

STRATÉGIE DE SÉCURISATION



Sommaire

- Pourquoi sécuriser Pire2Pire.com
- RGPD
- Les principes de sécurité appliqués à Pire2Pire.com
- Les risques et attaques courantes
- Sécurité de la base de données
- Sécurité de l'API
- Sécurité du DOM
- Sécurité du navigateur
- Conclusion



Pourquoi sécuriser Pire2Pire.com ?

- Pire2Pire.com gère des données sensibles
- Objectif : protéger les utilisateurs et éviter les cyberattaques
- Principales menaces : vol de données, usurpation d'identité, pannes

RGPD

Règlement Général sur la Protection des Données

Droits des utilisateurs

Données Personnelles

Responsabilité

Juridictions



Les principes de sécurité appliqués à Pire2Pire.com



Réduction de la surface d'attaque :

Limiter les points d'entrée

Défense en profondeur :

Plusieurs couches de protection

Moindres priviléges :

Accès limité selon les rôles

Chiffrement :

Protection des données en cas de vol

Les risques et attaques courantes

Injection SQL (SQLi) :

Manipulation de la base de données

CSRF (Cross Site Request Forgery) :

Exécution d'actions non voulues

LFI/RFI (inclusion de fichiers locaux/distant)

Accès à des fichiers sensibles

XSS (cross-site scripting) :

Injection de scripts malveillants

SSRF (Server-Side Request Forgery)

Exfiltration de données internes, accès non autorisé à des systèmes internes

XXE (XML External Entity)

