STI 2021 - Étude de menaces

Projet 2 - Application de messagerie sécurisée

20 janvier 2021

Noémie Plancherel & Axel Vallon

Introduction

Lors de la première phase du cours STI, pour le projet 1, nous avons dû implémenter une application de messagerie web simple sans aspect sécuritaire. Le but de ce second projet est de reprendre le projet 1 et d'effectuer dans un premier temps une analyse de menaces complètes. En second temps, nous apporterons les aspects sécuritaires manquant à l'application.

Le rapport est structuré en 4 parties distinctes ; nous décrirons premièrement le système déjà existant et nous identifierons ces biens, c'est-à-dire les éléments que l'on cherche à protéger. Deuxièmement, nous définirons les sources de menaces de notre application de messagerie. Ensuite, nous établisserons différents scénarios d'attaques en les décrivant au mieux possible. Nous nous aiderons du modèle STRIDE pour le faire. Finalement, nous présenterons les contre-mesures effectuées.

Description du système

Objectifs du système

Pour rappel, l'objectif principal de cette application Web consiste en une messagerie avec des utilisateurs connectés. Il est possible de s'y connecter pour rédiger, répondre ainsi que de visualiser des messages. Ainsi, il existe deux rôles différents, collaborateur et administrateur. Le rôle administrateur a accès à des fonctionnalités en plus ; il peut gérer les utilisateurs de la messagerie (ajout, modification, suppression). Le but étant de garantir la confidentialité des messages échangés ainsi qu'une haute disponibilité du système afin d'avoir une bonne réputation et fiabilité auprès des utilisateurs.

Hypothèses de sécurité

On peut émettre deux hypothèses différentes concernant la sécurité :

- Serveur Web de confiance
- Réseau interne et administrateurs de confiance

Exigences du système

Nous allons lister les exigences de sécurité du système :

- **Contrôle d'accès** : le contenu administratif ne doit seulement être accessible aux administrateurs
- **Contrôle d'accès** : l'utilisateur doit avoir un compte actif pour accéder à la messagerie
- **Authentification** : un message doit être rédigé ou lu par un utilisateur connecté
- **Information fiable** : le contenu doit être protégé en intégrité, non modifiable
- **Confidentialité** : un message doit être uniquement lu par son auteur et destinataire.s
- **Unicité** : le nom d'utilisateur doit être unique
- **Disponibilité** : le site Web doit être disponible à 99% du temps
- **Privacy** : les informations des utilisateurs doivent être protégées

Éléments du système

Nous pouvons retrouver les éléments suivants dans notre système :

- Base de données des utilisateurs (*avec username, mot de passe, validité du compte et rôle*)
- Base de données des messages (*avec id, date, auteur, destinataire, sujet et message*)
- Application Web

Rôles des utilisateurs

Comme précisé précédemment, il existe deux rôles différents au sein de l'application :

- **Collaborateur** qui a la possibilité de
  - Rédiger un message
  - Répondre à un message
  - Consulter sa messagerie
  - Modifier et supprimer un message
  - Modifier son mot de passe
- **Administrateur** qui a la possibilité de
  - Effectuer les mêmes fonctionnalités qu'un collaborateur
  - Gérer un utilisateur (ajout, modification, suppression)

On peut ajouter deux rôles supplémentaires qui pourraient interagir avec le système :

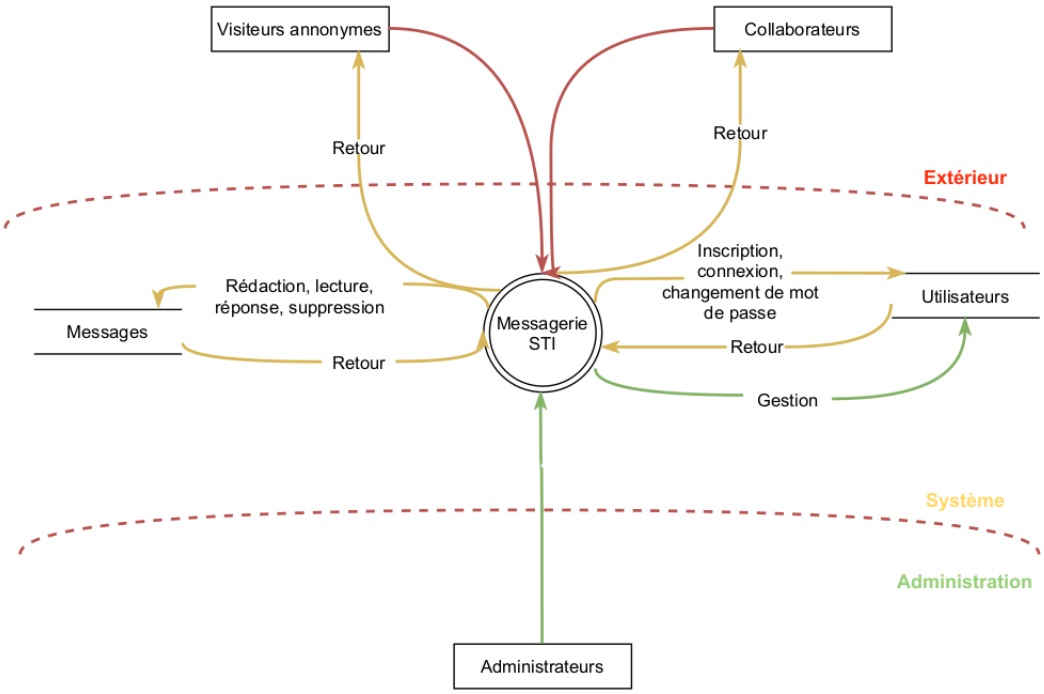
- **Administrateur du système/réseau** qui n'est pas directement inclu dans le système
- **Visiteur anonyme** qui n'a pas la possibilité d'accéder à la messagerie mais il peut se connecter ou créer un compte

