

# STRATÉGIE DE SÉCURISATION



Written by  
Gabriel Luthun  
October 8th 2024

## Global introduction

This document is a proposal for a security strategy for the pire2pire.com client.

To develop a robust security strategy for pire2pire.com, it is essential to incorporate several key principles.

**Defense in depth**, based on a multi-layered approach, ensures that if one layer fails, others continue to protect sensitive user data and financial information, thereby preventing unauthorized access and data breaches.

**Reducing the attack surface** aims to minimize potential entry points for attackers by limiting non-essential functionalities, which helps mitigate the risks of injection attacks and unauthorized access. This ensures that only **necessary** components are exposed to threats.

Finally, **GDPR compliance** is crucial to protect user privacy and avoid penalties for non-compliance. This involves effective management of user consent and transparency in data management, thereby enhancing user trust in the platform.

By integrating these principles, pire2pire.com can effectively secure its platform while ensuring regulatory compliance and strengthening user trust.

## 1. Back-end

### a) Introduction

Dans le cadre de la sécurisation du back-end de pire2pire.com, l'application de la **politique de moindre privilège** est une étape **cruciale**. Cette approche consiste à accorder aux utilisateurs et aux systèmes uniquement les permissions **nécessaires** pour accomplir leurs tâches spécifiques, sans accès supplémentaire.

La mise en œuvre de la **politique de moindre privilège** est essentielle pour limiter les risques associés à l'accès excessif aux ressources du système. En restreignant les permissions, on réduit la probabilité que des utilisateurs ou des processus puissent exploiter des priviléges non nécessaires pour accéder à des données sensibles ou effectuer des actions potentiellement dommageables.

Cette politique vise principalement à prévenir les **menaces internes et externes**, telles que les abus de privilèges et les mouvements latéraux au sein du système en cas de compromission d'un compte utilisateur. Dans le contexte de pire2pire.com, où différents types d'utilisateurs (administrateurs, formateurs, apprenants) interagissent avec la plateforme, il est crucial de s'assurer que chacun ne dispose que des accès strictement nécessaires à ses fonctions. Cela permet non seulement de protéger les données sensibles des utilisateurs et le contenu pédagogique, mais aussi d'assurer une conformité accrue avec les réglementations en matière de protection des données. En

appliquant cette politique, pire2pire.com peut renforcer sa sécurité globale tout en minimisant les risques d'erreurs humaines ou d'abus intentionnels.

## b) RBAC (Role-Based-Access-Control)

Le contrôle d'accès basé sur les rôles (RBAC) est un modèle **essentiel** pour gérer les permissions sur pire2pire.com, en attribuant des rôles spécifiques aux utilisateurs selon leurs fonctions.

Le RBAC renforce la sécurité en limitant l'accès des utilisateurs aux seules ressources nécessaires à leurs tâches, réduisant ainsi le risque d'accès non autorisé et de violations de données. Il simplifie également la gestion des permissions en centralisant le contrôle sous forme de rôles, minimisant les erreurs humaines et facilitant la conformité réglementaire.

Ce modèle lutte contre les abus de privilèges et les accès non autorisés.

Sur pire2pire.com, où coexistent administrateurs, formateurs et apprenants, le RBAC assure que chacun accède uniquement aux informations **pertinentes** pour son rôle. Par exemple, un administrateur peut gérer l'ensemble de la plateforme, tandis qu'un formateur gère uniquement ses cours. Cette segmentation protège les données sensibles et garantit que l'accès reste aligné avec les besoins opérationnels, tout en respectant les normes comme le RGPD. Ainsi, pire2pire.com assure une sécurité renforcée et une confiance accrue des utilisateurs

## 1.2) Bases de données

### a) Politique des mots de passe

Pour sécuriser les mots de passe des utilisateurs sur pire2pire.com, il est essentiel d'adopter une politique de mots de passe rigoureuse, reposant sur deux techniques clés : le hachage et le salage.

