Travail à faire : Lab2 SSDLC
Etudiant : Mahdi SELMANI

1. Protection des Données Sensibles selon l'OWASP ASVS

L'OWASP Application Security Verification Standard (ASVS) fournit des exigences pour sécuriser les applications. Voici les besoins relatifs à la protection des données sensibles (sensitive data), extraits du standard OWASP ASVS :

Catégorie : Contrôles de confidentialité des données sensibles
Exigence : ASVS 3.1 : Protéger les données sensibles lors du stockage

Référence CWE : CWE-200 (Exposition d'informations sensibles)
Description : Les données sensibles doivent être stockées de manière sécurisée, par exemple en utilisant des mécanismes de chiffrement forts.
Exigence : ASVS 3.2 : Protéger les données sensibles lors de leur transmission

Référence CWE : CWE-319 (Transfert non sécurisé de données sensibles)
Description : Les données sensibles doivent être chiffrées lors de leur transmission, y compris l'utilisation de TLS/SSL pour les communications web.
Exigence : ASVS 3.3 : Protéger les données sensibles dans les sauvegardes

Référence CWE : CWE-22 (Path Traversal) ou CWE-732 (Insufficiently Protected Storage)
Description : Les sauvegardes contenant des informations sensibles doivent être correctement protégées (chiffrement).
Exigence : ASVS 3.4 : Limiter l'accès aux données sensibles

Référence CWE : CWE-284 (Accès inapproprié au contrôle de la fonctionnalité)
Description : Mettre en place un contrôle d'accès basé sur des rôles (RBAC) pour limiter l'accès aux données sensibles aux utilisateurs autorisés.
Catégorie : Contrôles de confidentialité des données privées (personnelles)
Exigence : ASVS 4.1 : Protéger les informations personnelles
Référence CWE : CWE-676 (Accès non autorisé à la mémoire d'une application)
Description : Les informations personnelles identifiables (PII) doivent être traitées et protégées conformément aux lois sur la protection des données (comme le RGPD en Europe).

2. Recherche sur les Modèles de Menaces

Les modèles de menaces (Threat Modelling) sont des approches utilisées pour identifier, évaluer et gérer les menaces potentielles dans un système.

Principaux Modèles de Menaces :
VAST (Visual, Agile, and Simple Threat modeling) : Un modèle visuel qui se concentre sur la simplification du processus de modélisation des menaces et son adaptation aux pratiques agiles.

DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) : Un modèle de scoring des menaces qui évalue les risques en fonction de cinq critères : dommage potentiel, reproductibilité, facilité d'exploitation, nombre d'utilisateurs affectés, et découvrabilité.

TRIKE (Threat Risk and Impact Knowledge Engine) : Un modèle de modélisation des menaces axé sur l'identification des risques et des impacts associés à la menace dans un environnement logiciel.

STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) : Un modèle bien connu qui identifie les menaces sous six catégories, en aidant à détecter les vulnérabilités dans les systèmes.

PASTA (Process for Attack Simulation and Threat Analysis) : Un modèle basé sur la simulation d'attaques et l'analyse des menaces. Il prend en compte plusieurs étapes pour analyser un système, de la définition des objectifs à l'identification des contrôles de sécurité.

Outils TMT (Threat Modelling Tools) :
Microsoft TMT : Un outil graphique développé par Microsoft pour modéliser des menaces dans des systèmes logiciels. Il permet de créer des diagrammes de flux de données et d'analyser les menaces.

