

Seguridad en el Desarrollo de Software

Práctica con JWT

1. Crear (forge) un JWT que contenga al menos los siguientes datos:
 - a. Nombre y Apellido.
 - b. Email.
 - c. Rol (cliente, analista o administrador)

HEADER: ALGORITHM & TOKEN TYPE	
<pre>{ "alg": "HS256", "typ": "JWT" }</pre>	
PAYLOAD: DATA	
<pre>{ "nombre": "Agustin", "apellido": "Alvarez", "email": "agus@mail.com", "role": "admin" }</pre>	
VERIFY SIGNATURE	
<pre>HMACSHA256(base64UrlEncode(header) + "." + base64UrlEncode(payload), aGpl6XC5a78.a-ñq23Te5) <input type="checkbox"/> secret base64 encoded</pre>	

JWT:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJub21icmUiOiJBZ3VzdGluIiwiaXBlbGxpZG8iOiJBbHZhcmV6IiwiaWZw1haWwiOiJhZ3VzQG1haWwuY29tIiwicm9sZSI6ImFkbWluIn0.EfY_klq4sVlX0CGwrh09q5b0Jzmr8wJTJ0CUEqXvyA

2. Dado el siguiente JWT:

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiaWwudmFtZSI6ImZkcmNicnRsIiwiaWF0IjoiMjAyMy0xMi0yNSAwMTQyMDUybmFtZSImV4cCI6MTY2MDA1MDIwMSwib3JpZ19pYXQiOjE2NjAwMTQyMDUybmFtZSImRvY2VudGUifQ.ZqVxn2A60Yrdrj6lRbvPfyCHj_Hh9yUJnBH8FUaXFQIBWUVbu0jK6UOPUK7jidC3

¿Con qué clave fue firmado?

- c0ntr4s3ñ4-
- s3gur1d4d
- cl4v3s3cr3t4 → fue firmado con esta clave
- _s3cr3t#

3. Dados los siguientes JWT:

a.

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjojLCJ1c2VybmFtZSI6ImZkcmNi
cnRsIiwiaWZlhaWwioiJmZlHjYnJ0bEBmcmMudXRuImVkdS5hciIsImV4cCI6MTY2MDA1MDIwMSwib
3JpZ19pYXQiojE2NjAwMTQyMDEsInJvbCI6ImRvY2VudGUifQ.xJgZ6rDB5l-
sQwYz59L QuBkDsDQ9PMIfqe6IThCO → **HS256**

b.

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsInR5cCI6IkpzZW50L3NpdjE6ImZpbmFtZSI6ImZkcmNi
cnRsIiwiaWZlhaWwOiJmZHJjYnJ0bEBmcmMudXRuLmVkdS5hciIsImV4cCI6MTY2MDA1MDIwMSwiP3JpZl9pYXQiojE2NjAwMTQyMDEsInJvbCI6ImRvY2VudGUifQ.ZqVxn2A60Yrdrj6lRbvPfychj_H
h9yUJnBH8FUaxFQIBWUVbu0jk6UOPUK7jidC3 → H2384

C.

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyX2lkIjoxLCJ1c2VybmFtZSI6ImZkcmNi
cnRsIiwiaWlhaWwiOiJmZlJhYnJ0bEbmcmMudXRuLmVkdS5hcnR5ImV4cCI6MTY2MDA1MDIwMSwi3JpZ1
9pYXQiOiJlE2NjAwMTQyMDEsInJvbCI6ImRvY2VudGUifQ.sEycTxakRDId6LKXAr6inGuA3RT
IdgpyfvsXV0zQs093ZEYxqFCYWcEX22i00HVG4AtUiLNBHyDqjyi0Y7k6Ba → **HS512**

¿Cuál está firmado por HS256?

Esta firmado en HS256 el JWT a.

4. ¿Cuáles de los siguientes son campos estándares que pueden ir en el body de un JWT?

1. **iss** → issuer (emisor)
2. **exp** → expiration time (fecha de expiración)
3. test
4. from
5. **iat** → issued at (fecha de emisión)
6. **sub** → subject (sujeto, quien envió el JWT)
7. src

5. Dado un token, ¿Cómo podemos identificar si se trata de un JWT?

Necesitamos decodificarlo, no podemos saber si es un JSON Web Token a simple vista. Existen sitios en internet que lo hacen por nosotros.