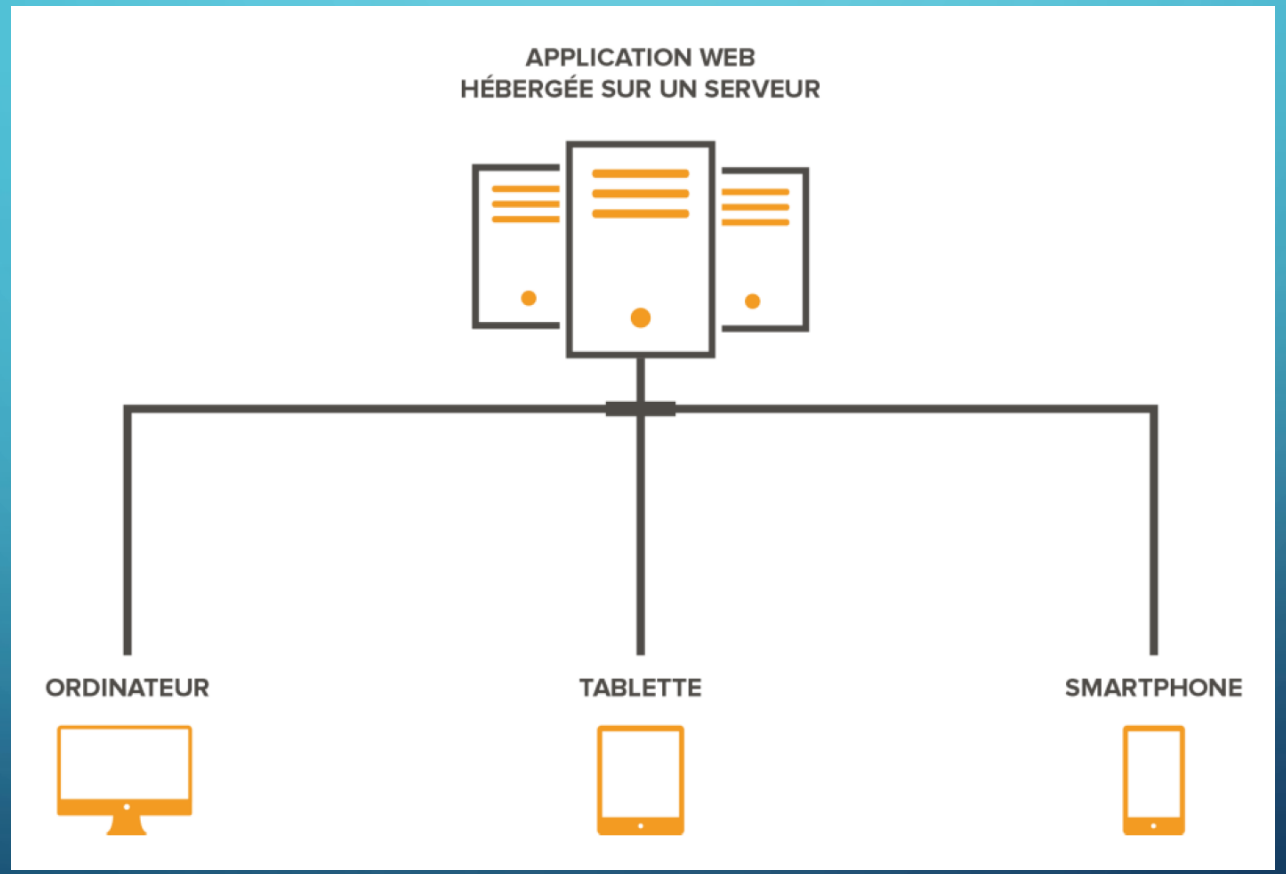
VEILLE TECHNOLOGIQUE

LA SÉCURITÉ DES DONNÉES WEB POUR UN DÉVELOPPEUR

LA SÉCURITÉ DES DONNÉES WEB POUR UN DÉVELOPPEUR

- Qu'est-ce qu'une application Web ?
- Les principales failles de sécurité des applications Web
- Solutions à ses attaques

