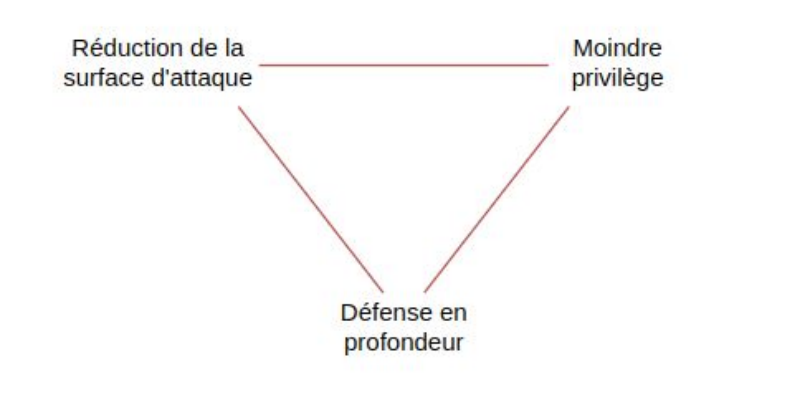
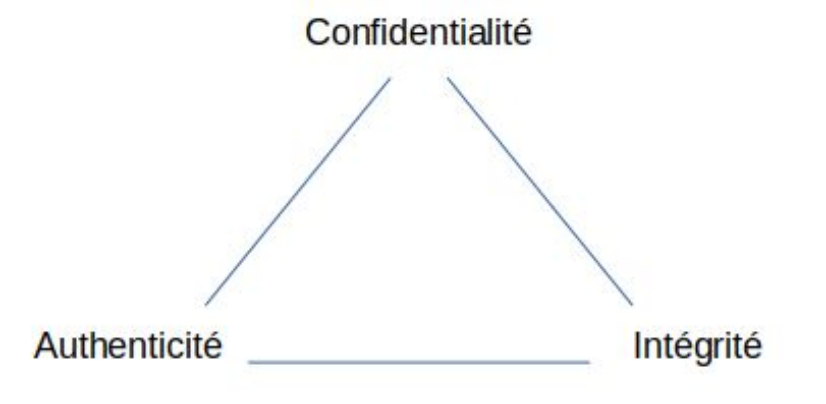
Proposition d'une stratégie de sécurisation d'application