Accès non autorisé à des fichiers locaux

Sécurité de la base de données

SQLi

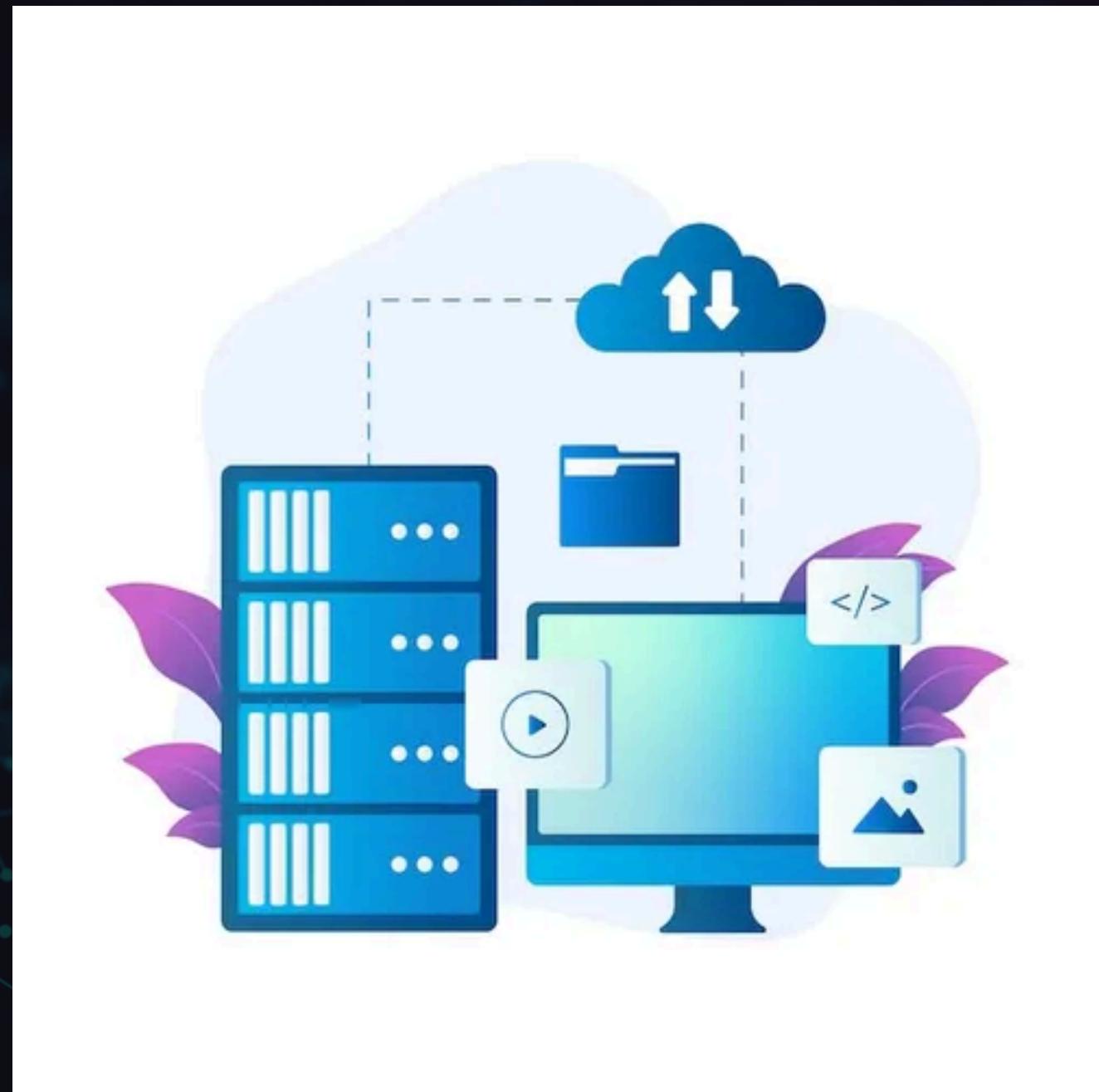
RBAC

Hachage

Attaques XSS et CSRF

Sauvegardes

Journalisation

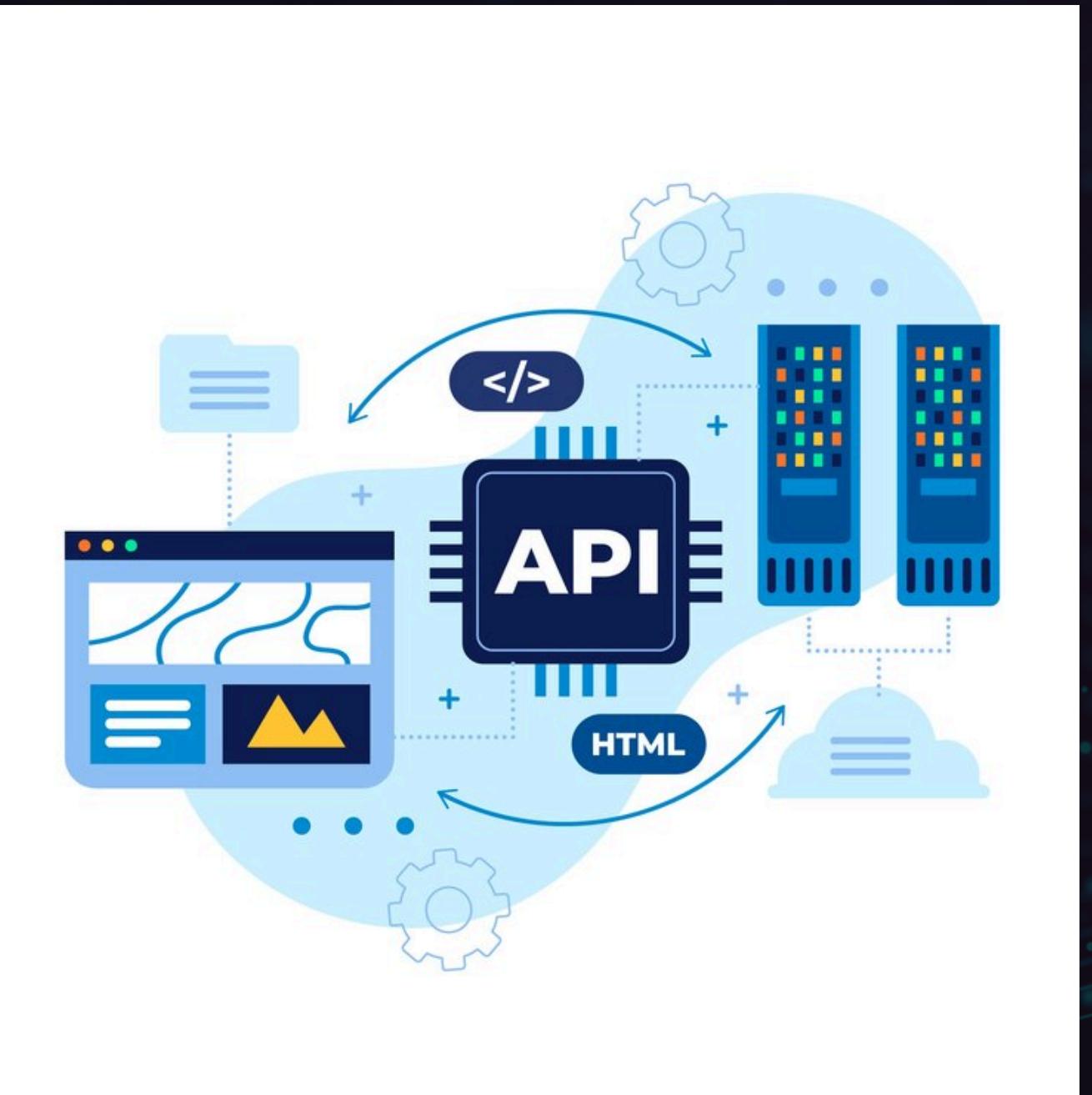


Sécurité de l'API

