1. What are the three parts of a JSON Web Token (JWT)?

2. If a JWT can be decoded by anyone, how are they useful? What problem do they solve and how do they solve it securely?

A JSON Web Token consists of a header, payload and signature. All of which are separated by dots, therefore a JWT typically looks like xxxxx.yyyyy.zzzzz. “The header typically consists of two parts, the type of token which is JWT and the signing algorithm being used, such as HMZC, SHA256 or RSA.” The next part is the payload which contains the claims. This is typically information about the user and additional data. There are three types which are registered claims, public claims and private claims. Then finally the JWT is finished with a signature, “to create that, it requires the encoded header, the encoded payload, a secret and the algorithm specified in the header and sign that.” The signature is used to verify the message wasn’t changed along the way and in the case of tokens signed with a private key, it can also verify that the sender of the JWT is who it says it is.

The signature solves the issue of being decoded by anyone and how it does it securely as well. JWTs can be either signed, encrypted or both. If a token is signed but not encrypted, everyone can read its contents but when you don’t know the private key, you can’t change the contents. If it is changed, then the receiver will notice the signature doesn’t match anymore. It works similarly with the message being encrypted, if you don’t know the “secret” and private key, you won’t be able to figure out the message that is being sent.

1 “https://jwt.io/introduction”