QU'EST-CE QU'UNE APPLICATION WEB

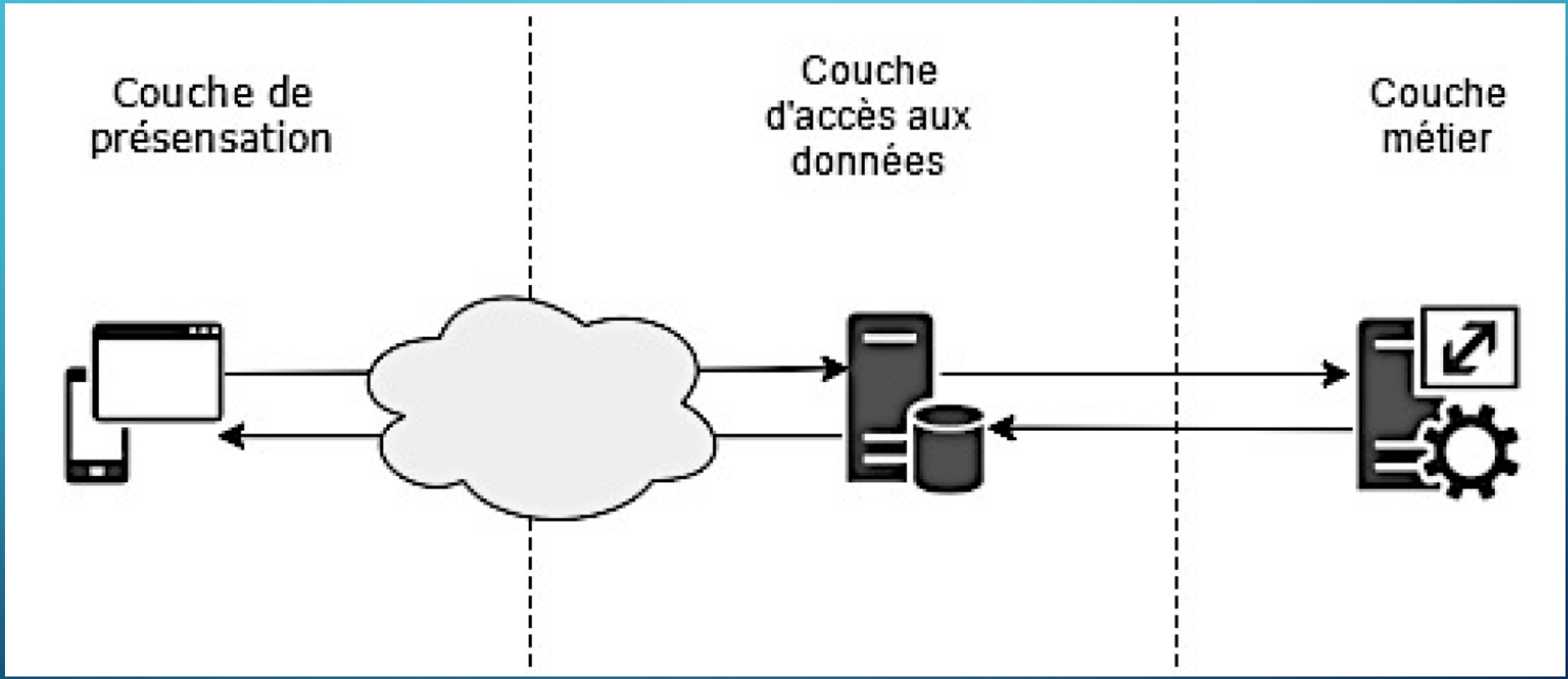


DEUX TYPOLOGIES

Orienté présentation

Orienté service

ARCHITECTURE



OWASP

VALEURS FONDAMENTALES DE L'OWASP

OUVERT

INNOVATION

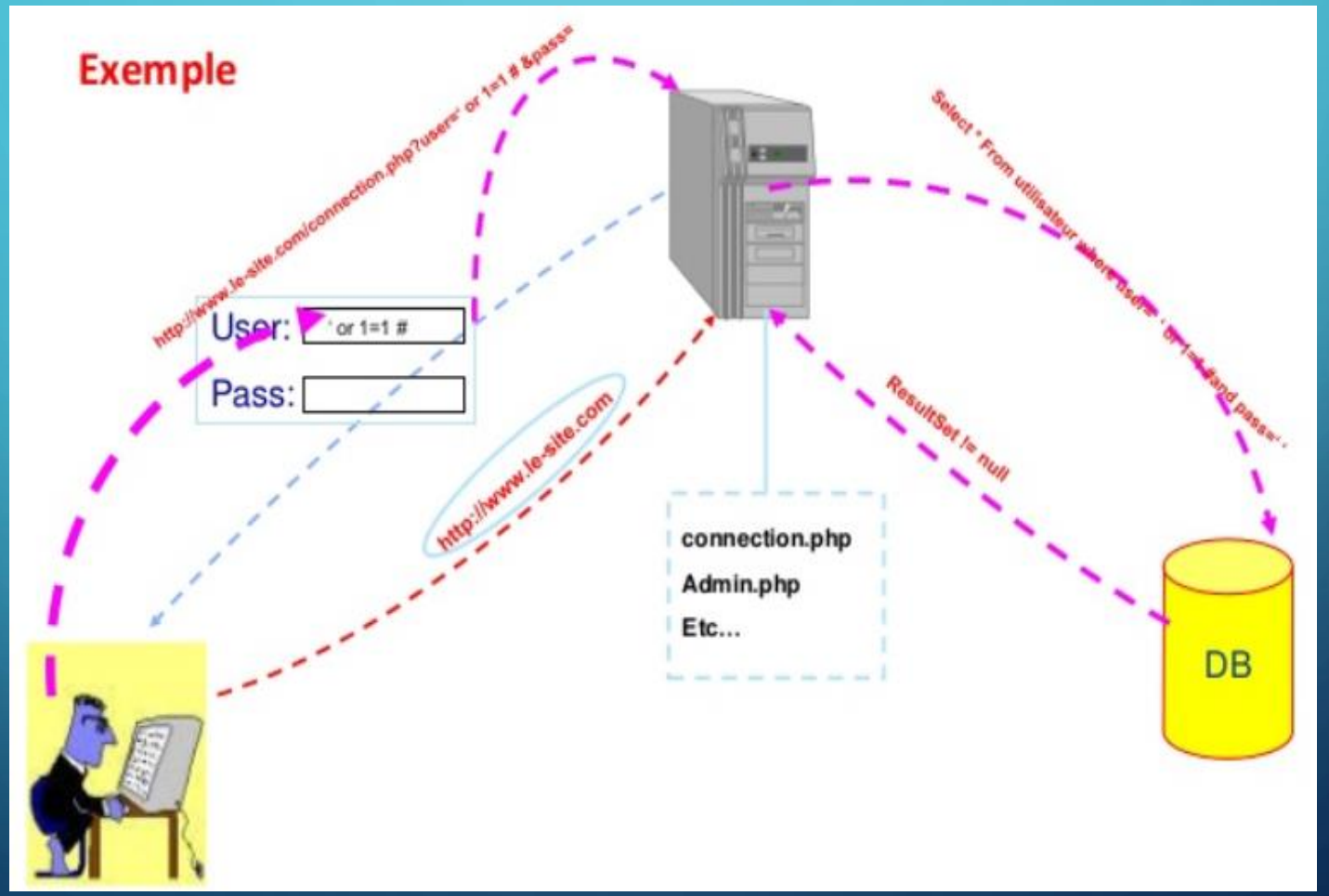
