Stratégie de Sécurité de l'Application

2025

Rédigé par :

* MOHAMMADI ZABIULLAH

**Sommaire**

**Introduction**

**Chapitre 1:** Analyse Initiale et Évaluation des Risques

1.1 Méthodologie d'évaluation des risques

1.2 Identification des actifs critiques

1.3 Analyse des menaces spécifiques aux applications pire2pire.com

1.4 Évaluation de la maturité sécuritaire actuelle

1.5 Définition des objectifs de sécurité

**Chapitre 2:** Sécurisation du Front-end

2.1 Stratégie d'authentification

2.2 Protection contre les vulnérabilités côté client

2.3 Sécurité des données côté client

2.4 Mise en œuvre de Content Security Policy (CSP)

2.5 Techniques de développement sécurisé

**Chapitre 3:** Sécurisation de l'API

3.1 Architecture de sécurité API

3.2 Authentification et autorisation

3.3 Validation et filtrage des données

3.4 Mesures de protection de l'infrastructure API

3.5 Monitoring et logging de sécurité

**Chapitre 4:** Sécurisation de la Base de Données

4.1 Architecture sécurisée de la base de données

4.2 Chiffrement des données

4.3 Contrôle d'accès à la base de données

4.4 Auditing et surveillance

4.5 Stratégies de sauvegarde et récupération

**Conclusion**

**Introduction**

The security of digital applications has become a critical concern in today's interconnected world. This comprehensive security strategy for pire2pire.com aims to establish a robust framework that addresses potential vulnerabilities across all layers of the application architecture. By adhering to established security standards such as ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), OWASP (Open Web Application Security Project), and RGPD (Règlement Général sur la Protection des Données), this strategy ensures not only technical security but also compliance with regulatory requirements.

This security strategy is structured around four key pillars, each addressing a critical component of the application architecture:

**Initial Analysis and Risk Assessment**: This chapter establishes the foundation of our security approach, identifying potential threats, vulnerabilities, and risk levels specific to pire2pire.com. It incorporates methodologies from ANSSI and OWASP to create a comprehensive threat model tailored to the application's architecture and business context.

**Front-end Security**: This section focuses on implementing client-side security measures, including secure authentication mechanisms, protection against cross-site scripting (XSS), CSRF protection, secure data storage on the client side, and implementation of Content Security Policy (CSP).

**API Security**: Recognizing that APIs form the backbone of modern web applications, this chapter details strategies for securing the application's APIs, including authentication and authorization protocols, rate limiting, input validation, and measures against common API vulnerabilities as defined in the OWASP API Security Top 10.

**Database Security**: The final chapter addresses the security of data at rest, covering database architecture security, encryption methodologies, access control implementation, regular auditing processes, and backup strategies that align with both security best practices and RGPD compliance requirements.

Each chapter provides detailed technical guidance, best practices, and implementation recommendations tailored to the unique requirements of pire2pire.com. The ultimate goal is to create a secure application environment that protects both the platform and its users while maintaining functionality and performance.

**Chapter 1**

**1. Analyse Initiale et Évaluation des Risques**

**1.1 Identification des Actifs**

**Données sensibles :** Informations des utilisateurs (emails, mots de passe), données transactionnelles.

**Systèmes critiques :** Serveur web, base de données, API.

**Infrastructure** : Hébergement, certificats SSL, pare-feu.

**1.2 Menaces Principales**

**Attaques courantes :**

Injection SQL

ross-Site Scripting (XSS)

Vol de sessions (Session Hijacking)

Brute Force sur les comptes utilisateurs

**Erreurs humaines :** Mauvaise gestion des permissions, mots de passe faibles.

**Défaillances techniques :** Pannes serveur, mises à jour manquées.

**1.3 Classification des Données par Sensibilité**

|  |  |  |
| --- | --- | --- |
| **Niveau** | **Type de Données** | **Exemple** |
| Élevé | Mots de passe, paiements | Hashés et stockés en sécurité |
| Moyen | Emails, historiques d'achats | Protégés et limités en accès |
| Faible | Contenus publics | Visibles par tous |

**1.4 Analyse des Risques**

|  |  |  |  |
| --- | --- | --- | --- |
| Risque | Impact | Probabilité | Mesure de Protection |
| Vol de données | Élevé | Moyen | Chiffrement, MFA |
| Attaque DDoS | Moyen | Élevé | Protection anti-DDoS |
| Exploitation de vulnérabilités | Élevé | Élevé | Mises à jour régulières |

**2. Plan de Sécurisation**

**2.1 Mesures de Protection Techniques**

**Authentification et Accès :**

* Implémentation de l’authentification à deux facteurs (MFA)
* Politique de mots de passe forts

**Protection des Données :**

* Chiffrement des mots de passe (bcrypt)
* Utilisation de HTTPS (Certificat SSL)

**Sécurisation des API :**

* Utilisation de JWT pour authentifier les requêtes
* Filtrage des entrées pour éviter les injections SQL/XSS

**2.2 Mesures de Protection Organisationnelles**

**Gestion des accès :** Définir des rôles et permissions pour les administrateurs et utilisateurs.

**Surveillance et audit :**

* Journalisation des accès et tentatives de connexion suspectes.
* Surveillance en temps réel avec des outils de détection d’intrusion.

**2.3 Plan de Réaction aux Incidents**

|  |  |
| --- | --- |
| Étape | Action |
| Détection | Identification de l’incident via logs et alertes |
| Containment | Blocage des accès compromis, activation des protections |
| Remédiation | Correction des vulnérabilités, mise à jour des systèmes |
| Communication | Notification aux parties concernées (utilisateurs, admins) |