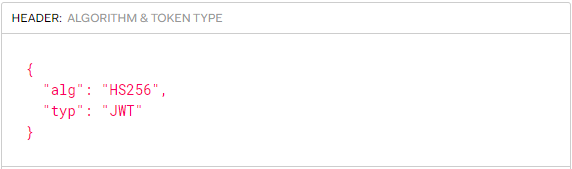
Seguridad en el Desarrollo de Software

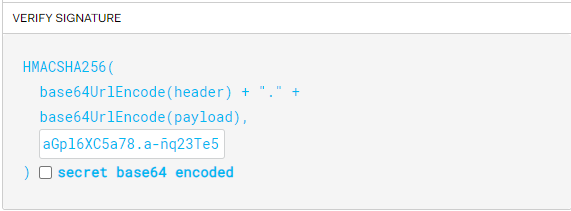
**Práctica con JWT**

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

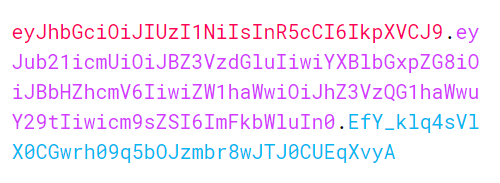


Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente



JWT:



1. Dado el siguiente JWT: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJ1c2VyX2lkIjoxLCJ1c2Vy bmFtZSI6ImZkcmNicnRsIiwiZW1haWwiOiJmZHJjYnJ0bEBmcmMudXRuLmVkd S5hciIsImV4cCI6MTY2MDA1MDIwMSwib3JpZ19pYXQiOjE2NjAwMTQyMDEsIn JvbCI6ImRvY2VudGUifQ.ZqVxn2A60Yrdrj61RbvPfyCHj\_Hh9yUJnBH8FUaX FQIBWUVbu0jK6UOPUK7jidC3

¿Con qué clave fue firmado?

* c0ntr4s3ñ4-
* s3gur1d4d
* cl4v3s3cr3t4 🡪 fue firmado con esta clave
* \_s3cr3t#

1. Dados los siguientes JWT:

a.

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoxLCJ1c2VybmFtZSI6ImZkcmNi cnRsIiwiZW1haWwiOiJmZHJjYnJ0bEBmcmMudXRuLmVkdS5hciIsImV4cCI6MTY2MDA1MDIwMSwib 3JpZ19pYXQiOjE2NjAwMTQyMDEsInJvbCI6ImRvY2VudGUifQ.xJgZ6rDB5l- sQwYz59L\_QuBkDsDQ9PMIfqe6IThCO 🡪 **HS256**

b.

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9**.**eyJ1c2VyX2lkIjoxLCJ1c2VybmFtZSI6ImZkcmNi cnRsIiwiZW1haWwiOiJmZHJjYnJ0bEBmcmMudXRuLmVkdS5hciIsImV4cCI6MTY2MDA1MDIwMSwib 3JpZ19pYXQiOjE2NjAwMTQyMDEsInJvbCI6ImRvY2VudGUifQ**.**ZqVxn2A60Yrdrj61RbvPfyCHj\_H h9yUJnBH8FUaXFQIBWUVbu0jK6UOPUK7jidC3 🡪 **H2384**

c.

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9**.**eyJ1c2VyX2lkIjoxLCJ1c2VybmFtZSI6ImZkcmNi cnRsIiwiZW1haWwiOiJmZHJjYnJ0bEBmcmMudXRuLmVkdS5hciIsImV4cCI6MTY2MDA1MDIwMSwi3JpZ19pYXQiOjE2NjAwMTQyMDEsInJvbCI6ImRvY2VudGUifQ**.**sEycTxakRDiD6LKXAr6inGuA3RT IdgpyfvsXV0zQs093ZEYxqFCYWcEX22i00HVG4AtUiLNBHyDgjyi0Y7k6Ba 🡪 **HS512**

**¿Cuál está firmado por HS256?**

Esta firmado en HS256 el JWT a.

1. ¿Cuáles de los siguientes son campos estándares que pueden ir en el body de un JWT?
2. iss 🡪 issuer (emisor)
3. exp 🡪 expiration time (fecha de expiración)
4. test
5. from
6. iat 🡪 issued at (fecha de emisión)
7. sub 🡪 subject (sujeto, quien envió el JWT)
8. src
9. 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.