Décrire le système, identifier ses actifs

**Objectifs**: fournir le moyen de communication interne à une Enterprise (messagerie web)

**Exigences** : uniquement les personnes autorisées ont accès, information complète et correcte

**Constitué de** : utilisateurs, base de donné, serveur local

**DFD :**

Notre système est assez simple : en tant que acteurs nous avons des administrateurs, des users standards et utilisateurs non authentifiés (le reste du monde). Il est évident que leur niveau de confiance n ’est pas le même.

**Analyse de menace :**

**Script-kiddies :**

Motivation : s’amuser

Cible : n’importe que élément

Potentialité : haute

**Cybercrime (spam, maliciels)**

Motivation : accès aux éléments interdits qui pourrons être utilisées plus tard

Cible : vol de credentials et/ou modification d’information

Potentialité : moyenne

**Concurrent :**

Motivation : vol d’information confidentiels, re utilisation du même contenu

Cible : serveur local

Potentialité : moyenne

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Component | S | T | R | I | D | E |
| External agent | ˅ |  | ˅ |  |  |  |
| Data store | ˅ | ˅ | ˅ | ˅ | ˅ | ˅ |
| Process |  | ˅ | ˅ | ˅ | ˅ |  |
| Data flow |  | ˅ |  | ˅ | ˅ |  |

S : Spoofing 🡪 connexion à l’application avec les informations volées. Mesures : transfert de données sécurisé.

T : Tampering 🡪 falsification de URL pour avoir les accès non autorisés. Mesures : accès contrôlé

R : Repudiation 🡪 modification de l’adresse de livraison d’une entreprise. Mesures : demande de l’information supplémentaire

I : information disclore 🡪 interception de trafic (wifi public). Mesures : chiffrer le trafic

D : Denial of service 🡪 allouer la mémoire de session en fonction des valeurs saisies par utilisateurs. Mesures : valider la taille avant l’allocation

E : Elevation of privileges🡪 copier/coller l’URL d’admin et y avoir accès. Mesures : mécanisme d’autorisation

**Scenario d’attaque 1** : User non authentifié essaie de se connecter à l’application

**Business impact** : élevé (image de l’entreprise, cout de remédiation)

M**otivation** : challenge, curiosité, accès aux données privés

**Scenario d’attaque** : injection du code

**Contrôle** : utilisation de requête de BD, validation des entrées de fichier.

**Scenario d’attaque 2** : Vol de base de donné

**Business impact** : élevé ou moyen (réputation, pertes d’actifs)

**Motivation :** financière

**Scenario d’attaque** : injection de code, bypass autorisation

**Contrôle :** validation des entrées de fichier, défense en profondeur, chiffrement de données

**Scenario d’attaque 3** : bruteforce de login et/ou mot de passe

**Business impact** : moyen (réputation, pertes d’information)

**Motivation :** avoir accès aux données privés

**Scenario d’attaque :** bruteforce

**Contrôle :** captcha, mot de passe fort

**Scenario d’attaque 4** : user accède aux messages d’un autre user (attaque horizontale)

**Business impact** : faible (réputation, pertes de confidentialité)

**Motivation :** avoir accès aux données privés

**Scenario d’attaque :** modification d’ID personnelle

**Contrôle :** prepared statement

**Scenario d’attaque 5**: user accède aux messages/privilèges d’un administrateur (attaque verticale)

**Business impact** : moyen/faible (pertes d’information/ confidentialité)

**Motivation :** avoir accès aux données privés, escalade de privilèges

**Scenario d’attaque :** modification d’ID, d’URL

**Contrôle :** prepared statement