LA SÉCURITÉ DES DONNÉES WEB POUR UN DÉVELOPPEUR

Fabien Dennel

Sommaire

1

Application Web

Qu’est-ce qu’une application Web ?

2

Failles de sécurité

Les principales failles de sécurite´des applications Web.

3

Solutions

Solutions a`ses attaques

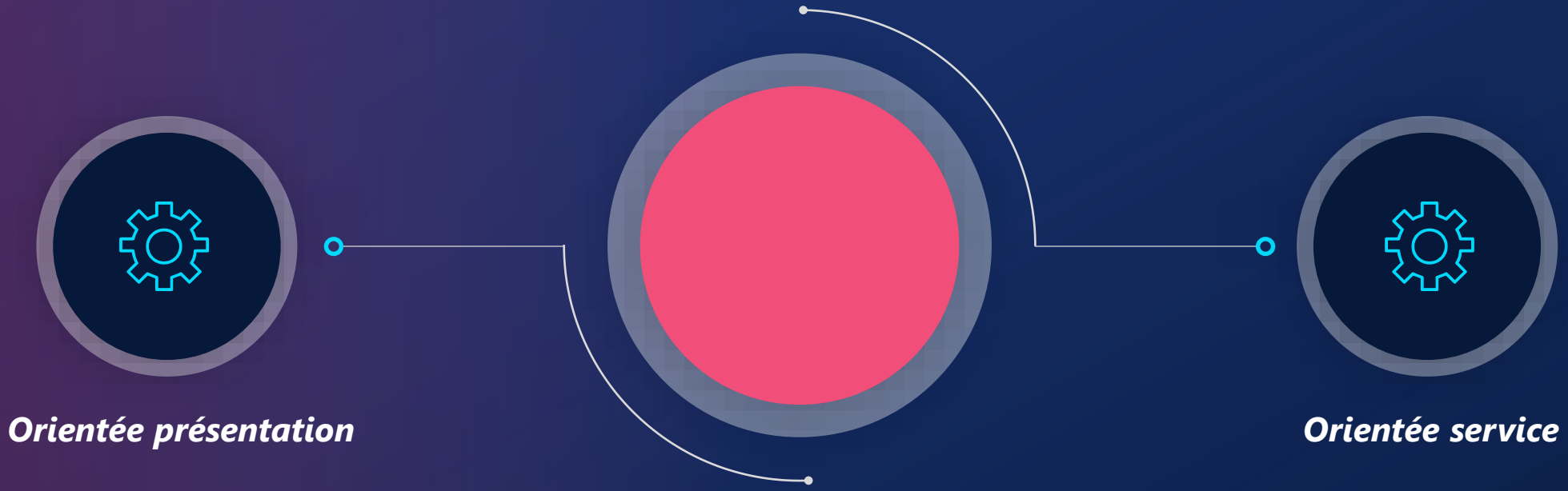
Introduction

Depuis quelques années, développer un site web est devenu très accessible. De plus en plus de gens se lancent dans la réalisation de leur propre page. Mais très peu sont informés sur les vulnérabilités présentes dans leur réalisation (plus couramment appelées failles), et cela peut s'avérer très dangereux.

Application Web

Une application web désigne un logiciel applicatif hébergé sur un serveur et accessible via un navigateur web.

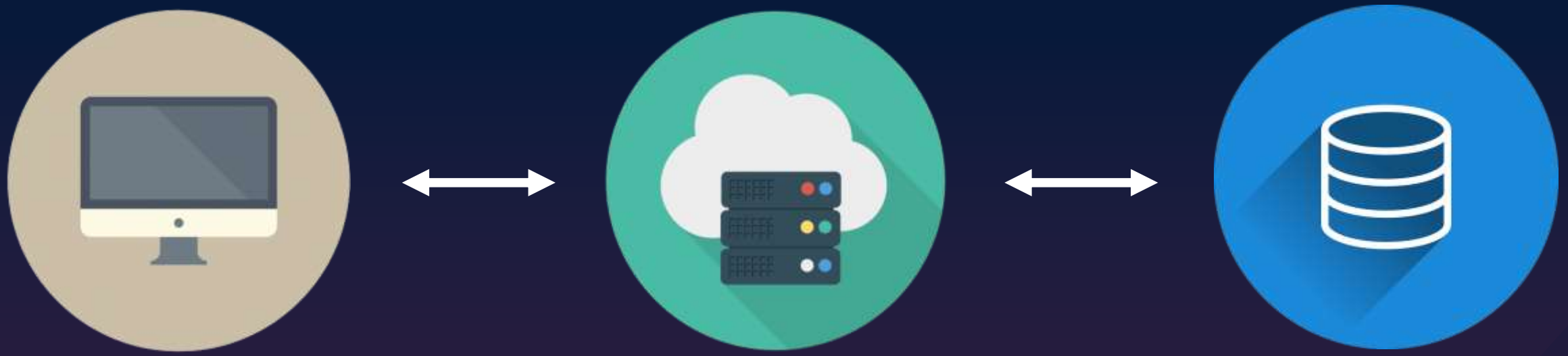
DEUX TYPOLOGIES



Orientée présentation

Orientée service

Architecture



Couche de présentation

Couche métier

Couche d'accès aux données

OWASP

Failles de sécurité

Top 10 des risques de sécurité des applications.

