**Audit Sécurité Time Manager**

**Are they injectable (XSS, Script, HTML) ?**

* Pas d’injection possible (filtre de tous les envois dans les inputs)

**Are they vulnerable to sql injections, nosql ?**

* Pas d’injection possible (filtre de tous les envois dans les inputs)

**Are there accessible configuration files ?**

* Non pas de fichiers de configurations accessibles

**Are password hashes difficult to break ?**

* Password hashé avec Argon 2

**Are routes accessible by unauthorized users ?**

* Toutes les routes et requêtes sont protégées avec un token

**Are endpoints accessible by unauthorized users ?**

* Toutes les routes et requêtes sont protégées avec un token

**Is it possible to fill the database and cause a denial of service when rendering the page ?**

* Nous ne savons pas exactement mais nous pensons que les attaques par déni de service sont possibles.
* Les solutions sont que la prévention se doit de se porter sur le renforcement des machines virtuels et non sur les serveurs. Pour cela déployer plusieurs instances de notre service serai une bonne solution.

**Are JWT tokens http-only ? If not, how to recover these tokens ?**

* Non, les tokens sont stockés en session.

**Are the passwords sent in clear? If so how do you recover them ?**

* Les passwords sont envoyés du front -> back uniquement et sont hachés avec Argon2. Notre token ne stock pas le mot de passe.

**Is the application available only in https? if not, how could a malicious user intercept a client’s requests to your server ?**

* Non l’application est disponible en http.
* Nous devons utiliser un email et un mot de passe lors de la connexion, en http tout est encodé en base 64, il est beaucoup plus facile de décoder les données. Types d’attaques par écoute.
* Attaque par rejeu, le but étant d’écouter plusieurs fois les échanges entre client et serveur afin d’obtenir les informations confidentielles.