Jeton JWT

Elément	Description
Compétences	Pouvoir mettre en œuvre des mécanismes d'authentification et d'autorisation.
Objectifs	A la fin de cette séquence, les apprentis seront capables • De décrire le contenu d'un jeton JWT. • D'expliquer deux types de jetons • D'expliquer les risques de sécurité posés par l'utilisation de jeton.
Durée estimée	15 min
Répertoire de travail	
Fichiers sources	
A produire	Répondre aux questions directement dans ce document

1. Contenu d'un jeton JWT

Citer les trois éléments qui constituent un token JWT. Décrivez l'utilité de chacun de ces éléments :

Un en-tête (header)

Une charge utile (payload)

Une signature numérique (Signature)

2. Type de jetons

Expliquer la différence entre un token HS256 et RS256. Que permet l'un et l'autre non ?

RS: asynchrone, utilise une clé publique et privée

HS: synchrone, utilise une seule clé

3. Perte de la clé secrète

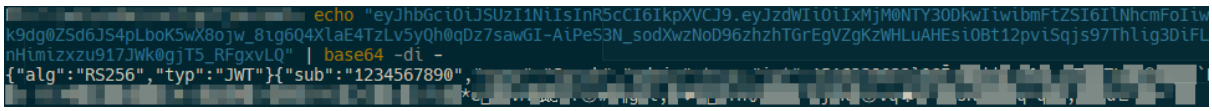
Comment est-ce qu'un attaquant pourrait exploiter une clé secrète ou une clé privée perdue ?

En se faisant passer par l'utilsateur

4. Vérification

Obtenir le contenu des jetons 1 et 2, à l'aide des ressources suivantes :

- base64 -di input > decoded



- https://github.com/ETML-INF/183-SecuriteApplication/supports/02-jwt-handbook-v0_14_2.pdf
- https://www.base64decode.org/
- https://jwt.io

Jeton 1 : jwt_User1.txt

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IlNhcmFoIiwiYWRtaW4iOnRydWUsImlhdCI6MTUxNjIzOTAyMn0.wQMSqPZusJCSgINwl_vOKtoN5UltUPAEyjiwzswd7AYEKW31GxeyGip-Ou28SYcxOJdGmMk3X-cmk9dg0ZSd6JS4pLboK5wX8ojw_8ig6Q4XlaE4TzLv5yQh0qDz7sawGI-AiPeS3N_sodXwzNoD96zhzhTGrEgVZgKzWHLuAHEsiOBt12pviSqjs97Thlig3DiFL9DWNtS5gEby8dWe5hK6qCKsc5jrTlTbEC-wKmUOtPxW_T-eXporyhZ_gEjuRRnh3Q7owO71JK3WWgM_namA7SLTavZrqAj1AXZ-xBaMiiYFzS936oOpxKnHimizxzu917JWk0gjT5_RFgxvLQ

Quelles informations avez-vous réussi à décoder :

algo: RS256, typ: jwt

"sub": "1234567890",
"name": "Sarah",
"admin": true,
"iat": 1516239022

Est-ce que la signature est valide ?

On peut pas le savoir sans la clé publique

Jeton 2 : jwt_User2.txt

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4iLCJtYWdhYWRtaW4iOnRydWUsImlhdCI6MTUxNjIzOTAyMn0.THoFMc49QqN-YeKPO_dKZcx1EnQtOIW_Yd5O3gHGqQDYl7sM0zwJAx1E-9OLpsseSn2nmgr9AVTWPlwtFsnbEmPNMPZu5DYSqBwzjYj0M81-t5w5k9gykraY6BQXOQtSHk23JttTJtGPOwgCXvj97giTKecmKvKzks364esXl-FZDH1nQSEsY7TgpnWLDVlh357Y4HaLMA-VDDQmah5bJhG0WyM8riPWYu4qsmJCbxgGV0btxTPCY3-5cMiKAnN2ty_cvZp_WNsKlYDx0VDVgFzglrgOSi4xRuo462wc4Vp2vnGV1dBZijxWxTOnKuYSnFdqq_2R_hiJdqtgipCRtg

Quelles informations avez-vous réussi à décoder :

"alg": "RS256",
"typ": "JWT"

"sub": "1234567890",
"name": "John",
"magaadmin": true,
"iat": 1516239022

Est-ce que la signature est valide ?

On peut pas savoir sans la clé publique

Que peut-on imaginer sur ce qu'il s'est passé avec ce jeton ?

Il s'est perdu