React JS

Qu'est-ce que c'est

Qu'est-ce que c'est

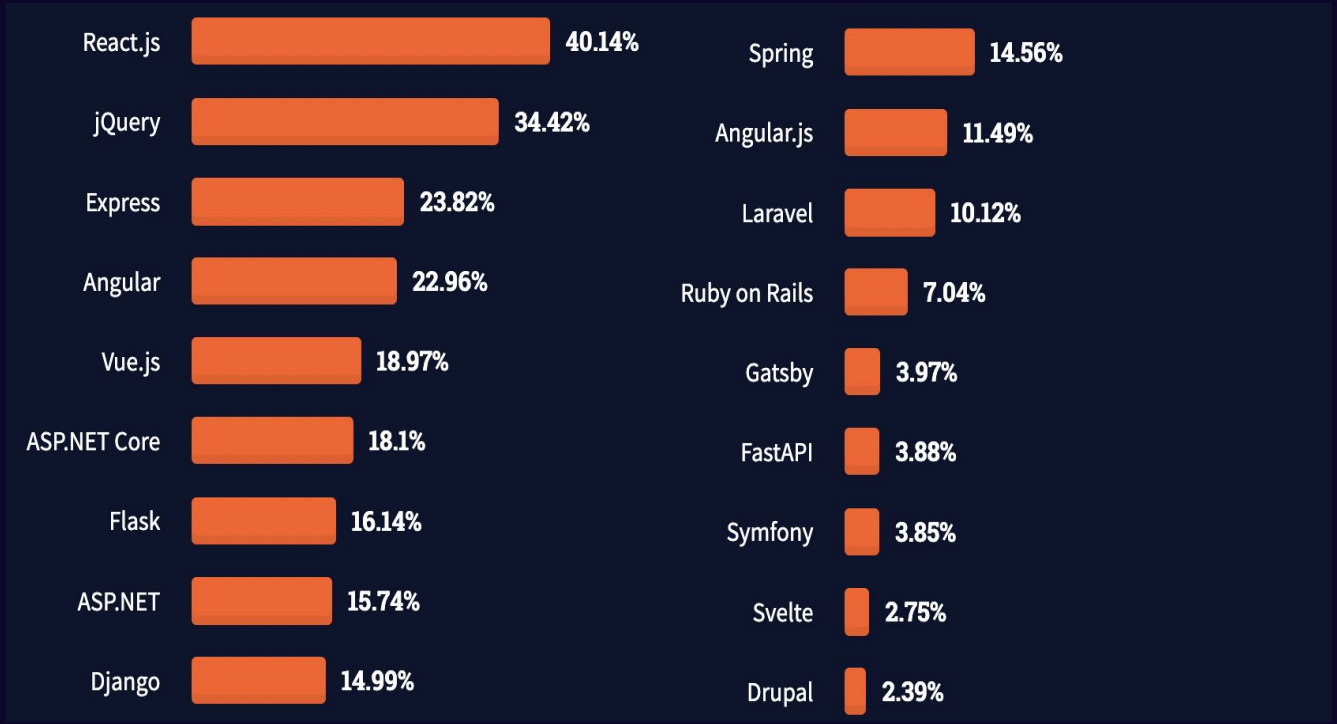
Une bibliothèque JavaScript open-source pour créer des interfaces utilisateur

Crée par Jordan Walke, développé par Facebook et disponibilisé publiquement le 29 avril 2013

Maintenu par Meta (anciennement Facebook) et une communauté de développeurs individuels et d'entreprises

Popularité des frameworks web

Enquête Stack Overflow 2021 - 67,593 responses

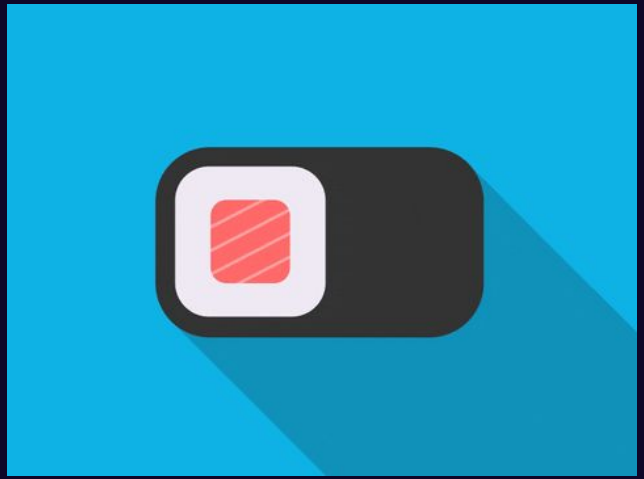


Point Principaux

- Interface utilisateur déclarative
- Architecture à base de composants
- Simple et rapide
- Flexible