Mission locale du Valenciennois

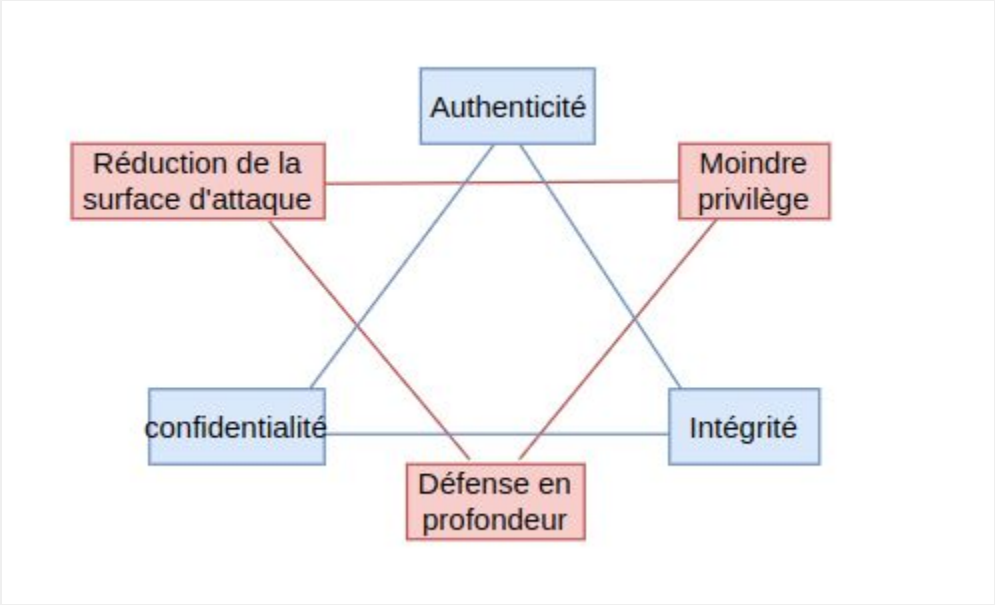
Table des matières

Introduction

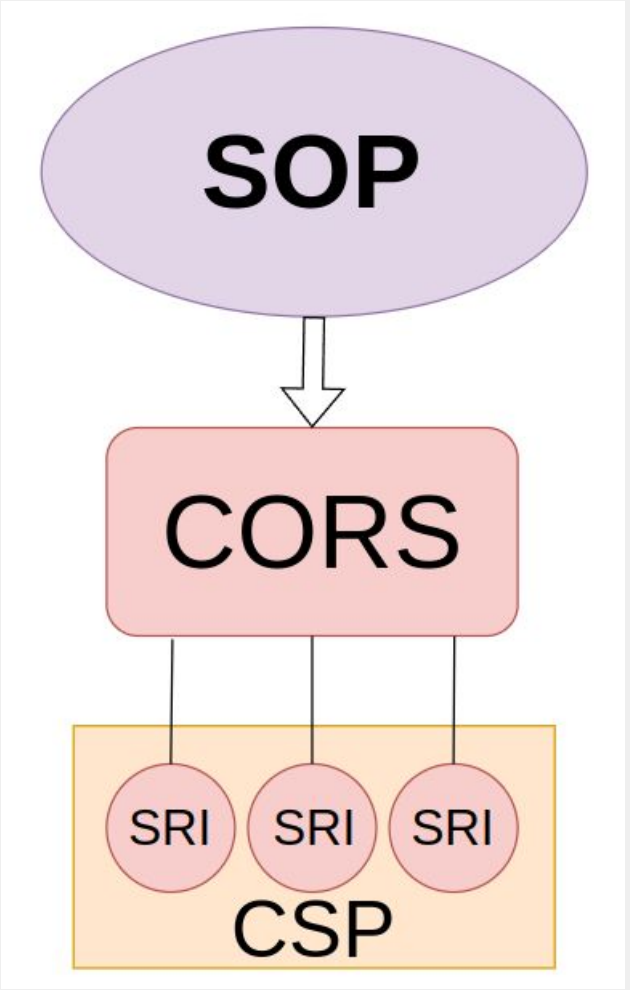




