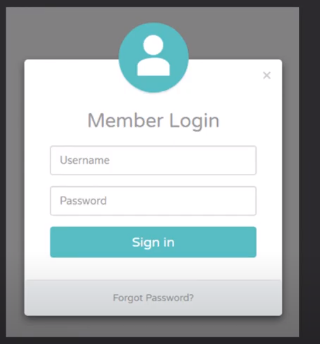
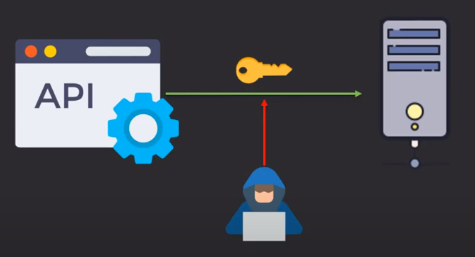
El metodo por autenticación por password ha sido el más utilizado, pero tambien más inseguro.



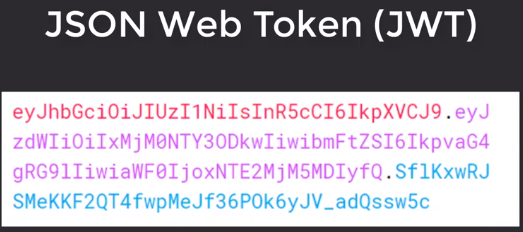
Cuando enviamos las credenciales para comunicarnos con el servidor, los datos de clave los enviamos como parte del request.

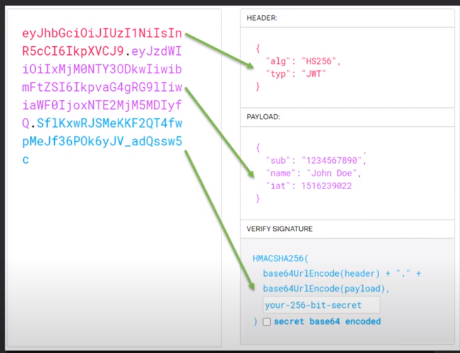


Si la red es publica puede ser cacheada por un tercero.

A pesar de una red segura, la información llega al servidor y esta puede replicarla a otro sitios que no tendrian esta seguridad.

Ejemplo de token fisico que utilizan algunos bancos.



HEADER metadatos del token, eje. El algoritmo con el cual fue firmado.

JSON que describe el token y como procesarlo. Esta parte es sensible porque no esta encriptada.

PAYLOAD

Carga util, cualquier información que queramos agregar al token.

JSON datos persona autenticada y valides del token. Poner la vigencia del token.

Esta parte es sensible porque no esta encriptada.

VERIFY SIGNATURE

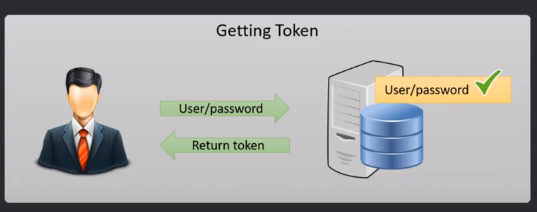
Sección de cifrado y verificación, esta suma las 2 anteriores secciones y gener un Hash, si movemos cualquier caracter de las 2 sesiones, el token no seria valido.

Cuando se firma un token lo que hacemos es generar las 2 primeras secciones y luego con esta 2 secciones generamos la 3 seccion que esta firmada mediante una llave privada, para luego enviar al cliente.

Cuando el cliente recibe el token, el lo almacena y cuando quiera consumir un servicio lo envia de regreseo.

Lo que debemos hacer es validar la tercera sección si fue generado de las 2 secciones anteriores y si fue firmado por la llave secreta. Si coincide se da como un token valido.

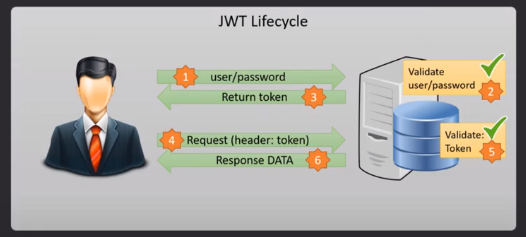
**1era forma lograr autenticación mediante token**



Con el logueo se genera el token, pero este no seguira enviando los datos luego si no el token generado

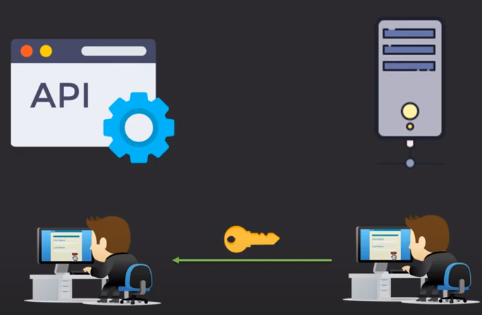
De acuerdo al tipo de usuario de logueo podremos dar unos permisos

El atacante podria obtener el token, pero no podria generar uno nuevo y los token caducan



Ciclo vida del token

**2da forma lograr autenticación mediante token**



Se utiliza cuando 2 aplicativos necesitamos que se comunican mediante un API.

Se deben porner en contacto los dos administradores de los sistemas por una via externa.

El administrador del servidor le envia un token por correo o metodo seguro al administrador del aplicativo que debe consumir el API.

Esta llave privada o token, se almacena y se configura en el aplicativo para que luego cuando el aplicativo tenga que consumir la API, simplemente envia el token.

Si el token llega a ser exponer o ser vulnerado, simplemente se invalida y se genera un nuevo token para enviar al administrador del otro sistema.

Ejemplo el uso de github que generamos token y cuando necesitamos subir cambios debemos enviar el token.