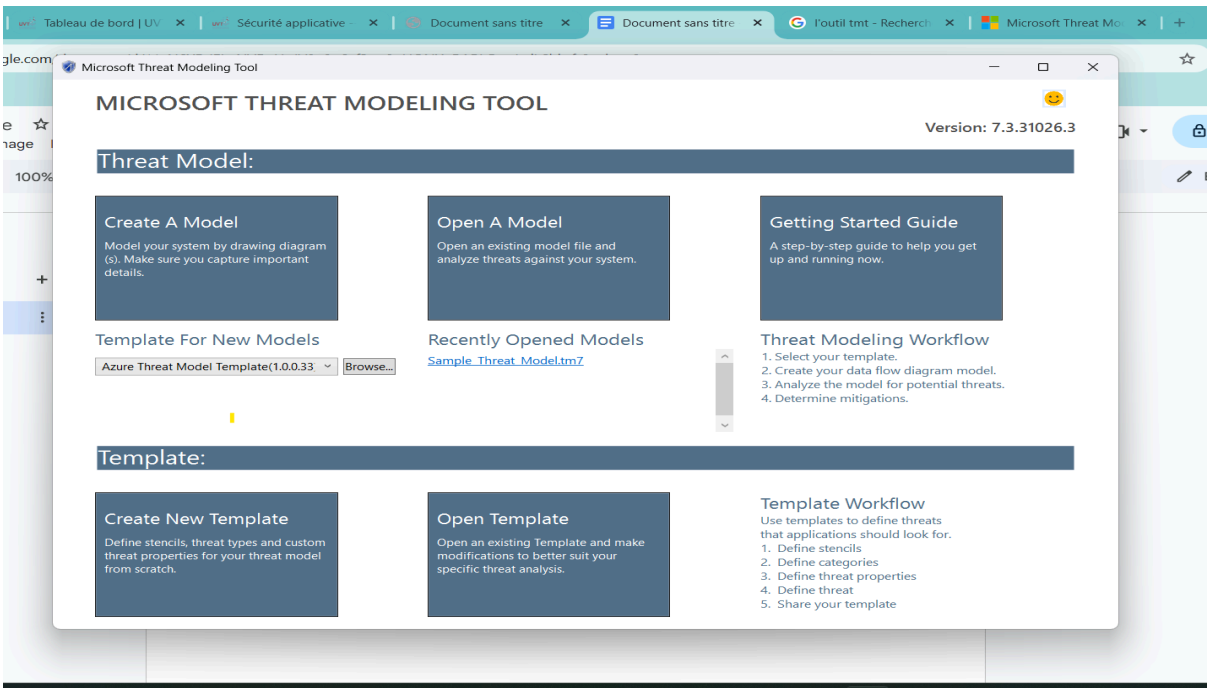
pyTMT : Un outil Python pour le modélisation des menaces qui permet de créer et d'analyser des modèles de menaces à l'aide d'un langage de programmation.

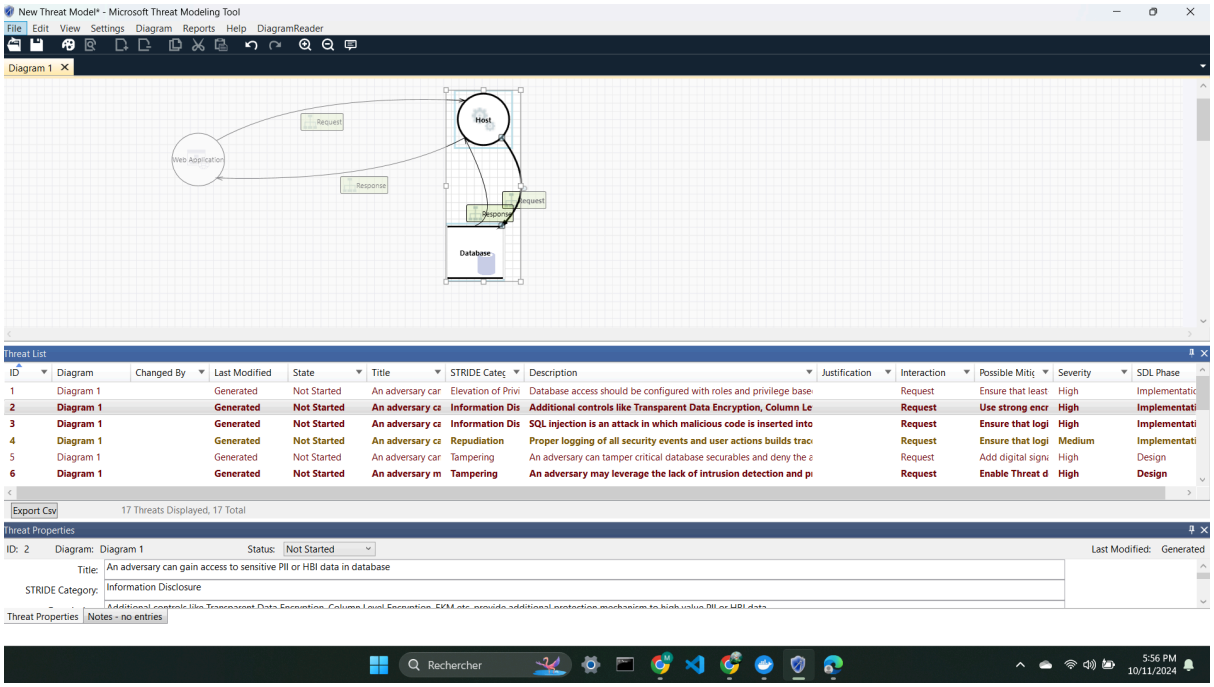
3. Installation et Utilisation de l'Outil TMT

