Prueba con Postman
  - *Caso de Estudio*: **Consulta RUC**

JWT

Universidad Tecnológica del Perú

Qué es

JWT

JSON Web Token

Es un formato **compacto y seguro** para transmitir información entre partes como un **token firmado digitalmente**, que se puede usar para **autenticación y autorización** en aplicaciones web

JWT

Universidad Tecnológica del Perú

Cómo luce un

JWT

JSON Web Token

Un JWT tiene tres partes codificadas en Base64:

HEADER.PAYLOAD.SIGNATURE

Ejemplo

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiJ1c3VhcmlvMSIsImlhdCI6MTY5NTY2NzYyMCwiZXhwIjoxNjk1NjcxMjIwfQ.
h0Oes_RuJXvRUtvN2fYHoDZWi0TyMMRWVmGiQUNZ2Fc

Universidad Tecnológica del Perú

Cómo decodificar un

JWT

JSON Web Token

HEADER.PAYLOAD.SIGNATURE

Ejemplo: TOKEN JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiJ1c3VhcmlvMSIsImlhdCI6MTY5NTY2NzYyMCwiZXhwIjoxNjk1NjcxMjIwfQ.
h0Oes_RuJXvRUtvN2fYHoDZWi0TyMMRWVmGiQUNZ2Fc

HEADER:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
PAYLOAD
eyJzdWIiOiJ1c3VhcmlvMSIsImlhdCI6MTY5NTY2NzYyMCwiZXhwIjoxNjk1NjcxMjIwfQ
SIGNATURE
h0Oes_RuJXvRUtvN2fYHoDZWi0TyMMRWVmGiQUNZ2Fc

Usar la herramienta disponible en:
https://www.base64decode.org/es/
Para cada parte del TOKEN, ingrese el parte superior la cadena Base64 y en la parte inferior visualice la expresión decodificada

Universidad Tecnológica del Perú

Partes de un JWT

JSON Web Token

HEADER

Define el algoritmo de firma y el tipo de token

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

"alg"

Algoritmo usado para firmar el token. En este caso, HS256 (HMAC con SHA-256).

"typ"

Tipo de token. En este caso, JWT (JSON Web Token).

Universidad Tecnológica del Perú

Partes de un JWT

JSON Web Token

HEADER

¿Qué es HS256?

HS256 = HMAC con SHA-256

algoritmo de firma simétrica muy usado para firmar JSON Web Tokens (JWT).

Usa una clave secreta compartida para firmar y verificar el token.
Es simétrico (misma clave para firmar y validar).

¿Qué significa "simétrica"?
Tanto la firma como la verificación del JWT se hacen usando la misma clave secreta compartida:
El emisor usa la clave para firmar el token.
El receptor usa esa misma clave para validar que el token no ha sido alterado.

Universidad Tecnológica del Perú

Partes de un JWT

JSON Web Token

HEADER

¿Qué es HS256?

HMAC → Hash-based Message Authentication Code:
Un mecanismo para verificar integridad y autenticidad de los datos usando un hash criptográfico (función matemática) más una clave secreta.

SHA-256 → Secure Hash Algorithm 256-bit:
Una función de hash que produce un digest de 256 bits (32 bytes).

JWT

Verificación JWT de la integridad y autenticidad

Supón que recibes este JWT: **header.payload.signature**

El servidor que lo recibe:

Recalcula la firma con el mismo algoritmo (HS256) y la clave secreta.
Compara su resultado con el signature del JWT.

Si coinciden:

- La integridad está garantizada: el contenido no fue alterado.
- La autenticidad está garantizada: el token fue generado con la clave secreta conocida (ej. por tu servidor de login).

Si NO coinciden:

- El token fue manipulado o no proviene de una fuente confiable → se rechaza.

Universidad Tecnológica del Perú

Partes de un JWT

JSON Web Token

PAYLOAD (contenido o "claims")

Contiene la información que quieres transmitir, como:

```
{
  "sub": "usuario1",
  "role": "admin",
  "iat": 1695667620, (fecha y hora de generación del token)
  "exp": 1695671220 (fecha y hora de expiración de token)
}
```

sub: sujeto (identificador del usuario)
iat: "issued at" (fecha de emisión)
exp: fecha de expiración
Puedes incluir claims personalizados como role, email, etc.

Puede acceder a https://www.cdmon.com/es/apps/conversor-timestamp para convertir fechas de tiempo UNIX a formato convencional

Universidad Tecnológica del Perú

Partes de un JWT

JSON Web Token

SIGNATURE

Es la firma digital generada usando un algoritmo como HS256 (HMAC con SHA-256) y una clave secreta:

```
HMACSHA256
(
  base64UrlEncode(header) + "." + base64UrlEncode(payload),
  secretKey
)
```

Sirve para verificar que el token no ha sido alterado y que fue generado por el emisor legítimo.

JWT

Universidad Tecnológica del Perú

Partes de un JWT

JSON Web Token

HEADER.PAYLOAD.SIGNATURE

+ CLAVE SECRETA

```
HMACSHA256
(
   base64UrlEncode(header) + "." + base64UrlEncode(payload),
   secretKey
)
```

JWT

Universidad Tecnológica del Perú

Para que se usa

JWT

JSON Web Token

Autenticación

El servidor emite un JWT después de que el usuario inicia sesión correctamente. Este token se guarda en el cliente (por ejemplo, en el localStorage o una cookie) y se envía con cada petición.

Autorización

Basado en los datos del JWT (como role: admin), el backend puede permitir o denegar el acceso a ciertos recursos.

Universidad Tecnológica del Perú

Ventajas de usar

JWT

JSON Web Token

Autocontenible:
Toda la información está en el token, no se necesita consultar una base de datos para verificar la sesión.

Stateless:
No se guarda sesión en el servidor.

Seguro:
Firmado digitalmente (puede ser con clave secreta o clave pública/privada).

Compacto:
Ideal para uso en HTTP headers.

Universidad Tecnológica del Perú

Consideraciones de Seguridad

JWT

JSON Web Token

- Nunca guardes información sensible en el payload (como contraseñas o tarjetas de crédito), porque aunque está firmado, no está cifrado.
- Usa HTTPS siempre.
- Implementa mecanismos para invalidar tokens (como listas negras o expiración corta).

Caso de Estudio: Consulta RUC

Universidad Tecnológica del Perú

Servicio de Consulta RUC

Práctica

Practiquemos

30 minutos

Intégrate a tu equipo de trabajo en la sesión de clase, e…

Implementa
Un Endpoint protegido con JWT
Para la consulta RUC

Terminado el tiempo, los equipos de trabajo regresan a la sala principal de la plataforma Zoom para compartir el trabajo realizado, a fin de recibir la retroalimentación respectiva que permita el logro del aprendizaje

Cierre

Universidad Tecnológica del Perú

¿Qué aprendiste hoy?

Participa por audio o chat | ✋ Levanta la mano para participar por audio


UTP
Universidad
Tecnológica
del Perú