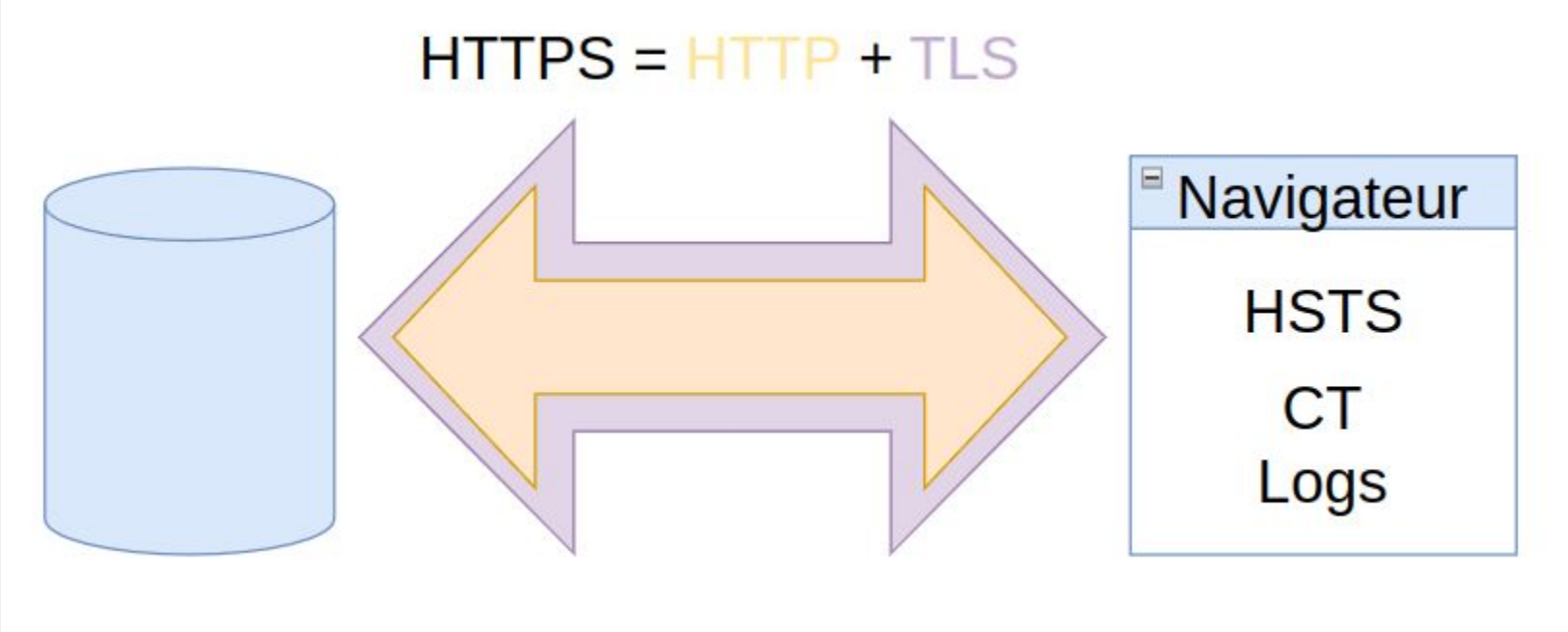
Introduction



La protection navigateur

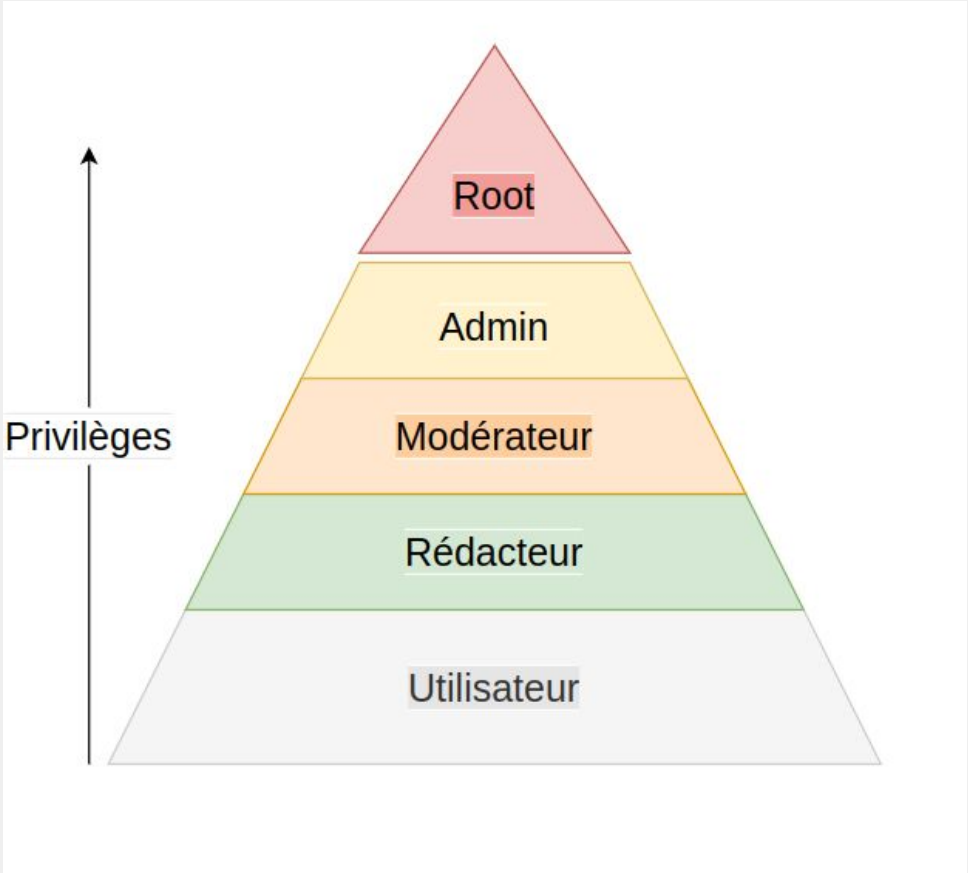