Prenons comme exemple une application web avec une API RESTful qui stocke des données sensibles d'utilisateurs.

Architecture :
Frontend (Web Application) : L'application envoie des données via HTTPS vers le backend.
Backend (Hostl) : Le backend reçoit et traite les données, les stocke dans une base de données sécurisée.
Base de données (Database) : Stocke les informations sensibles comme les mots de passe, les numéros de carte de crédit..

l'outil Microsoft ™





Le rapport a généré 17 menaces, mais on se limiite à l'explication des 6 cas suivants :

1. Accès non autorisé à la base de données

État : Non commencé
Priorité : Haute
Description : L'absence de protection réseau permet à un attaquant d'accéder à la base de données sans autorisation.
Atténuation suggérée : Configurer un pare-feu pour restreindre l'accès à la base de données.

2. Règles d'autorisation laxistes

État : Non commencé
Priorité : Haute
Description : Des règles d'autorisation mal configurées peuvent permettre à un attaquant d'accéder à la base de données.
Atténuation suggérée : Utiliser des comptes à privilèges minimaux pour l'accès à la base de données.

3. Accès aux données sensibles (PII/HBI)

État : Non commencé
Priorité : Haute
Description : L'absence de chiffrement peut exposer des données sensibles dans la base de données.
Atténuation suggérée : Activer des méthodes de chiffrement pour les données sensibles.

4. Injection SQL

État : Non commencé
Priorité : Haute
Description : Un attaquant peut exploiter une vulnérabilité d'injection SQL pour accéder à la base de données.
Atténuation suggérée : Assurer un audit des connexions et valider les entrées pour prévenir les injections SQL.

5. Absence d'audit des actions sur la base de données

État : Non commencé

Priorité : Moyenne
Description : Sans audit des connexions et actions, il devient difficile de tracer les actions des utilisateurs et de détecter les attaques.
Atténuation suggérée : Activer l'audit des connexions et des actions sur le serveur SQL.

6. Chiffrement faible ou inexistant

État : Non commencé
Priorité : Haute
Description : Si des données sensibles sont stockées avec un chiffrement faible, elles peuvent être compromises.
Atténuation suggérée : Utiliser un chiffrement fort pour protéger les données sensibles.

4. Consultation du Guide OWASP SCP (Secure Coding Practices)

Le guide OWASP Secure Coding Practices (SCP) fournit des bonnes pratiques pour sécuriser les applications. Voici les bonnes pratiques concernant la Database Security et la Communication Security :

Database Security :
Utiliser des requêtes préparées et des paramètres liés pour éviter les attaques par injection SQL.
Limiter l'accès aux bases de données sensibles et appliquer des contrôles d'accès basés sur des rôles (RBAC).
Chiffrer les données sensibles dans la base de données en utilisant des algorithmes de chiffrement modernes.
Mettre en place des sauvegardes sécurisées et s'assurer que celles-ci sont chiffrées.
Communication Security :
Utiliser TLS (Transport Layer Security) pour sécuriser les communications réseau.
Ne jamais envoyer d'informations sensibles en texte clair (comme les mots de passe) sans les chiffrer.
Vérifier l'intégrité des données échangées pour éviter les attaques de type Man-in-the-Middle (MITM).