#### Hachage

Le hachage est une méthode qui convertit un mot de passe en une chaîne cryptographique **fixe**. Cela permet de stocker les mots de passe de manière sécurisée, car le haché ne peut pas être facilement inversé pour retrouver le mot de passe original.

Pour garantir une sécurité optimale, il est crucial d'utiliser des algorithmes de hachage robustes tels que **bcrypt**, qui utilise un hachage SHA-256.

Ces algorithmes sont conçus pour être résistants aux attaques par force brute en ralentissant le processus de hachage, ce qui rend les tentatives d'attaque coûteuses en termes de temps et de ressources.

#### Salage

Le salage consiste à ajouter une valeur aléatoire unique, appelée sel, à chaque mot de passe avant son hachage.

Cette pratique renforce la sécurité du mot de passe en introduisant une variabilité supplémentaire dans le processus de hachage :

- Unique pour chaque utilisateur : Chaque utilisateur doit avoir un sel différent pour garantir que même si deux utilisateurs ont le

même mot de passe, leurs hachés seront différents. Cela empêche l'utilisation efficace des tables arc-en-ciel, qui sont des pré-calculs d'hachés pour accélérer les attaques.

- Longueur suffisante : Les sels doivent être suffisamment longs (au moins 16 octets) pour assurer une bonne protection contre les collisions et les attaques par force brute.
- Stockage sécurisé : Le sel doit être stocké dans la base de données avec le haché du mot de passe mais séparément du reste des données utilisateur pour minimiser les risques en cas de compromission partielle du système.

En combinant le hachage avec un salage efficace, pire2pire.com peut considérablement **renforcer** la sécurité des mots de passe stockés, protégeant ainsi les utilisateurs contre les tentatives d'accès non autorisé et contribuant à la conformité avec les meilleures pratiques en matière de sécurité des données.

Pour renforcer la sécurité des mots de passe sur pire2pire.com, il est crucial d'établir une politique de **complexité** qui impose des exigences spécifiques en termes de longueur et de robustesse.

## b) UUID

L'utilisation des **UUID** (Identifiants Uniques Universels) dans la gestion des bases de données de pire2pire.com offre plusieurs avantages stratégiques, tant en termes de sécurité que de gestion efficace des données.

Les UUID garantissent l'unicité des identifiants à travers le système, ce qui est essentiel pour éviter les collisions d'identifiants, surtout dans un environnement où les données peuvent provenir de sources multiples ou être fusionnées. Cela permet à pire2pire.com de gérer les enregistrements de manière sécurisée et sans conflits, même à grande échelle.

L'utilisation des UUID aide à prévenir les problèmes liés aux identifiants séquentiels classiques, tels que les risques de prédiction et l'exposition involontaire de la structure interne de la base de données.

Contrairement aux identifiants numériques incrémentaux, les UUID ne révèlent pas d'informations sur l'ordre ou le nombre total d'enregistrements, renforçant ainsi la sécurité en rendant plus difficile pour un attaquant de déduire des informations sensibles.

En adoptant les UUID, pire2pire.com peut non seulement améliorer la sécurité et l'intégrité des données mais aussi se préparer à une croissance future et à une intégration harmonieuse avec d'autres systèmes.

## c) Politique de rétention

La mise en place d'une politique de rétention efficace pour les sauvegardes est **cruciale** pour garantir la disponibilité et l'intégrité des données sur pire2pire.com. Cette politique doit inclure des stratégies claires concernant l'automatisation, le nombre de sauvegardes à conserver et la fréquence des sauvegardes.

La sauvegarde régulière des données est essentielle pour protéger contre les pertes de données dues à des pannes système, des erreurs humaines ou des attaques malveillantes. Pour pire2pire.com, une politique de sauvegarde bien définie assure que les données peuvent être restaurées rapidement et efficacement en cas d'incident.

