CDA-P5-VALS

STRATÉGIE DE SÉCURISATION

Writed by

Kenzo KERACHI

March 20th 2025

Global Introduction

This document presents a proposed security strategy for the pire2pire.com client.

To design robust security, several fundamental principles must be integrated.

A security-in-depth strategy, based on multiple layers of protection, ensures that even if one layer is compromised, the others remain intact to protect sensitive user and financial data, reducing the risk of unauthorized access and breach.

Reducing the attack surface is essential to limiting potential vulnerabilities. By limiting non-essential functionality, the risk of injection attacks and unauthorized intrusions is significantly reduced, exposing only the necessary components to potential threats.

In addition, GDPR compliance is essential to protect user privacy and avoid regulatory penalties. Proper management of user consent and transparency in data processing strengthen trust in the platform while ensuring compliance with legal requirements.

By adopting these principles, pire2pire.com can establish a secure environment that not only meets compliance standards but also enhances user confidence.

Sécurisation du Back-End : Principes et Bonnes Pratiques

1.1 Introduction

Avant de détailler les méthodes spécifiques de protection du back-end, il est essentiel de comprendre trois principes clés qui doivent guider toute stratégie de sécurité :

- La réduction de la surface d'attaque.
- La défense en profondeur.
- La politique du moindre privilège.

1.2 Réduction de la surface d'attaque **(p.11-12 ANSSI cote navigateur)**

Ce principe d'attaque représente l'ensemble des points d'entrée dans lesquels un attaquant peut tenter d'exploiter un système. Une réduction efficace implique de :

- Désactiver les services et fonctionnalités non nécessaires.
- Limiter l'exposition des API en autorisant uniquement les routes essentielles.
- Restreindre l'accès aux ports et services inutiles.
- Masquer les informations sensibles en évitant d'exposer des messages d'erreur techniques.

1.3 Défense en profondeur **(p.11 ANSSI cote navigateur)**

Ce principe consiste à multiplier les couches de protection pour qu'une faille à un niveau ne compromette pas l'ensemble du système. Cela inclut donc :

- Une authentification forte pour les accès administratifs.
- Des contrôles d'entrée robustes à tous les niveaux (Validations des entrées, restrictions API).
- Un chiffrement des données sensibles.
- Une journalisation continue de l'application.

1.4 Politique du moindre privilège **(p.11 ANSSI cote navigateur)**

L'accès aux ressources doit être limité au strict nécessaire. Cela implique :

- Des permissions seulement strictement nécessaires pour fonctionner pour les comptes utilisateurs et les services.
- Des rôles distincts pour chaque fonction (ex : utilisateur, modérateur, administrateur).

Protection des Identifiants et Comptes Utilisateurs

2.1 Stockage et gestion des mots de passe

- Utilisation d'un hachage robuste (avec l'aide par exemple de bcrypt pour JavaScript). **(R32 ANSSI Authentification et mots de passe)**
- Ajout d'un sel unique long à chaque mot de passe pour éviter les attaques de table pré-calculées. **(R32 ANSSI Authentification et mots de passe)**
- Recommandation imposant 12 caractères minimum pour les mots de passe avec un niveau de sensibilité moyen à fort et 15 caractères avec un niveau de sensibilité fort à très fort. **(R33 ANSSI Authentification et mots de passe)**

2.2 Protection contre les attaques par force brute

- Limite de tentatives de connexion avant blocage temporaire. **(R9 ANSSI Authentification et mots de passe)**
- Délai progressif entre chaque tentative échouée. **(R10 ANSSI Authentification et mots de passe)**
- Ajout d'un CAPTCHA après plusieurs échecs. **(R9 ANSSI Authentification et mots de passe)**
- Surveillance des connexions suspectes. **(R9 ANSSI Authentification et mots de passe)**

Protection contre les Cyberattaques

3.1 Protection contre les injections SQL (SQLi)

- Utilisation de requêtes préparées. **(R15 ANSSI cote navigateur)**
- Restrictions des permissions en base de données. **(R15 ANSSI cote navigateur)**
- Masquage des erreurs pour éviter de donner des informations aux attaquants. **(R59 ANSSI cote navigateur)**

3.2 Protection contre le Cross-Site Scripting (XSS)

- Filtrage et échappement des entrées utilisateur avant affichage. **(R7 ANSSI cote navigateur)**
- Activation d'une politique CSP (Content Security Policy) pour restreindre l'exécution de scripts non approuvés. **(R13 ANSSI cote navigateur)**

3.3 Protection contre les injections SQL (SQLi)

- Utilisation de tokens CSRF uniques pour les requêtes sensibles. **(R38 ANSSI cote navigateur)**

Sécurisation des Communications et Sessions

4.1 Chiffrement des Échanges

- Forcer l'utilisation de HTTPS. **(R1 ANSSI cote navigateur)**
- Activer HTTP Strict Transport Security (HSTS). **(R2 ANSSI cote navigateur)**

4.2 Sécurisation des Cookies et Sessions

- Activer HttpOnly, Secure, et SameSite=Strict sur les cookies. **(R26 ANSSI cote navigateur)**

Surveillance et Maintenance Sécurisée

5.1 Journalisation et Détection des Menaces

- Stocker toutes les tentatives de connexion et activités suspectes. **(R3.7 ANSSI cote navigateur)**
- Utiliser un système de monitoring en temps réel. **(R3.7 ANSSI cote navigateur)**

5.2 Mise à jour et Tests Réguliers

- Mises à jour systématiques des librairies et frameworks. **(R62 ANSSI cote navigateur)**
- Organisation de tests d'intrusion réguliers. **(R3.6 ANSSI cote navigateur)**
- Implémentation d'un programme de bug bounty. **(R3.6 ANSSI cote navigateur)**