Actifs à haute valeur

- **Base de données des utilisateurs** (données)
  - Confidentialité, sphère privée
  - Un incident pourrait nuire à la réputation du site
- **Base de données des messages** (données)
  - Confidentialité, sphère privée (uniquement utilisateurs concernés peuvent consulter le message)
  - Intégrité (message non modifiable une fois envoyé)
  - Un incident pourrait nuire à la réputation du site
- **Infrastructure**
  - Intégrité, disponibilité
  - Un incident pourrait être critique et nuire à la réputation, disponibilité ainsi qu'à la crédibilité du site Web

DFD

Afin de bien comprendre les interactions entre les différents rôles du système, nous avons dessiné un DFD (Data Flow Diagram). Les flèches rouges représentent l'interaction avec les utilisateurs externes, les flèches vertes l'interaction avec la partie administration du système et quant au flèches jaunes, elles représentent les interactions du système.



Périmètre de sécurisation

La sécurisation de l'application de messagerie se concentrera uniquement à l'applicatif. Ce qui concerne la sécurisation du serveur web (apache, https, . . .) ou la sécurisation de la machine (os, vm) est exclu du périmètre.

Sources de menaces

Nous allons définir quelques types de menaces possibles. Pour chaque cas, nous allons préciser les motivations, les cibles ainsi que la potentialité de la menace. Les cibles potentielles sont l'application Web de messagerie ainsi que la base de données avec tous les utilisateurs et tous les messages.

Hackers, script-kiddies

- **Motivation** : s'amuser, gagner la gloire
- **Cible** : application web, comptes utilisateurs, messages
- **Potentialité** : haute

Cybercrime (spam, maliciels

- **Motivation** : financières (rançons ou revente de données)
- **Cible** : vol de credentials des utilisateurs, modification d'informations, récupération des messages
- **Potentialité** : moyenne

Employés / Utilisateurs malins

- **Motivation** : accès au compte administrateur

- **Cible** : gestion des utilisateurs (ajout, suppression, modification)
- **Potentialité** : moyenne

Concurrents

- **Motivation** : espionnage industriel
- **Cible** : récupération des messages des utilisateurs
- **Potentialité** : moyenne

Scénario d'attaques

Scénario de menace 1 : Deviner des mots de passe

Impact sur l'entreprise Haut

Source de menace Hacker, Cybercrime, Employé, Concurrent

Motivation Pour les hackers, l'attaque peut être vue comme un amusement ou un défi personnel. Pour les concurrents ou un cybercrime, le but premier serait d'avoir accès à l'application de messagerie. Pour un employé, ce serait de se faire passer pour quelqu'un d'autre de l'entreprise, de lire les messages ou d'utiliser des fonctionnalités d'administrateur

Actif ciblé Utilisateurs (credentials)

Scénario d'attaque

Contre-mesures

Scénario de menace 2 : Vol de base de données (injection SQL)

Impact sur l'entreprise Haut

Source de menace Hacker, Cybercrime, Concurrent

Motivation La motivation principale de la récupération de données, sensibles ou non, de la base de données, est financière

Actif ciblé Base de données des utilisateurs et des messages

Scénario d'attaque Étant donné que la base de données n'est pas directement retournée au formulaire, car il permet uniquement la vérification de l'authentification, on peut utiliser l'outil sqlmap qui permet d'effectuer des injections SQL. Il permet d'identifier puis exploiter une injection SQL sur des applications web.

