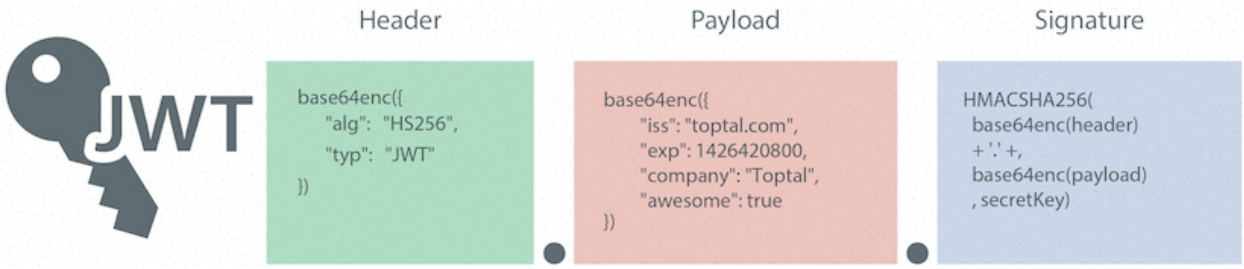
JWT

Commençons par étudier la structure d’un JWT.

https://www.youtube.com/watch?v=A2-YImhNVMU



On peut l'envoyer via l'entête Authorization (en HTTP).

```
Authorization: Bearer [TOKEN_JWT]
```

Il est également souvent utilisé sur un site web via un cookie, il est cependant recommandé d’utiliser IndexDB ou LocalStorage. Les cookies ont certes une notion d’expiration, contrairement à indexDB ou LocalStorage, cependant ils sont transmis à chaque requête HTTP.

Le développeur doit maitriser dans quel cas soumettre le JWT.

Révoquer un Jeton

C’est un des problème majeur des JWT, ont peut effectivement leur donner une “durée de vie” (expiration), cependant une fois cette durée de vie attribuée au jeton, il “n’est plus possible” de rejeter le jeton.

Il faudra gérer la révocation de jeton via une base de donnée de jetons révoqués si besoin

Failles JWT

Swapping d’algo

Un token JWT peut également utiliser un algorithme `none` qui n’est donc ni chiffré ni signé.
Si l’implémentation du type d’algorythme permet le Swapping (changement d’algo), cela est problématique, car le pirate pourrait changer l’algo en `none` et omettre la signature.

Le vol de clé privée

Si la clé est stockée dans un fichier, et que le pirate trouve une faille de sécurité lui permettant de lire les fichiers sur le serveur. Les failles permettant de lire le contenu de fichier sur le serveur sont multiple, LFI, RFI, Injection de commande, injection SQL (en fonction de la configuration), SSRF, ...
Après avoir volé la clé le pirate peut forger des signatures.

Cassage de clé privée

Si une clé est trop faible, un pirate peut tenter de la bruteforcer, c’est à dire à essayer diverses clé jusqu’à obtenir la bonne.

Après avoir obtenu la clé le pirate peut forger des signatures.

Comment craquer la clef secrète d'un JWT

En utilisant hashcat déjà installé sur Kali Linux

```
hashcat -a0 -m 16500 "LA_CLEF_JWT_A_CRAQUER" /usr/share/wordlists/rockyou.txt
```

Une fois craqué, on peut facilement recréer notre JWT avec un payload différent sur https://jwt.io/ avec la clé secrète.