Les protocoles de sécurisation de l'échange de donnée

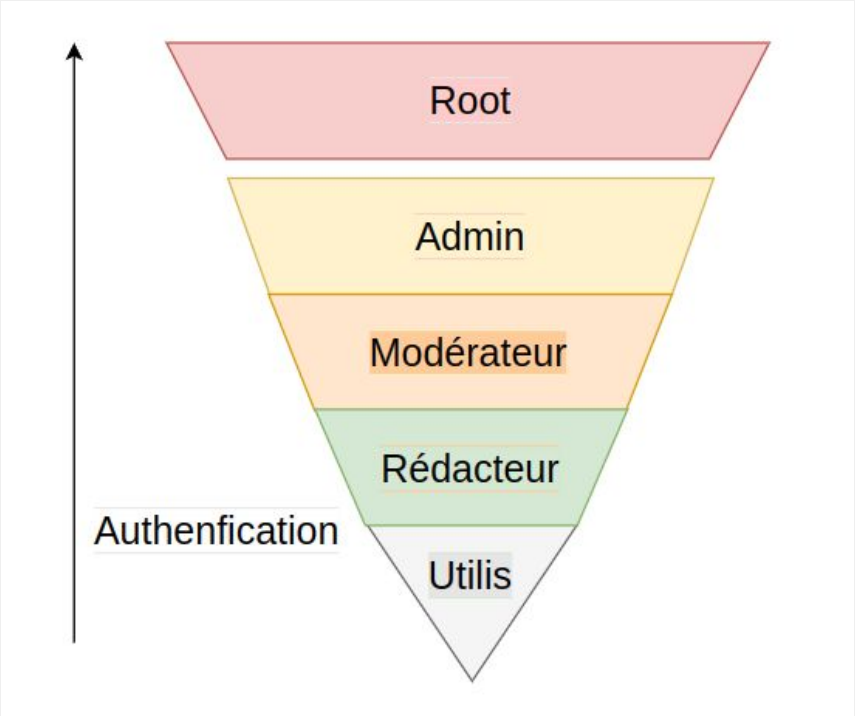


L’accès aux données

RBAC : *Role Based Access Control*

