# Proposition de sécurisation d'une application

Présentée par Rim Idrissi zouggari

# Sommaire

# Sécuriser un système

RGPD : Règlement Général sur la Protection des Données

**moindre privilége:**limiter les permission d'accès au API A interface de programmation d'application

**La réduction de la surface d'attaque**(au niveau : de reseau, systéme (désactivation des services non necessaires dans la configuration exemple désactivé FTP un serveur qui permet de transférer des fichier par internet , d'application (Eloinier les composants non necessaire par exemple tous qui est réservé au developpement (module proxy , bibliothéque....) )

**Défense en profondeur**

# Pourquoi ?

- Il existe de nombreuses failles :
- XSS (Cross-site scripting)
- SQLI (SQL injection)

**Scénarios d'attaque :**

- Redirection vers un autre site (concurrent, phishing, etc.)
- Vol de sessions
- Modification de la page visitée

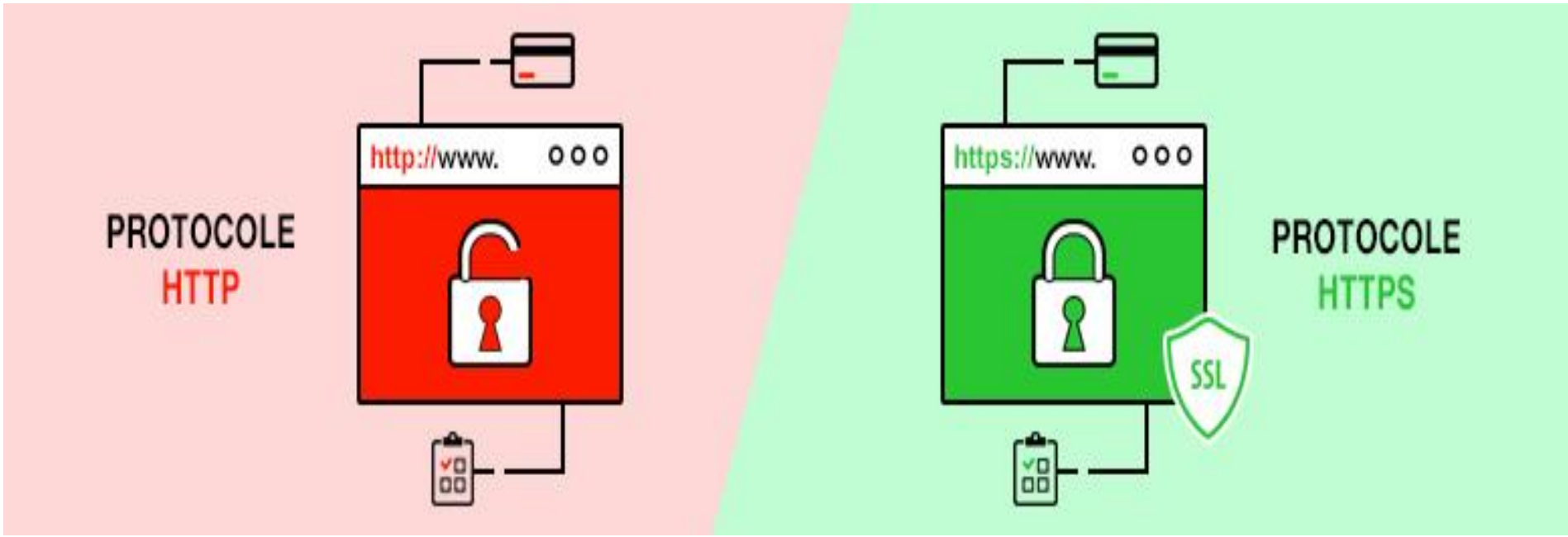
**Scénarios d'attaque :**

- Contourner l'authentification
- Accès en lecture / écriture à la BDD
- Permettre l'exécution de commande système