Interface Utilisateur Déclarative

React facilite la création d'interfaces utilisateur interactives, concevant des vues simples pour chaque état de l'application, et la mettant à jour lorsque les données changent. Cela est possible grâce au DOM virtuel.



Interface Utilisateur Déclarative

DOM = Document Object Model

Il définit la structure logique des documents et la manière dont un document est accessible et manipulé.

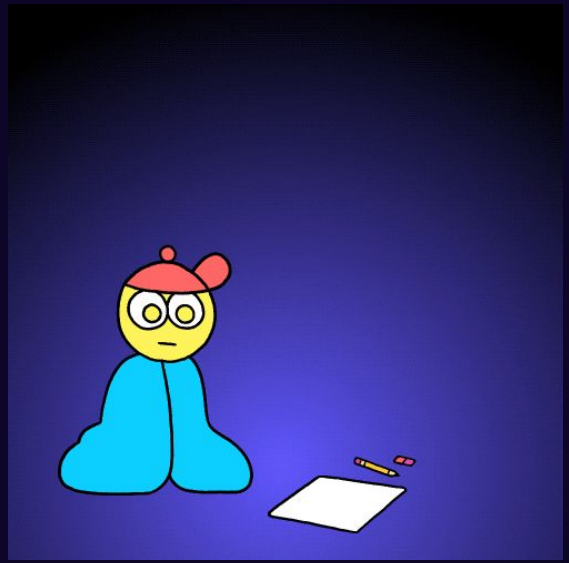
VDOM = Virtual DOM

Le DOM virtuel est un concept de programmation dans lequel une représentation idéale ou "virtuelle" d'une interface utilisateur est conservée en mémoire et synchronisée avec le "vrai" DOM par une bibliothèque telle que ReactDOM.

Ce processus s'appelle la réconciliation.

Basé sur les composants

React nous permet de créer des composants encapsulés qui gèrent leur propre état, et ainsi crée des interfaces utilisateur complexes.



Basé sur les composants

Ont peut facilement transmettre des données riches via l'application et garder l'état hors du DOM.

Ce qui facilite le debug et la gestion du code.

Simple et Rapide

Grande communauté avec plein d'exemples et solutions.

React as des fonctions pré-construites.

C'est possible de démarrer un projet rapidement et facilement.

Flexible

C'est possible de l'utiliser dans un projet déjà existant, petit à petit.

On peut utiliser des composants de tiers et les adapter.

Ont peut facilement intégrer avec d'autres technologies.

Sites web qui utilisent ReactJS

React Native

NextJS

- Crée par Vercel

- SEO:
  - SSG (Static Site Generation)

  - SSR (Server Side Rendering) vs CSR (Client Side Rendering)

- Next gagne énorme popularité entre les application web React

Sécurité

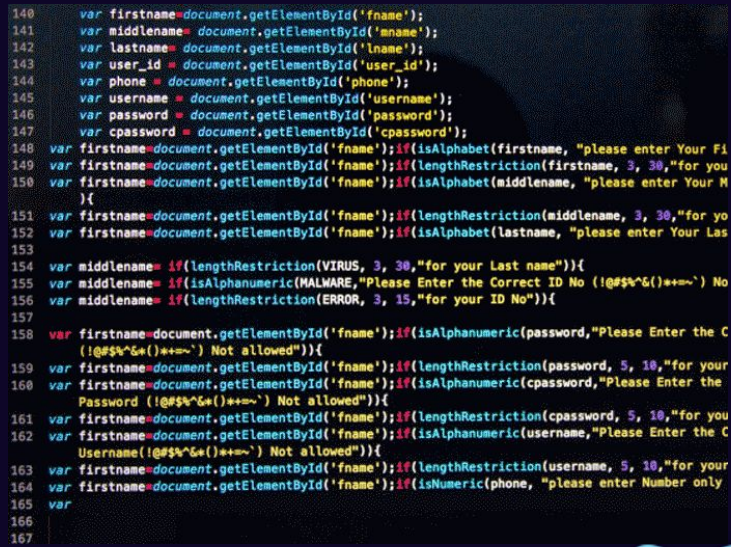
1. Grande % du code de tiers
2. Cross-site Scripting (XSS)
3. Broken Authentication
4. SQL Injection
5. XML External Entity Attack (XXE)
6. Zip Slip