Dans le cadre de pire2pire.com, il est recommandé de suivre une politique de rétention automatisée avec des paramètres spécifiques :

- **Nombre de sauvegardes**

Il est important de déterminer le nombre optimal de sauvegardes à conserver. Cela dépendra de la capacité de stockage disponible et des besoins spécifiques de l'entreprise en matière de récupération. Une règle courante est de conserver plusieurs générations de sauvegardes (par exemple, quotidienne, hebdomadaire, mensuelle) pour assurer une flexibilité dans la restauration des données.

- **Fréquence de sauvegardes**

La fréquence des sauvegardes doit être adaptée aux besoins opérationnels de pire2pire.com. Pour une plateforme en ligne traitant potentiellement des données sensibles et en constante évolution, il

est recommandé d'effectuer des sauvegardes quotidiennes. Cela garantit que les données sont toujours à jour et minimise la perte potentielle d'informations entre deux sauvegardes.

En mettant en œuvre une politique de rétention avec une automatisation adéquate, pire2pire.com peut assurer la continuité de ses opérations tout en protégeant efficacement ses données contre divers risques. Cette approche permet également de répondre aux exigences réglementaires en matière de protection et de récupération des données.

## 1.3) API

### a) Sécurisation des communications

Pour sécuriser les communications entre les API de pire2pire.com et ses utilisateurs, il est essentiel de mettre en place des protocoles robustes tels que TLS et HSTS.

- **TLS**

TLS est un protocole de sécurité qui chiffre les données transmises entre le client et le serveur, garantissant que les informations ne peuvent pas être interceptées ou altérées par des tiers malveillants. Cela protège la confidentialité des données utilisateur et renforce la confiance dans la plateforme.

TLS protège contre les attaques de type interception de données (man-in-the-middle).

Dans le contexte de pire2pire.com, où des informations personnelles et potentiellement sensibles sont échangées, l'utilisation de TLS est indispensable pour sécuriser ces communications et assurer que seules les parties autorisées peuvent accéder aux données.

- **HSTS**

HSTS est une politique de sécurité qui indique aux navigateurs d'accéder uniquement à pire2pire.com via des connexions sécurisées (HTTPS). Cela empêche les attaques de type downgrade, où un attaquant pourrait forcer une connexion non sécurisée pour intercepter les données.

HSTS lutte contre les attaques de type man-in-the-middle en forçant l'utilisation du protocole HTTPS. Pour pire2pire.com, cela garantit que toutes les communications restent chiffrées, même si un utilisateur tente d'accéder au site via HTTP. Cela renforce la sécurité globale du site en éliminant la possibilité d'une connexion non sécurisée.

En intégrant **TLS** et **HSTS**, pire2pire.com peut assurer une protection **solide** des communications API, renforçant ainsi la sécurité des données utilisateur et la confiance dans la plateforme.

## b) Sécurisation des origines

La sécurité des origines vise à contrôler les interactions entre différentes sources et à protéger contre les attaques potentielles qui exploitent ces interactions.

En voici quelques unes :

- **SOP (Same-Origin Policy) : même origine**

La SOP est une politique de sécurité fondamentale qui restreint les scripts exécutés sur une page web à interagir uniquement avec des ressources provenant de la **même origine**. Cela empêche les scripts malveillants d'un site tiers d'accéder aux données sensibles sur pire2pire.com.

La SOP protège contre les attaques de type cross-site scripting (XSS) et le vol de données. Dans le contexte de pire2pire.com, elle assure que seules les requêtes provenant du même domaine peuvent accéder aux ressources critiques, renforçant ainsi la sécurité des données utilisateur.

- **CORS (Cross-Origin Resource Sharing) : différentes origines**

CORS est un mécanisme qui permet aux serveurs de spécifier quelles origines sont autorisées à accéder à leurs ressources. Cela offre une flexibilité pour permettre certaines interactions **inter-origines** tout en maintenant la sécurité.

