**Dans nos sites habituels (PHP, ASP.NET), comment est-ce qu’on gère l’inscription, l’authentification et l’autorisation?**

* Habituellement, on match le mot de passe et nom d’utilisateur avec ce qu’y se trouve dans la base de données.

**De quelle façon ces opérations diffèrent-elles pour un site utilisant le paradigme Frontend/Backend?**

* Habituellement un site envoie le nom d’utilisateur et le mot de passe au serveur, qui le vérifie sécuritairement avec HTTPS et en encryptant les données

**Pour une API où on a aucune authentification, quels seraient les principaux vecteurs d’attaque ou d’abus?**

* La base de données, et les routes Delete ou Edit

**Pourquoi est-il une mauvaise idée d’envoyer les informations de connexion à chaque demande faite auprès de l’API?**

* Il est plus facile pour un attaqueur d’intercepter l’envoi si on envoie plusieurs fois les informations

**Regardez sur le site relié** [**ICI**](https://www.jwt.io/) **pour voir comment un jeton JWT est encodé. Quelles informations sont véhiculées dans le jeton?**

* L’encodage, les données à envoyer, et la signature.

**Mettez-vous du point de vue d’un acteur malveillant. Vous avez réussi à intercepter le jeton d’accès d’un utilisateur. Quelles opérations pouvez-vous accomplir en son nom? Comment les systèmes de jeton de sécurité résolvent-ils ce problème?**

* Un acteur malveillant peut utiliser le jeton d’accès d’un utilisateur pour se faire passer pour celui-ci en faisant des requêtes API avec le jeton, sans besoin de se connecter. Un jeton de sécurité empêche cela puisqu’il change à des intervalles réguliers, rendant le jeton d’accès inutilisable.

**À la lumière de ce que vous comprenez des jetons de sécurité, comment pensez-vous qu’un service de connexion comme « Login with Facebook » permet-il de fournir de façon sécuritaire une méthode de connexion universelle à des sites variés, qui n’appartiennent peut-être même pas à l’écosystème Facebook?**

* Un service comme celui-ci parvient probablement à fournir une connexion sécuritaire en générant un jeton sécuritaire et en laissant le travail d’encryptions à un tiers reconnu et fiables pour la sécurité