| Projet M1 – Compte-rendu de Réunion<br>« Développement d'une messagerie instantanée sécurisée » | Réunion 1<br>15/12/2022<br>(Semaine 50) |
|---|---|

| Présents :<br>o LANGLAIS Sébastien<br>o CHATEL Emilio<br>o LEFEVRE Edgar | Objet : Bilan des attentes pour le projet |
|---|---|

## I) Objectifs du projet

- Relecture de la présentation du déroulement global du projet.
- Visualisation des premiers schémas du site à créer.
- Explication des différentes fonctionnalités de base du site *(fonction backdoor, envoie de messages entre 2 personnes, page d'authentification, ajout d'autres utilisateurs, obligation de s'inscrire pour envoyer un message et/ou être ajouté).*
- Précision sur différents points du site *(site responsive sur téléphone et ordinateur sous Chrome et Safari, utilisation PHP et MariaDB côté serveur, bouton verrouillage et déverrouillage pour passer de http à https, enregistrements des messages des utilisateurs).*
- Explication du mode de fonctionnement des 2 versions du site : en mode sécurisé il n'y a aucune failles actives et en mode non-sécurisé c'est à nous de choisir les failles qui restent actives.

## II) Les différentes failles à mettre en œuvre

- Cross-site scripting (XSS) :
  - Injection et exécution de code JavaScript au travers du chat.
- Injections SQL :
  - Injection SQL lors de l'authentification *(soit sans mdp et pseudo soit sans le mdp mais avec un pseudo d'utilisateur déjà enregistré).*
  - Injection SQL lors de l'ajout d'un nouvel utilisateur.
  - Injection SQL dans le chat si on peut enregistrer les messages pour réussir à atteindre la base de données.
- Injection de fichier :
  - Injecter n'importe quel type de fichier pour exécuter du code.
- Backdoor :
  - Utilisation des fonctionnalités backdoor par des utilisateurs qui ne sont pas censé connaître ces fonctions.
- Attaque DDOS avec des images :
  - Envoi de nombreuses images pour ralentir le disque dur du destinataire.
- Algorithme de hachage faible (MD5) :
  - Mot de passe de la base de données hachés en MD5 et donc facile à décrypter.
- Cross-site request forgery (XSRF) :
  - Forcer l'utilisateur à exécuter une fonctionnalité du site pour qu'il à se déconnecte par exemple.
- Directory browsing :
  - Récupération de fichiers php.bak ou autres fichiers sensibles.

## III) Objectifs première semaine

- Commencer à réfléchir aux différentes options pour réaliser le site web.
- Chercher des fonctionnalités supplémentaires pour le site ou des failles en plus.
- Se documenter sur les différentes attaques/failles à réaliser.
- Etablir une chronologie et un déroulement des étapes du projet

Date de la prochaine réunion : Jeudi 12 janvier 2023 à 11h