CORS protège contre les requêtes non autorisées provenant d'origines externes. Pour pire2pire.com, il permet de contrôler et sécuriser les accès aux API depuis des domaines tiers autorisés, tout en empêchant les accès non désirés.

- **CSP (Content Security Policy) : différentes ressources**

CSP est une politique de sécurité qui aide à prévenir les attaques XSS en contrôlant **quelles ressources** peuvent être chargées et exécutées par une page web.

CSP protège contre l'injection de contenu malveillant. Pour pire2pire.com, cela signifie que seules les ressources provenant de sources approuvées peuvent être intégrées ou exécutées, ce qui renforce la sécurité globale du site.

- **Utilisation d'un ORM (Object-Relational Mapping)**

Un ORM facilite l'interaction sécurisée avec la base de données en permettant aux développeurs d'utiliser des objets plutôt que des requêtes SQL brutes, réduisant ainsi le risque d'injections SQL.

Dans le contexte de pire2pire.com, son utilisation permet d'assurer que toutes les interactions avec la base de données sont sécurisées et conformes aux meilleures pratiques en matière de développement sécurisé.

## c) Authentification

Pour renforcer la sécurité des API de pire2pire.com, il est essentiel de mettre en place des mécanismes d'authentification robustes et de contrôler l'accès aux API via la limitation d'appels.

L'authentification est cruciale pour s'assurer que seules les entités autorisées peuvent accéder aux ressources API.

Pour mettre en place des mécanismes d'authentification solide, voilà quelques préconisations :

- **Token**

L'utilisation de tokens pour l'authentification permet de vérifier l'identité des utilisateurs ou des applications accédant à l'API. Les tokens sont générés après une authentification réussie et sont utilisés pour valider les requêtes ultérieures sans nécessiter de renvoyer les identifiants sensibles.

Les tokens aident à prévenir les accès non autorisés et à sécuriser les sessions utilisateur.

Dans le contexte de pire2pire.com, ils permettent une authentification sans état, ce qui est particulièrement utile pour les applications web et mobiles nécessitant un accès constant aux API. Les tokens peuvent être configurés avec des durées de vie limitées et des permissions spécifiques, renforçant ainsi la sécurité.

- **Limitation d'appel API**

La limitation d'appel API (ou rate limiting) contrôle le nombre de requêtes qu'un utilisateur ou une application peut effectuer dans un laps de temps donné. Cela protège les ressources du serveur contre les abus et prévient les attaques par déni de service (DoS).

Cette mesure lutte contre les abus de l'API, tels que les attaques par force brute ou le scraping excessif.

Pour pire2pire.com, la limitation d'appel API assure que le service reste disponible pour tous les utilisateurs légitimes même lors de pics d'activité ou en cas de tentative d'attaque. Elle permet également de gérer efficacement la charge du serveur et d'améliorer l'expérience utilisateur globale.

## 2. Front-end

### Introduction

Dans le développement et la sécurisation des API de pire2pire.com, une règle d'or **fondamentale** est de ne **jamais** faire confiance au client, c'est-à-dire au navigateur ou à toute autre application cliente.

Cette approche préventive est essentielle pour protéger la plateforme contre diverses menaces potentielles.

Les clients, tels que les navigateurs web, sont souvent la cible d'attaques et peuvent être compromis par des acteurs malveillants. En ne faisant pas confiance aux données reçues du client, pire2pire.com peut éviter l'injection de contenu malveillant et garantir que seules les données valides et sécurisées sont traitées par le serveur.

Cette règle lutte contre les attaques telles que l'injection SQL, le cross-site scripting (XSS), et d'autres formes de manipulation de données.

Dans le contexte de pire2pire.com, où des informations sensibles sont échangées via les API, il est crucial de valider et de filtrer toutes les entrées provenant du client. Cela inclut la vérification des formats de données attendus, l'utilisation de listes blanches pour les valeurs acceptables, et le rejet systématique des entrées suspectes ou malformées.