TLS et Authentification

CORS

DoS et DDoS



CSRF

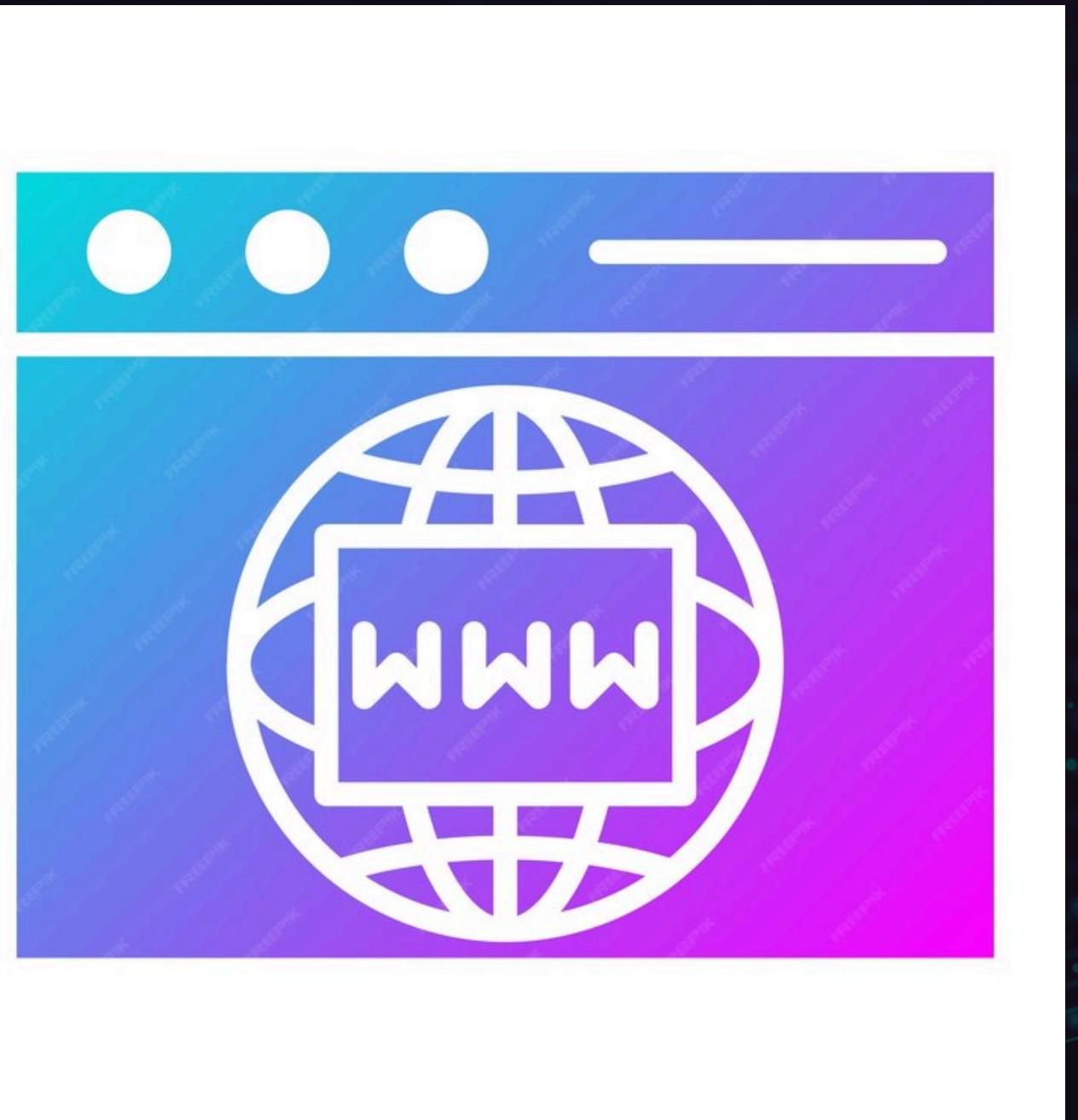
SSRF

XXE

Sécurité du DOM

Manipulation du DOM

Clickjacking



Validation et nettoyage des entrées

Sécurité du navigateur

HTTPS

HSTS



Cookies

Stockage Web

Conclusion