Code de Tiers

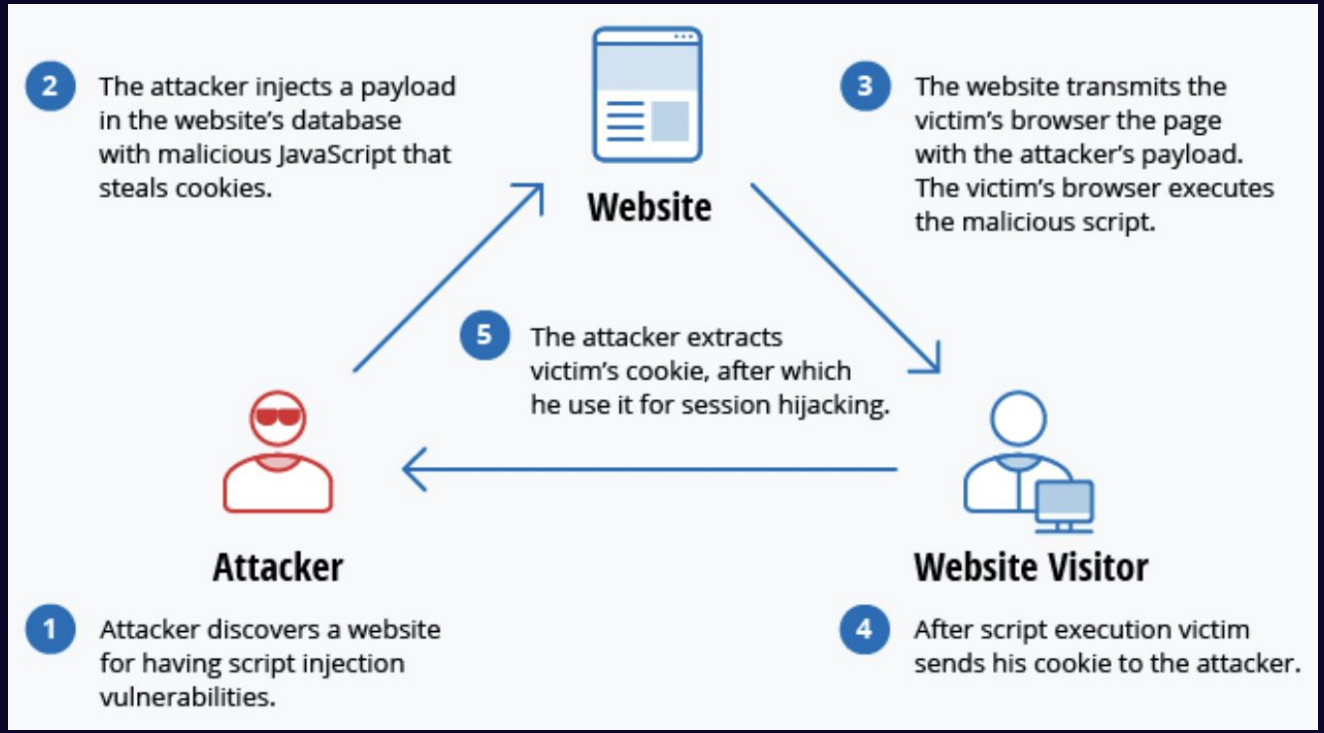
Il faut se méfier des codes dont on ne connaît pas les sources.

Ont doit se maintenir au courant.

Ont doit prendre les message de GitHub oú d'un autre référentiel Git très sérieusement.