En appliquant strictement cette règle, pire2pire.com peut renforcer la sécurité de ses API en s'assurant que toutes les interactions avec le client sont soigneusement contrôlées et sécurisées. Cela protège non seulement les données utilisateur mais aussi l'intégrité du système dans son ensemble.

### a) Protocoles de sécurité côté Front-end

Pour assurer la sécurité côté front-end de pire2pire.com, il est crucial de mettre en œuvre divers protocoles de sécurité qui protègent les données des utilisateurs et garantissent l'intégrité des communications.

Voici une vue détaillée de ces protocoles :

- **HTTP + TLS = HTTPS**

HTTPS est la version sécurisée du protocole HTTP, utilisant TLS (Transport Layer Security) pour chiffrer les données échangées entre le client et le serveur. Cela garantit que les informations sensibles ne peuvent pas être interceptées ou modifiées par des tiers malveillants.

HTTPS protège contre les attaques de type écoute clandestine (eavesdropping) et l'interception de données (man-in-the-middle). Dans le contexte de pire2pire.com, où des informations personnelles et financières peuvent être transmises, l'utilisation d'HTTPS est essentielle pour assurer la confidentialité et la sécurité des communications.

- **HSTS (HTTP Strict Transport Security)**

HSTS est une politique qui indique aux navigateurs d'accéder uniquement à pire2pire.com via des connexions sécurisées (HTTPS). Cela empêche les attaques de type downgrade, où un attaquant pourrait forcer une connexion non sécurisée.

HSTS lutte contre les attaques man-in-the-middle en forçant l'utilisation du protocole HTTPS. Pour pire2pire.com, cela garantit que toutes les communications restent chiffrées, même si un utilisateur tente d'accéder au site via HTTP, renforçant ainsi la sécurité globale du site.

- **TLS (Transport Layer Security)**

TLS assure la confidentialité et l'intégrité des données échangées entre le client et le serveur. Il est utilisé pour chiffrer les communications et garantir qu'elles ne peuvent pas être altérées en transit.

TLS protège contre l'écoute clandestine et l'interception de données. Pour pire2pire.com, c'est une couche essentielle qui sécurise toutes les interactions sensibles, protégeant ainsi les utilisateurs et leurs données.

- **SOP (Same-Origin Policy)**

La SOP est une politique de sécurité qui restreint les scripts exécutés sur une page web à interagir uniquement avec des ressources provenant de la même origine. Cela empêche les scripts malveillants d'un site tiers d'accéder aux données sensibles sur pire2pire.com.

La SOP protège contre les attaques cross-site scripting (XSS) et le vol de données. Dans le contexte de pire2pire.com, elle assure que seules les requêtes provenant du même domaine peuvent accéder aux ressources critiques, renforçant ainsi la sécurité des données utilisateur.

## CSP (Content Security Policy)

CSP aide à prévenir les attaques XSS en contrôlant quelles ressources peuvent être chargées et exécutées par une page web. Elle permet de spécifier quelles sources sont approuvées pour charger du contenu sur le site.

CSP protège contre l'injection de contenu malveillant.

Pour pire2pire.com, cela signifie que seules les ressources provenant de sources approuvées peuvent être intégrées ou exécutées, ce qui renforce la sécurité globale du site.

## Referrer Policy

La Referrer Policy contrôle la quantité d'informations envoyées dans l'en-tête HTTP Referer lors de la navigation entre pages. Elle permet de limiter l'exposition des URL complètes aux sites tiers.

Cette politique protège contre la fuite d'informations sensibles contenues dans les URL. Pour pire2pire.com, elle assure que seules les informations nécessaires sont partagées avec des sites externes, réduisant ainsi le risque d'exposition involontaire de données sensibles.

## SRI (Subresource Integrity)

SRI permet aux navigateurs de vérifier que les fichiers récupérés (comme des scripts ou des styles) n'ont pas été modifiés par rapport à ce qui était prévu. Cela se fait en comparant un haché cryptographique spécifié dans le code source avec celui du fichier récupéré.