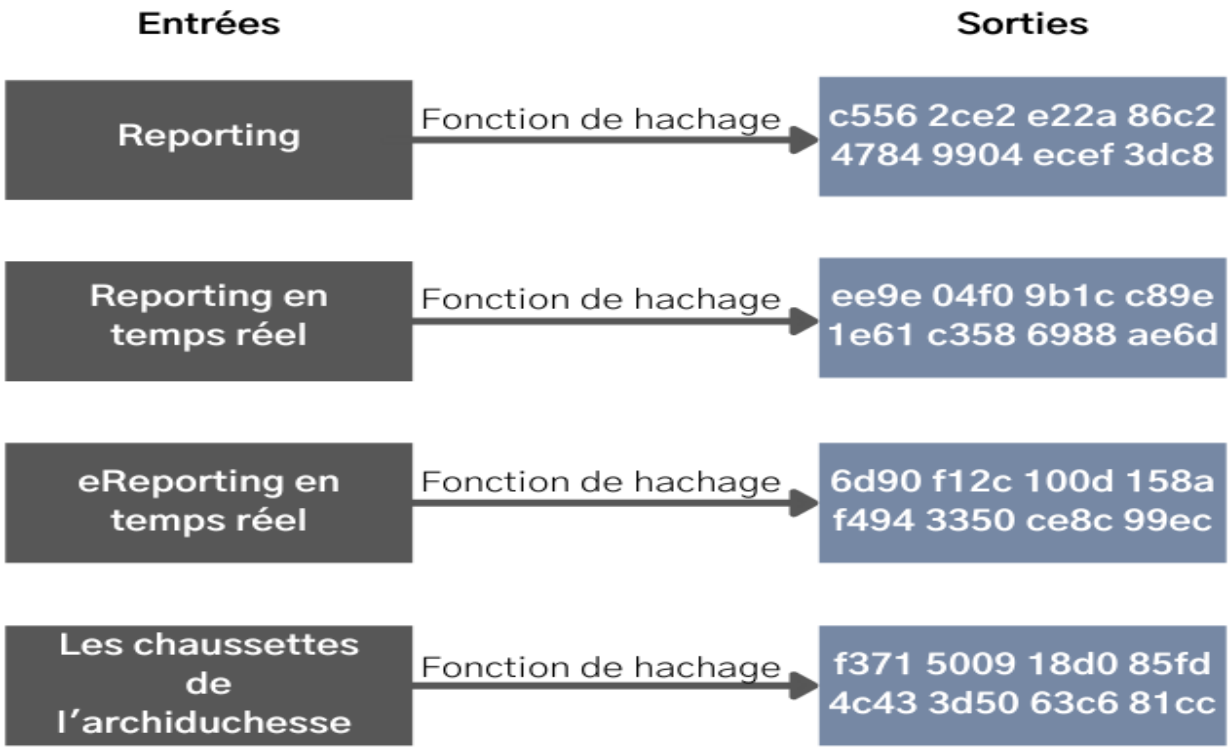
**Recommandations :**

- Utiliser les requêtes paramétrées / Utiliser les procédures stockées
- Utiliser une validation des entrées par liste blan
- Respecter le principe de moindre privilège

# la mise en place du protocole HTTPS



# Hachage


Entrées
Sorties
Reporting
Fonction de hachage
c556 2ce2 e22a 86c2
4784 9904 ecef 3dc8
Reporting en temps réel
Fonction de hachage
ee9e 04f0 9b1c c89e
1e61 c358 6988 ae6d
eReporting en temps réel
Fonction de hachage
6d90 f12c 100d 158a
f494 3350 ce8c 99ec
Les chaussettes de l'archiduchesse
Fonction de hachage
f371 5009 18d0 85fd
4c43 3d50 63c6 81cc

# La protection navigateur

- SOP: same Origin Policy : objectif de fournir un cadre de controle des interaction
- ==impose des restriction dans la communication entre composants lorsque ceux ci on des origins différent

- CORS : Cross-Origin Resource Sharing spécifie les conditions d'acceptation d'echange ==>contourner SOP la sécurité par default du navigateur
- ==> afin de permettre l'appel de ressource controler par la stratégie CSP (la liste blanche ) en dehor de l'Original

# Politique de mots de passe

# Sanitization


# Sécurisation de l'authentification

# La sécurisation API (Interface de programmation)

merci