Bilan sécurité

Voici un bilan regroupant les mesures de sécurité et les test d'intrusion qui ont été réalisés dans le but de sécuriser la plateforme.

Serveur web

- Restriction des privilèges utilisateur
- Mise en place d'AppArmor (logiciel de restriction des accès)
- Mise en place de Fail2Ban (logiciel de prévention d'intrusion)
- Désactivation des connexions SSH en tant que Root
- Modification du port de connexion SSH
- Fermeture des ports non utilisés
- Utilisation de mots de passe forts
- Analyse Nessus (résultats négatifs)

Site web

- Analyse ZAProxy (résultats positifs, révélés faussés)
- Tentatives d'injection SQL (résultats négatifs)

Les analyses menées avec les outils Nessus et ZAProxy ont été réalisées sur une même version du site web hébergée sur un Nas Synology.

Les mesures mises en place contribuent de manière complémentaire à la sécurité de la plateforme. Les modifications apportées au serveur réduisent considérablement le risque de compromission, les champs sur le site web sont quant à eux invulnérables à de l’injection SQL.
Ces éléments ne réduisent pas à 0 le risque d’attaque mais garantissent une sécurité envers la plupart des attaquants, les résultats sont déjà observables sur les logs du serveur où l’on observe que depuis les modifications les tentatives de brute force sont quasiment inexistantes.