SRI protège contre l'injection malveillante dans des ressources tierces chargées sur le site. Pour pire2pire.com, cela garantit que tous les scripts et styles externes n'ont pas été compromis avant leur exécution sur le site, renforçant ainsi la sécurité et l'intégrité du contenu chargé. En mettant en œuvre ces protocoles de sécurité côté front-end, pire2pire.com peut assurer une protection robuste des données utilisateur tout en maintenant un haut niveau d'intégrité et de confiance dans ses communications web.

## Conclusion

En conclusion, la sécurisation de pire2pire.com repose sur une stratégie intégrée qui répond aux besoins de sécurité, de conformité et d'expérience utilisateur.

**Sécurité et Conformité** : L'utilisation de TLS et HSTS protège les communications, tandis que le hachage et le salage des mots de passe assurent la confidentialité des informations d'authentification. Les UUID garantissent l'unicité des enregistrements, renforçant la sécurité des données.

**Contrôle d'accès** : Le modèle RBAC et le principe de moindre privilège limitent les permissions aux seules ressources nécessaires, réduisant ainsi les risques d'abus tout en respectant le RGPD.

**Protection des API** : L'authentification par token et la limitation d'appel API sécurisent l'accès aux ressources, tandis que SOP, CORS, et CSP contrôlent les interactions inter-origines pour prévenir les attaques XSS.

**Sécurité Front-End** : HTTPS, CSP, Referrer Policy, et SRI protègent contre l'injection de contenu malveillant, assurant des interactions utilisateur sécurisées.

**Disponibilité** : Une politique de rétention automatisée garantit la continuité des opérations et une récupération rapide en cas d'incident.

Cette approche globale assure une plateforme sécurisée, conforme et fiable, renforçant la confiance des utilisateurs et soutenant le succès à long terme du projet.

## Idées d'amélioration

Pour améliorer encore la sécurité et l'efficacité de pire2pire.com, voici quelques suggestions :

1. **Authentification Multifactorielle (MFA)** : Mettre en place une authentification à deux facteurs pour renforcer la sécurité des comptes utilisateurs, en ajoutant une couche supplémentaire de vérification lors de la connexion.
2. **Surveillance et Alertes en Temps Réel** : Implémenter des systèmes de surveillance qui détectent et signalent les activités suspectes en temps réel. Cela permet de réagir rapidement aux incidents de sécurité potentiels.
3. **Tests de Pénétration Réguliers** : Effectuer des tests de pénétration périodiques pour identifier et corriger les vulnérabilités avant qu'elles ne soient exploitées par des attaquants.
4. **Formation à la Sécurité** : Sensibiliser les utilisateurs et le personnel aux meilleures pratiques en matière de sécurité, y compris la reconnaissance des tentatives de phishing et l'importance de maintenir des mots de passe sécurisés.
5. **Mise à Jour Automatique des Logiciels** : S'assurer que tous les systèmes et logiciels utilisés sont automatiquement mis à jour pour inclure les derniers correctifs de sécurité.

6. **Chiffrement des Données au Repos** : En plus du chiffrement des données en transit, envisager le chiffrement des données au repos pour protéger les informations sensibles stockées dans la base de données.
7. **Gestion Avancée des Journaux** : Mettre en place une gestion avancée des journaux pour suivre toutes les actions effectuées sur la plateforme, facilitant ainsi les audits et l'analyse post-incident.
8. **Évaluation Continue des Risques** : Établir un processus d'évaluation continue des risques pour identifier les nouvelles menaces et ajuster les mesures de sécurité en conséquence.

En intégrant ces améliorations, pire2pire.com peut renforcer sa posture de sécurité, améliorer sa résilience face aux menaces émergentes et continuer à offrir une expérience utilisateur sécurisée et fiable.