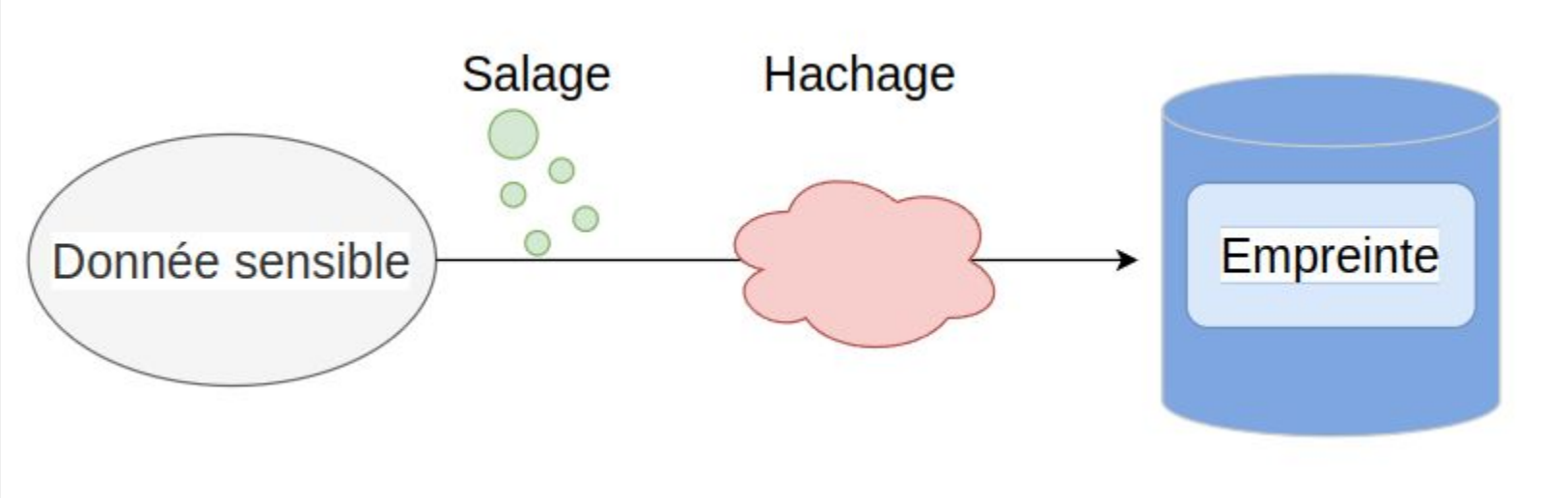


Authentification, session et token



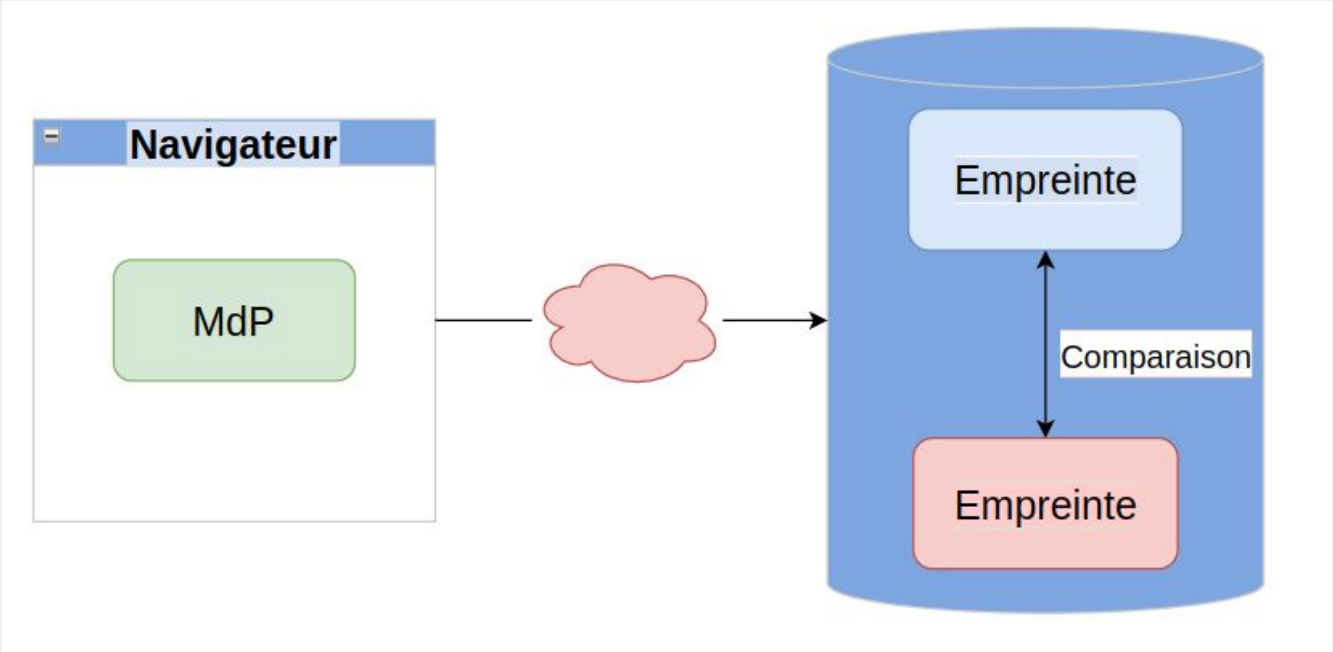
Hachage, salage et gestion des mots de passe