On peut premièrement vérifier sur le code source de la page web, quels sont les champs du formulaire qui sont envoyés en POST et depuis quelle page. Une fois cela vérifié, on exécute l'outil `sqlmap` avec les paramètres suivants :

- `--url` : URL cible pour tester les injections
- `--data` : données qui doivent être envoyées dans la requête POST
- `--dbms` : précise le type de base de données utilisée
- `--risk` : différents risques d'attaques. Ci-dessous le risque 3 effectue des attaques lourdes
- `--level` : différents niveaux d'attaques. Ci-dessous le niveau 5 effectue des attaques lourdes

- `--dump-all` : extraire les données de la DB

En exécutant la commande suivante, il est possible de récupérer toutes les données de la base de données de l'application web.

```
python2 sqlmap.py --url=http://localhost:8080/verificationLogin.php --data="inputLogin=111&
    inputPassword=222" --dbms=SQLite --risk=3 --level=5 --dump-all
```

Contre-mesures

Scénario de menace 3 : Bruteforce de mots de passe

Impact sur l'entreprise Haut

Source de menace Hacker, Cybercrime, Employé, Concurrent

Motivation Pour les hackers, l'attaque peut être vue comme un amusement ou un défi personnel. Pour les concurrents ou un cybercrime, le but premier serait d'avoir accès à l'application de messagerie. Pour un employé, ce serait de se faire passer pour quelqu'un d'autre de l'entreprise, de lire les messages ou d'utiliser des fonctionnalités d'administrateur

Actif ciblé

Scénario d'attaque

Contre-mesures

Scénario de menace 4 : Vol de mots de passe (interception)

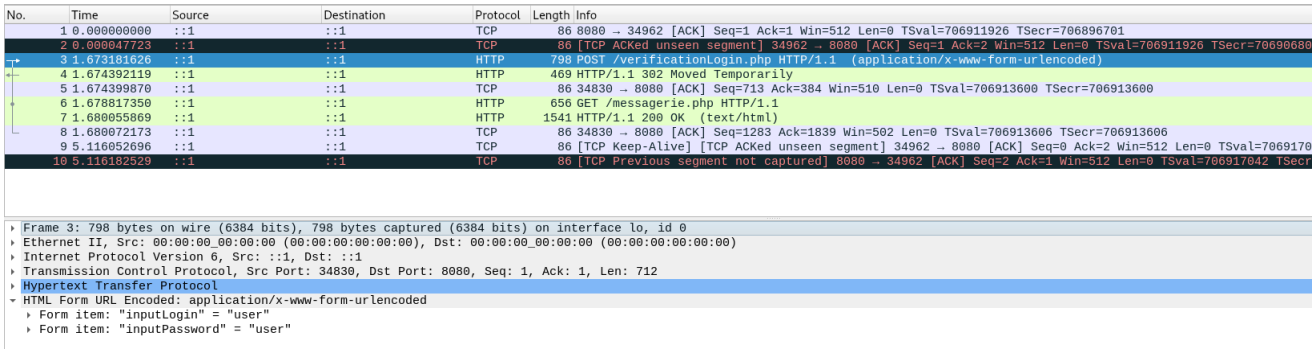
Impact sur l'entreprise Haut

Source de menace Employé (ou quelqu'un qui aurait accès au réseau interne de l'entreprise)

Motivation Le but peut être de se faire passer pour quelqu'un d'autre de l'entreprise, de lire de les messages ou d'utiliser les fonctionnalités d'administrateur

Actif ciblé Utilisateurs (credentials)

Scénario d'attaque On peut effectuer l'attaque en utilisant un sniffer de réseau comme Wireshark. Si le protocole utilisé est HTTP, les identifiants de l'utilisateur sont envoyés en clair et il est possible de capturer la trame.



Contre-mesures

Scénario de menace 5 : Vol de session

Impact sur l'entreprise Haut

Source de menace Hackers, Concurrent, Employé (avec des compétences avancées)

Motivation

Actif ciblé Utilisateurs, Administrateur

Scénario d'attaque

Contre-mesures

Scénario de menace 6 : Denial Of Service (DOS)

Impact sur l'entreprise Moyen à haut (indisponibilité du service de messagerie)

Source de menace Hackers, Concurrent, Employé (avec des compétences avancées)

Motivation

Actif ciblé Système entier

Scénario d'attaque

Contre-mesures

Scénario de menace 7 : Suppression des utilisateurs (XSS)

Impact sur l'entreprise Moyen

Source de menace Hacker, Concurrent, Employé (avec des compétences avancées)

Motivation

Actif ciblé Utilisateurs

Scénario d'attaque

Contre-mesures

Scénario de menace 8 : Modification d'un rôle d'un utilisateur (CSRF)

Impact sur l'entreprise

Source de menace Hacker, Concurrent, Employé (avec des compétences avancées)

Motivation

Actif ciblé

Scénario d'attaque

Contre-mesures

Scénario de menace 9 : Phishing

STRIDE

Contre-mesures