Cahier des charges mybank.io

Avant de commencer le projet

- Le projet est à réaliser par groupe de 1 ou 2
- La première étape du projet est de créer un *fork* du dépot GitHub https://github.com/lp1dev/Mybank_WebSec_Exercise **en PRIVÉ** ainsi que d'ajouter les droits en écriture à l'utilisateur *github.com/lp1dev*
- Le rendu devra se faire sous forme de projet **fonctionnel** pouvant être lancé à l'aide d'un `docker-compose up` à la racine de votre dépot

---

Liste des tâches à réaliser

- Audit des vulnérabilités de l'applicatif (manuel / automatisé)
- Reporting des vulnérabilités de l'application (cf. section vulnérabilités de ce document)
- Fix des soucis de sécurité via des regles NGINX (lorsque possible)

Vulnérabilités

Remplacez ici cette section d'exemple par les vulnérabilités que vous avez remarquées sur l'applicatif fourni.

Exemple

Vulnérabilité	**Injection SQL**
Description	Le paramètre GET post_id de l'URL https://website.com/blog est utilisé par le back-end sans vérification de la presence de caractères pouvant causer une injection SQL.
Criticité	Critique
Exploitation	https://website.com/blog?id=1 UNION SELECT * FROM users
Remédiation	Ajouter une règle dans le pare-feu pour bloquer les requêtes contenant le mot clé UNION