GLOBAL

INTEGRITÉ

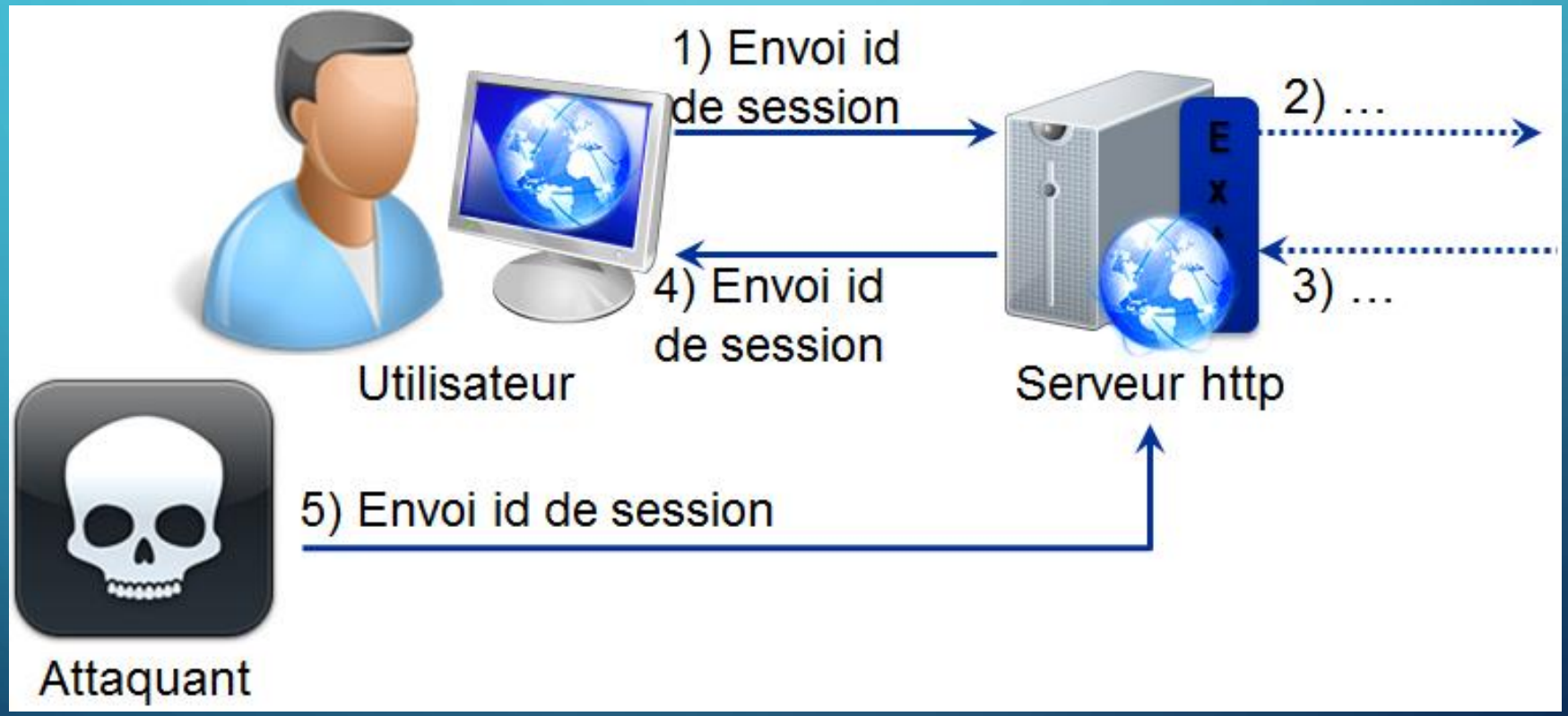
LES 10 FAILLES DE L'OWASP

- Injection SQL
- Violation des gestions d'authentification et de session
- Cross Site Scripting (XSS)
- Violation de contrôle d'accès
- Mauvaise configuration de sécurité
- Exposition des données sensibles
- Protection insuffisante contre les attaques
- Falsification des requêtes intersites
- Utilisation des composants avec des vulnérabilités connues
- APIs non sécurisées

