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)

JWT:


```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
Jub21icmUiOiJBZ3VzdGluIiwiYXBlbGxpZG8iO
iJBbHZhcmV6IiwiZW1haWwiOiJhZ3VzQG1haWwu
Y29tIiwicm9sZSI6ImFkbWluIn0.EfY_klq4sVl
X0CGwrh09q5bOJzmbr8wJTJ0CUEqXvyA
```

2. Dado el siguiente JWT:

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJ1c2VyX2lkIjoxLCJ1c2VybmFtZSI6ImZkcmNicnRsIiwiZW1haWwiOiJmZHJjYnJ0bEBmcmMudXRuLmVkdS5hciIsImV4cCI6MTY2MDA1MDIwMSwib3JpZ19pYXQiOjE2NjAwMTQyMDEsInJvbCI6ImRvY2VudGUifQ.ZqVxn2A60Yrdrj61RbvPfyCHj_Hh9yUJnBH8FUaXFQIBWUVbu0jK6UOPUK7jidC3

¿Con qué clave fue firmado?

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

3. Dados los siguientes JWT:

a.

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoxLCJ1c2VybmFtZSI6ImZkcmNicnRsIiwiZW1haWwiOiJmZHJjYnJ0bEBmcmMudXRuLmVkdS5hciIsImV4cCI6MTY2MDA1MDIwMSwib3JpZ19pYXQiOjE2NjAwMTQyMDEsInJvbCI6ImRvY2VudGUifQ.xJgZ6rDB5l-sQwYz59L_QuBkDsDQ9PMIfqe6IThCO → **HS256**

b.

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJ1c2VyX2lkIjoxLCJ1c2VybmFtZSI6ImZkcmNicnRsIiwiZW1haWwiOiJmZHJjYnJ0bEBmcmMudXRuLmVkdS5hciIsImV4cCI6MTY2MDA1MDIwMSwib3JpZ19pYXQiOjE2NjAwMTQyMDEsInJvbCI6ImRvY2VudGUifQ.ZqVxn2A60Yrdrj61RbvPfyCHj_Hh9yUJnBH8FUaXFQIBWUVbu0jK6UOPUK7jidC3 → **H2384**

c.

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJ1c2VyX2lkIjoxLCJ1c2VybmFtZSI6ImZkcmNicnRsIiwiZW1haWwiOiJmZHJjYnJ0bEBmcmMudXRuLmVkdS5hciIsImV4cCI6MTY2MDA1MDIwMSwiaWF0IjoxNjYwMDE0MjAxLCJyb2wiOiJkb2N1bWVudGUifQ.sEycTxakRDiD6LKXAr6inGuA3RTIdgpyfvsXV0zQs093ZEYxqFCYWcEX22i00HVG4AtUiLNBHyDgjyi0Y7k6Ba → **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.