- La fonction de hachage:

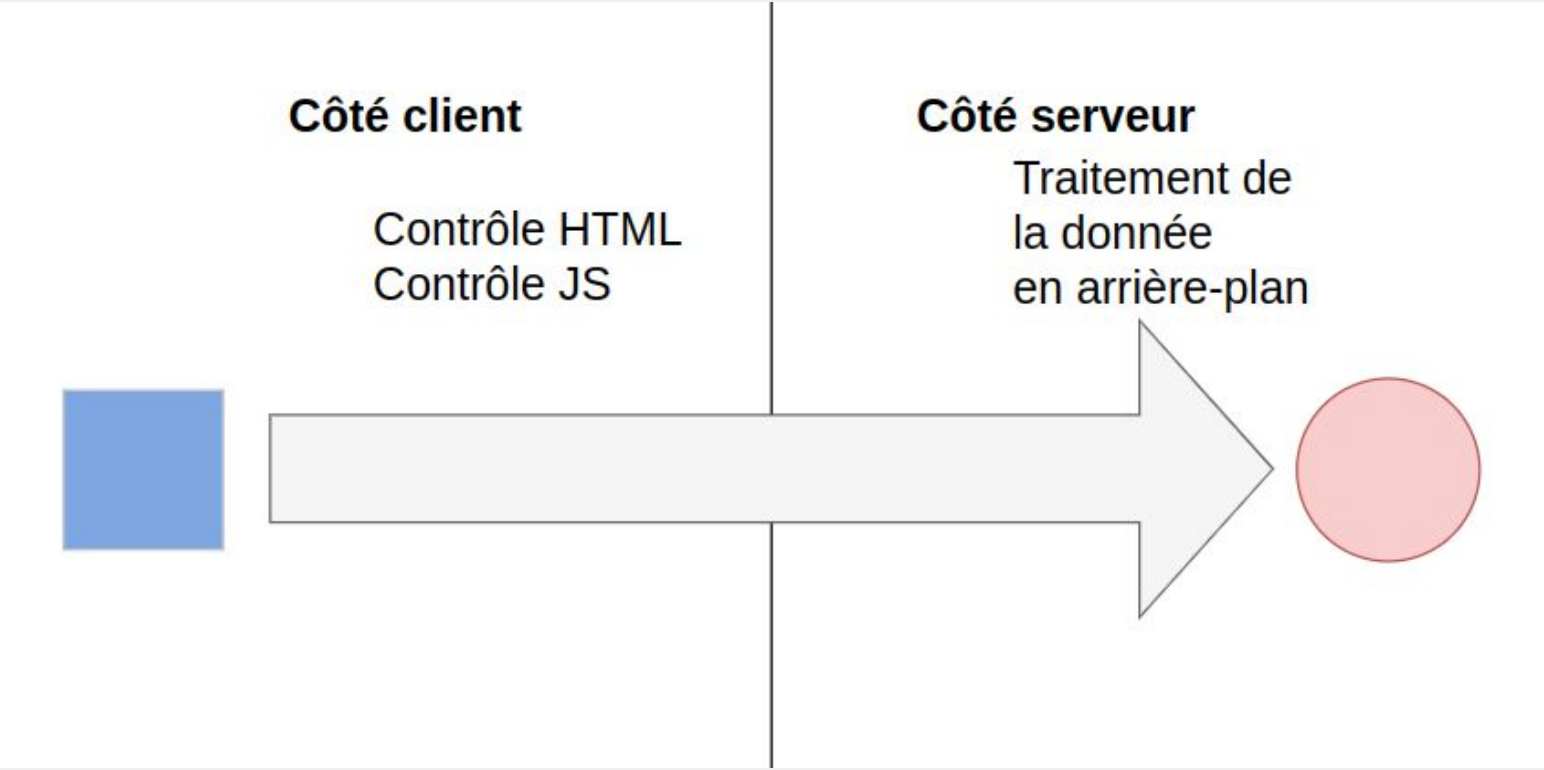


Hachage, salage et gestion des mots de passe

- La gestion des mots de passe :

