

[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/>