⇒ Many application use JWT to allow the client to indicate its identity for further exchange after authentication

⇒ JWT used to carry 1. information related to identity.
2. characteristic of a client.

→ verify signature :

⇒ [(Base64(Header)].[Base64(Payload)].[Base64(signature)]

⇒ Issues of JWT Tokens :

1. None Hashing algorithm.

↳ when an attacker alters the token and changes the hashing algorithm to indicate through the none keyword that the integrity of the token has already been verified.

has three main parts

jwt = header | payload | signature

↓ identifier which algorithm to use to generate signature

header { "alg" : "HS256", "type" : "jwt" }

2. Token SideJacking

↳ attack occurs when a token has been intercepted / stolen by an attacker and then they will use it to gain access to the system using targeted user identity.

3. No Built in Token Revocation by the user :

↳ inherent to JWT because a token only becomes invalid when it expires. User has no built-in feature to explicit revoke the validity of token

4. Token information Disclosure

↳ when an attacker has access to a token and extracts information stored in it.

5. Token Storage on client side

↳ when an application stores the token in a manner exhibiting the following behaviors.

1. cookie storage
2. local storage container
3. token accessible in case of XSS.

6. Weak token secret