# Analyse des Risques d'une Application To-Do List

## Description de l'Application

L'application To-Do List est développée avec Django et propose une interface utilisateur intuitive pour gérer les tâches personnelles. Les fonctionnalités incluent l'inscription, l'authentification, la gestion des tâches.

## Actifs de l'Application

Les éléments critiques de l'application sont les suivants :

* - Données utilisateur : Noms, emails, mots de passe hashés.
* - Données des tâches : Titres, descriptions, échéances.
* - Sessions utilisateur et cookies pour l'authentification.
* - Infrastructure : Serveurs d'application, base de données.

## Menaces Identifiées

Voici les menaces potentielles identifiées :

* - Accès non autorisé aux données des tâches des utilisateurs.
* - Manipulation de cookies non sécurisés.
* - Risques d'injection SQL et XSS via les champs de saisie des tâches.
* - Vol de sessions utilisateur.
* - Mauvaise gestion des permissions pour les fonctionnalités de partage.

## Vulnérabilités

Les vulnérabilités de l'application incluent :

* - Headers de sécurité manquants (Content-Security-Policy, Strict-Transport-Security).
* - Absence de validation des entrées utilisateur dans les champs de tâche.
* - Manque de chiffrement des communications (absence de HTTPS).
* - Permissions insuffisamment restreintes sur les fonctionnalités de partage.

## Analyse des Risques

Tableau des risques :

|  |  |  |  |
| --- | --- | --- | --- |
| Risque | Probabilité | Impact | Niveau de Risque |
| Accès non autorisé aux données utilisateur | Élevée | Élevé | Critique |
| Manipulation de cookies | Moyenne | Moyen | Important |
| Injection SQL/XSS | Élevée | Élevé | Critique |
| Vol de sessions utilisateur | Élevée | Élevé | Critique |
| Mauvaise gestion des permissions | Moyenne | Moyen | Important |

## Plan d'Atténuation des Risques

* - Implémenter HTTPS (TLS) pour sécuriser toutes les communications.
* - Renforcer l'authentification avec 2FA.
* - Valider et désinfecter toutes les entrées utilisateur dans les champs de tâche.
* - Configurer des headers de sécurité (Content-Security-Policy, HSTS).
* - Tester régulièrement les vulnérabilités avec des outils comme OWASP ZAP.
* - Mettre en place des permissions strictes pour les fonctionnalités de partage.

## Conclusion

Cette analyse a permis d'identifier les risques critiques de l'application To-Do List et propose des solutions pratiques pour améliorer sa sécurité. La mise en œuvre des recommandations renforcera la résilience de l'application face aux menaces potentielles.