#1 *Contrôles d'accès défaillants*

#2 *Exposition de données sensibles*

#3 *Injection SQL*

#4 *Conception non sécurisée*

#5 *Mauvaise configuration de sécurité*

#6 *Composants vulnérables et obsolètes*

#7 *Identification et authentification de mauvaise qualité*

#8 *Manque d'intégrité des données et du logiciel*

#9 *Carence des systèmes de contrôle et de journalisation*

#10 *Falsification de requête côté serveur*

Contrôles d'accès défaillants

Shéma du mécanisme d'authentification des applications Web

L'utilisateur non authentifié demande l'accès à une page Web

Le serveur Web fait appel à un service pour vérifier la validité de l'identifiant/mot de passe

Le serveur renvoie une page d'authentification

L'utilisateur remplit le formulaire en fournissant un identifiant et un mot de passe

Utilisateur

Serveur Web

Exposition de données sensibles

Liste des données sensibles

Origine raciale ou ethique

Orientations sexuelles

Convictions religieuses ou philosophiques

Opinions politiques

Opinions syndicales

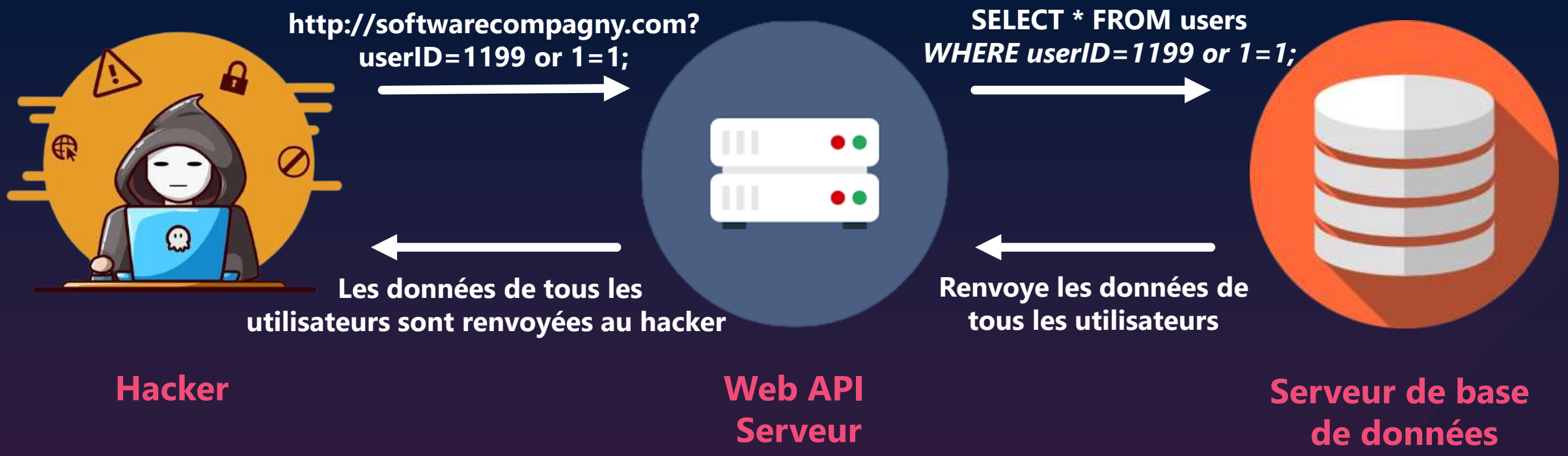
Etat de santé

Données biométriques

Données génétiques

Condannations pénales et infractions

Injection SQL



Solutions à ses attaques

Contrôles d'accès défaillants

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

Injection SQL

Il suffit d'utiliser des requêtes préparées.

Exposition de données sensibles

-Collecter seulement les informations des utilisateurs nécessair.

-Identifier les données sensibles, et s’assurer qu’elles sont cryptées avec un algorithme.

-S’assurer que des algorithmes récents et reconnus sont utilisés pour crypter/hacher les données.

Merci pour votre écoute