Cross-site Scripting (XSS)

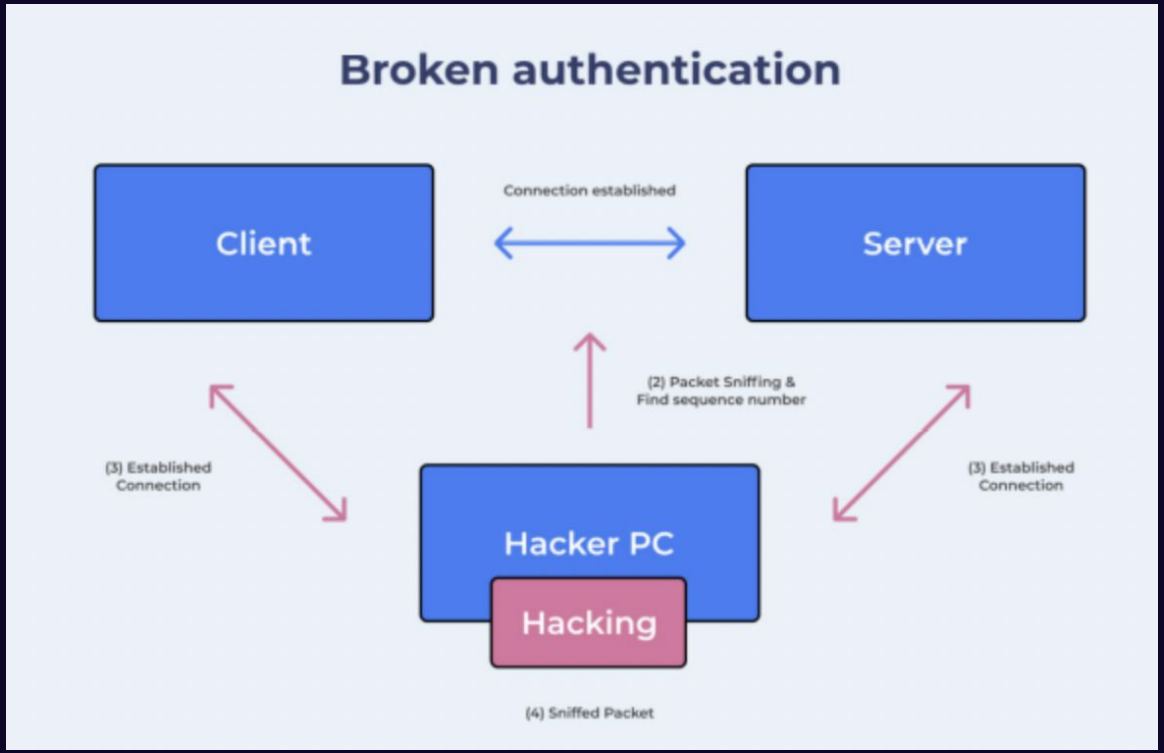


Cross-site Scripting (XSS)

XSS se produit lorsqu'un attaquant injecte des scripts malveillants côté client dans les applications Web. Ces scripts seront très probablement exécutés en tant que code légitime et l'attaquant pourrait obtenir le contrôle sur l'application.
Il existe plusieurs types de XSS attack, comme attaques DOM, stockage et réfléchissant.

Pour se défendre les développeurs doivent comprendre comment valider les données que l'utilisateur va introduire dans un input, et faire très attention avec dangerouslySetInnerHtml() par exemple.

