Etudiant : Mahdi SELMANI

1. Extraction des besoins relatifs à la protection des données sensibles de l'OWASP ASVS

Le standard OWASP ASVS (Application Security Verification Standard) fournit des lignes directrices pour protéger les données sensibles. Voici les principales catégories et quelques exemples de contrôles :

Catégorie : Contrôles de Cryptographie (V6)

- **V6.1.1 :** S'assurer que toutes les données sensibles sont cryptées en transit. (Référence CWE : CWE-319 - Cleartext Transmission of Sensitive Information)
- **V6.2.2 :** Utiliser des algorithmes cryptographiques approuvés pour protéger les données sensibles. (CWE-327 - Use of a Broken or Risky Cryptographic Algorithm)
- **V6.3.1 :** Les données sensibles doivent être chiffrées à l'aide de techniques de chiffrement approuvées lorsqu'elles sont stockées. (CWE-311 - Missing Encryption of Sensitive Data)

Catégorie : Contrôles d'Authentification (V2)

- **V2.3.1 :** Ne pas afficher de données sensibles dans les URL ou les logs. (CWE-598 - Information Exposure Through Query Strings in GET Request)
- **V2.4.1 :** Utiliser l'authentification multifacteur pour accéder aux données sensibles. (CWE-307 - Improper Restriction of Excessive Authentication Attempts)

Catégorie : Contrôles de Gestion des Sessions (V3)

- **V3.4.2 :** Garantir que les tokens d'authentification sont protégés pendant le transit et en stockage. (CWE-384 - Session Fixation)

2. Recherche sur les modèles de menaces et outils TMT

Modèles de menaces :

- **STRIDE** : Développé par Microsoft, il évalue les menaces en six catégories : Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.
- **DREAD** : Utilisé pour quantifier et prioriser les menaces en fonction des critères : Damage, Reproducibility, Exploitability, Affected Users, et Discoverability.
- **PASTA (Process for Attack Simulation and Threat Analysis)** : Modèle en sept étapes qui évalue les menaces à partir des objectifs de l'attaquant.
- **VAST (Visual, Agile, and Simple Threat)** : Conçu pour s'intégrer aux méthodologies Agile et DevOps.
- **TRIKE** : Un modèle orienté sur la gestion des risques qui se concentre sur les rôles, les atouts et les actions de sécurité.

Outils de Threat Modeling :

- **Microsoft Threat Modeling Tool (TMT)** : Un outil de Microsoft permettant de modéliser les menaces en suivant la méthodologie STRIDE.
- **pyTMT** : Un outil open-source qui offre une approche simplifiée de la modélisation des menaces.

3. Installation et utilisation de TMT pour analyser une architecture simple

Supposons une architecture simple composée d'une application web qui communique avec une base de données via une API REST. Voici comment installer et utiliser TMT pour ce scénario :

1. **Installation** : Téléchargez et installez le Microsoft TMT à partir du site officiel. Une fois installé, configurez une architecture de base en utilisant des composants comme le serveur d'application, le serveur de base de données et les utilisateurs.
2. **Analyse des menaces** : Utilisez TMT pour ajouter des flux de données et des composants. Lancez ensuite une analyse automatique.
3. **Types de menaces détectés** :
    - **Disclosure of Information** : Risque d'exposition de données sensibles via des erreurs de configuration réseau ou des requêtes non chiffrées.
    - **Tampering** : Manipulation des données en transit entre l'application et la base de données.
    - **Denial of Service** : Menace de déni de service sur le serveur d'application, pouvant entraîner une indisponibilité de l'application.

4. Bonnes pratiques OWASP SCP pour la sécurité des bases de données et la sécurité des communications

Database Security :

- **Accès minimal** : Limitez les privilèges aux utilisateurs de la base de données afin qu'ils n'aient que l'accès nécessaire pour exécuter leurs fonctions.
- **Séparation des environnements** : Évitez de mélanger les environnements de production et de développement, et utilisez des bases de données distinctes.
- **Chiffrement des données** : Chiffrez les données sensibles et utilisez des mots de passe forts pour les connexions à la base de données.

Communication Security :

- **Chiffrement des communications** : Utilisez des protocoles sécurisés comme TLS pour toutes les communications entre l'application et la base de données ou entre les utilisateurs et le serveur.
- **Authentification mutuelle** : Lorsque cela est possible, implémentez une authentification mutuelle pour vérifier à la fois le client et le serveur.
- **Protection contre les attaques par interception** : Activez HSTS (HTTP Strict Transport Security) pour forcer les navigateurs à utiliser les connexions sécurisées, réduisant ainsi les risques de détournement de sessions.