INJECTION SQL



VIOLATION DES GESTIONS D'AUTHENTIFICATION ET DE SESSION



CROSS SITE SCRIPTING (XSS) – DEUX TYPES

XSS réfléchis

Non permanente

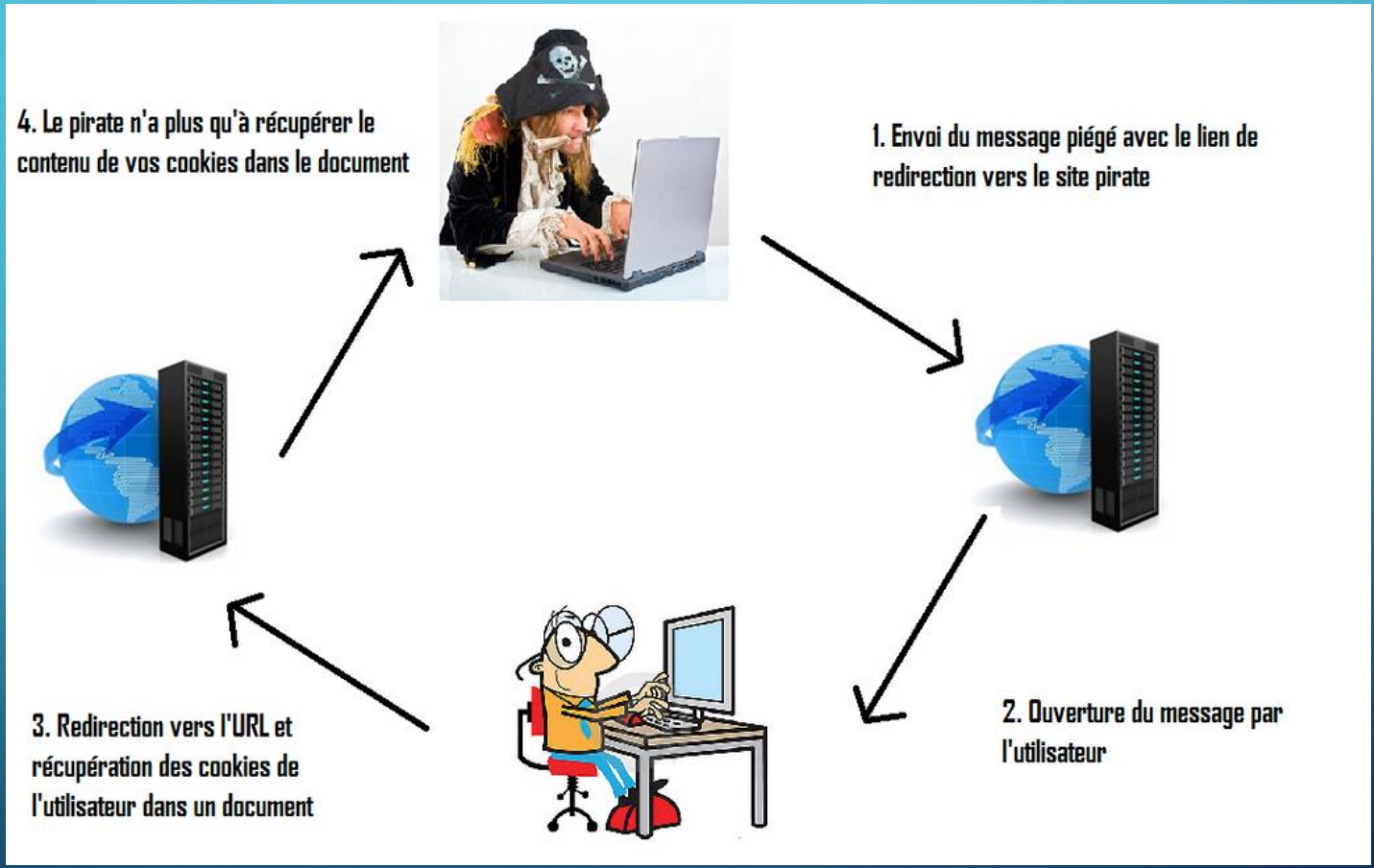
Non enregistré dans un fichier ou dans une base de données (ex : Se connecter à son espace)

XSS stockées

Permanente

Sauvegarder dans un fichier ou dans une base de données (ex : Poster un commentaire)

CROSS SITE SCRIPTING (XSS)



SOLUTIONS À SES ATTAQUES

Injection SQL

Il suffit d'utiliser des requêtes préparées.

Cross Site Scripting (XSS)

Utiliser la fonction htmlspecialchars() . Cette fonction permet de filtrer les symboles du type <, & ou encore ", en les remplaçant par leur équivalent en HTML.

Violation des gestions d'authentification et de session

Mettre à disposition du développeur un ensemble unique de contrôles destinés à la gestion des sessions et des authentifications.

Mettre en œuvre des mesures efficaces pour éviter les failles XSS, particulièrement utilisées pour voler les ID de session.

OUTILS PERMETTANT DE CONTRÔLER LA SÉCURITÉ DES APPLICATIONS

NAXSI