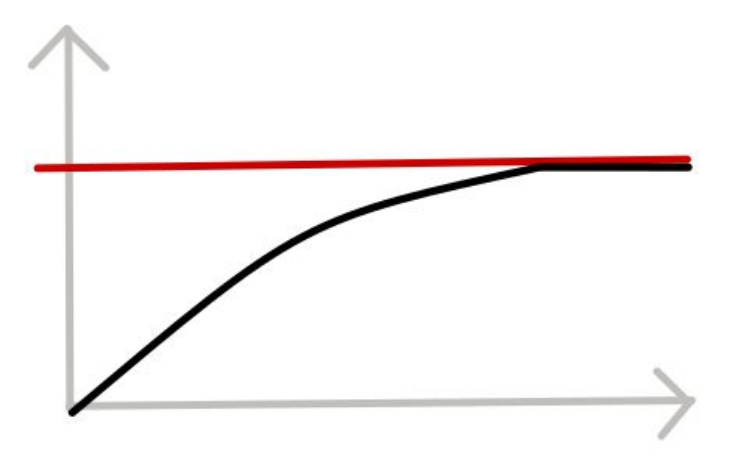


La sanitisation : Never Trust User Input!

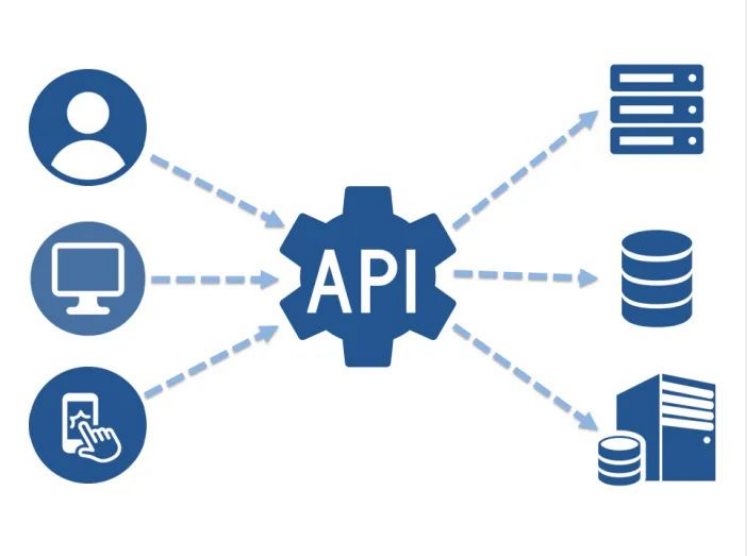


La sécurisation de l’API

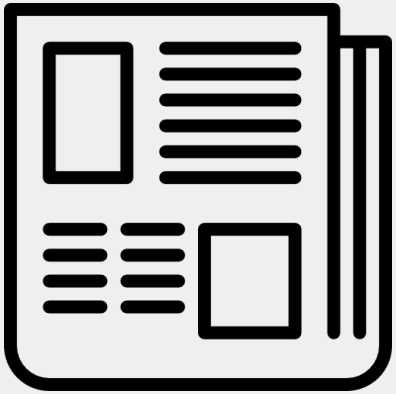
Quotas de limite d’utilisation



Utilisation d’une API Stateless



La journalisation



- Événements liés à la sécurité

- Journaux sur des périodes glissantes de 6 mois (recommandations ANSSI)

- Implications :
  - Information
  - Protection
  - Procédures

Sécurisation en phase finale et maintenance

- Phase de **Bug Bounty**:

- Audit **PASSI** :