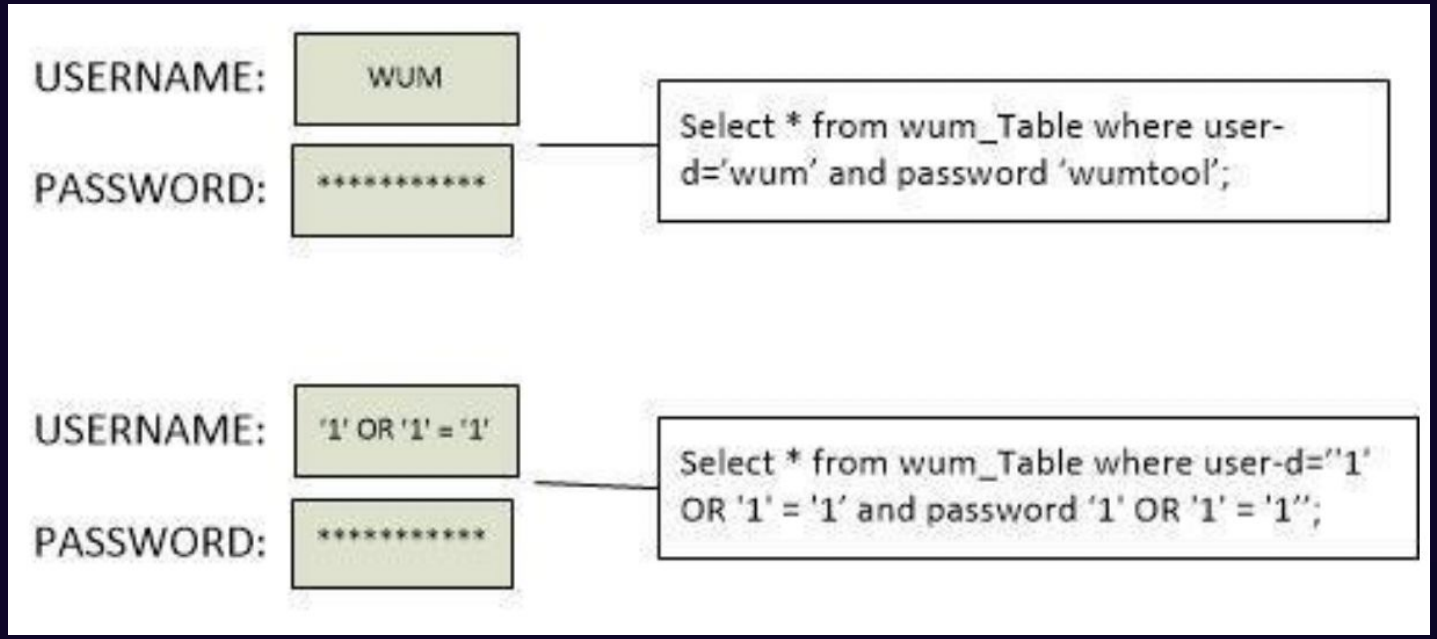
Broken Authentication



Broken Authentication

Les attaques par authentification brisée visent à prendre le contrôle d'un ou plusieurs comptes en donnant à l'attaquant les mêmes privilèges que l'utilisateur attaqué.
L'authentification est « rompue » lorsque les attaquants sont en mesure de compromettre les mots de passe, les clés ou les jetons de session, les informations de compte d'utilisateur et d'autres détails pour assumer l'identité des utilisateurs.

SQL Injection



SQL Injection

SQL = Standard Query Language

Une attaque par injection SQL consiste en l'insertion d'une requête SQL via les données d'entrée du client vers l'application. Un exploit d'injection SQL peut lire des données sensibles de la base de données, modifier les données, exécuter des opérations d'administration (comme l'arrêt du SGBD), récupérer le contenu d'un fichier et, dans certains cas, envoyer des commandes au système d'exploitation.

L'attaque d'entité externe XML (XXE)

XML = eXtensible Markup Language

L'attaque d'entité externe XML est un type d'attaque contre une application qui analyse l'entrée XML. Cette attaque se produit lorsqu'une entrée XML contenant une référence à une entité externe est traitée par un analyseur XML mal configuré.

Zip Slip

Zip Slip est une vulnérabilité d'extraction d'archive critique répandue, permettant aux attaquants d'écrire des fichiers arbitraires sur le système, entraînant généralement l'exécution de commandes à distance.

Arbitrary Code Execution

Une exécution de code arbitraire (ACE) provient d'une faille logicielle ou matérielle. Un pirate détecte ce problème, puis il peut l'utiliser pour exécuter des commandes sur un appareil cible.

Merci pour votre attention

Ressource

- https://reactjs.org/
- https://reactjs.org/docs/faq-internals.html
- https://en.wikipedia.org/wiki/React_(JavaScript_library)
- https://insights.stackoverflow.com/survey/2021?_ga=2.235361217.1154405696.1654427774-862332690.1654427774#section-most-popular-technologies-web-frameworks
- https://www.typescriptlang.org/
- https://en.wikipedia.org/wiki/TypeScript
- https://www.reactnative.com/
- https://reactnative.dev/
- https://nextjs.org/
- https://www.freecodecamp.org/news/best-practices-for-security-of-your-react-js-application/
- https://fossa.com/blog/react-security-how-fix-common-vulnerabilities/
- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/attacks/SQL_Injection