VISA DE SÉCURITÉ

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Conclusion

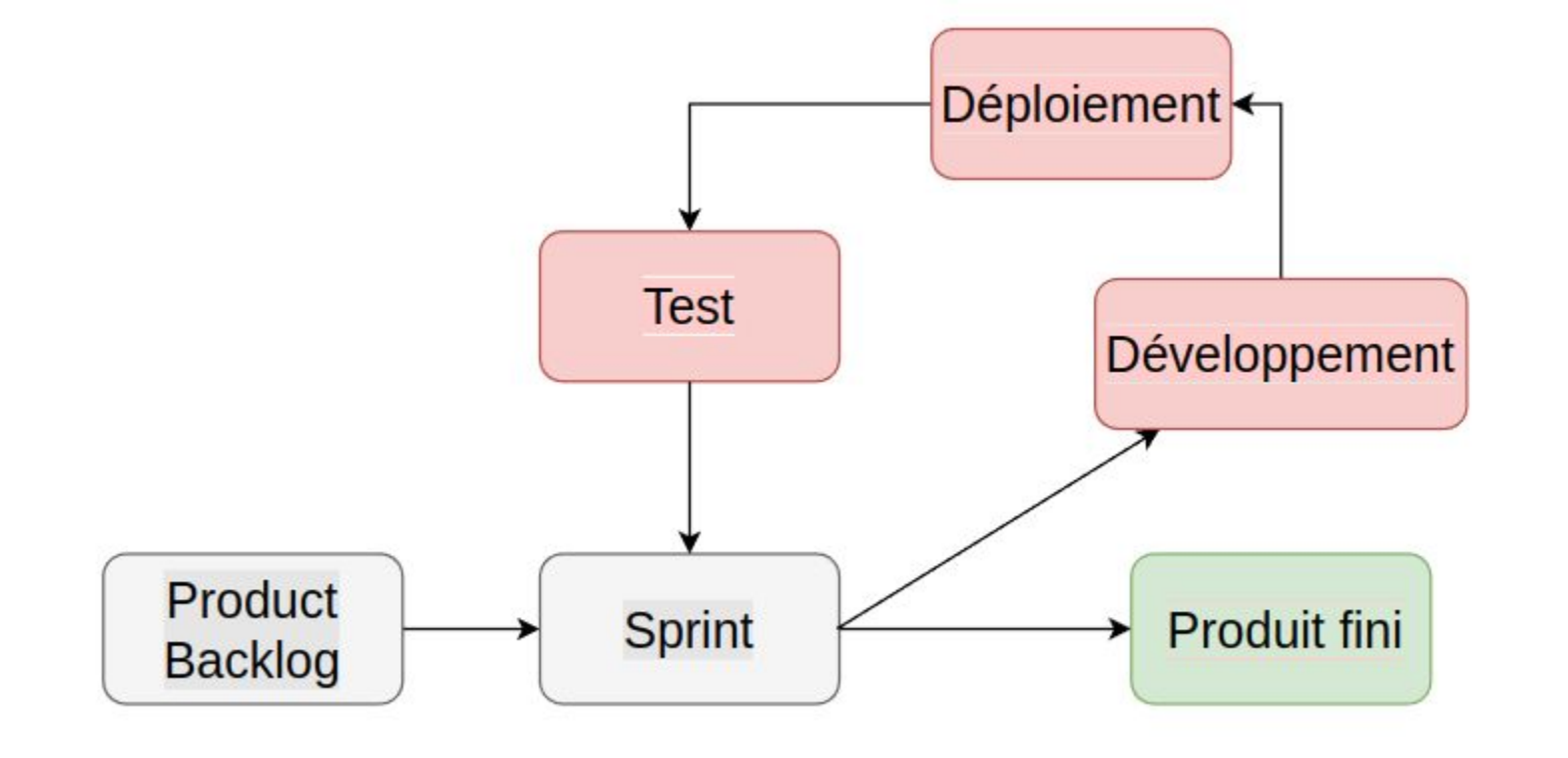

Déploiement
Test
Développement
Product Backlog
Sprint
Produit fini

Schéma supplémentaire