

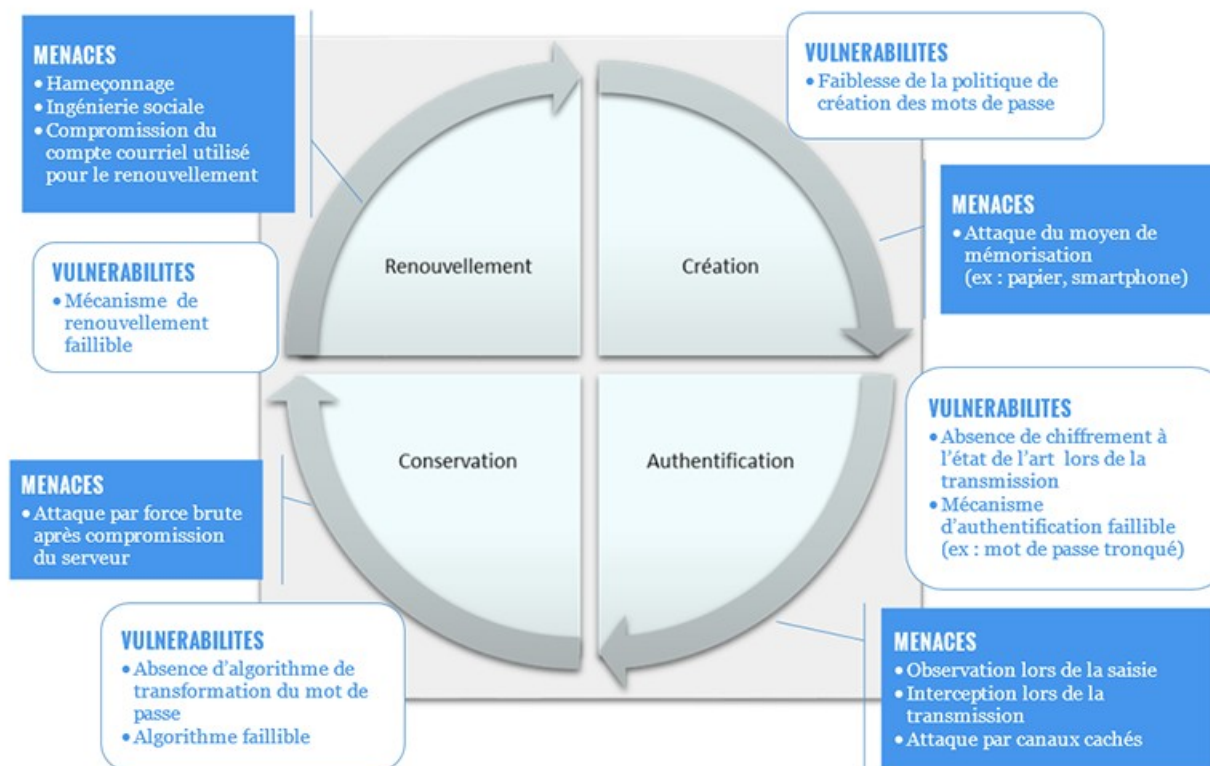
Politique d'entreprise : sécurité des applications Web

Principaux types de vulnérabilités

Sur l'Authentification : **direct et courant**

Type d'attaque : force brute (tests massifs par robots) ; variante « password spraying » (utilisation sur plusieurs comptes des mot de passes courants).

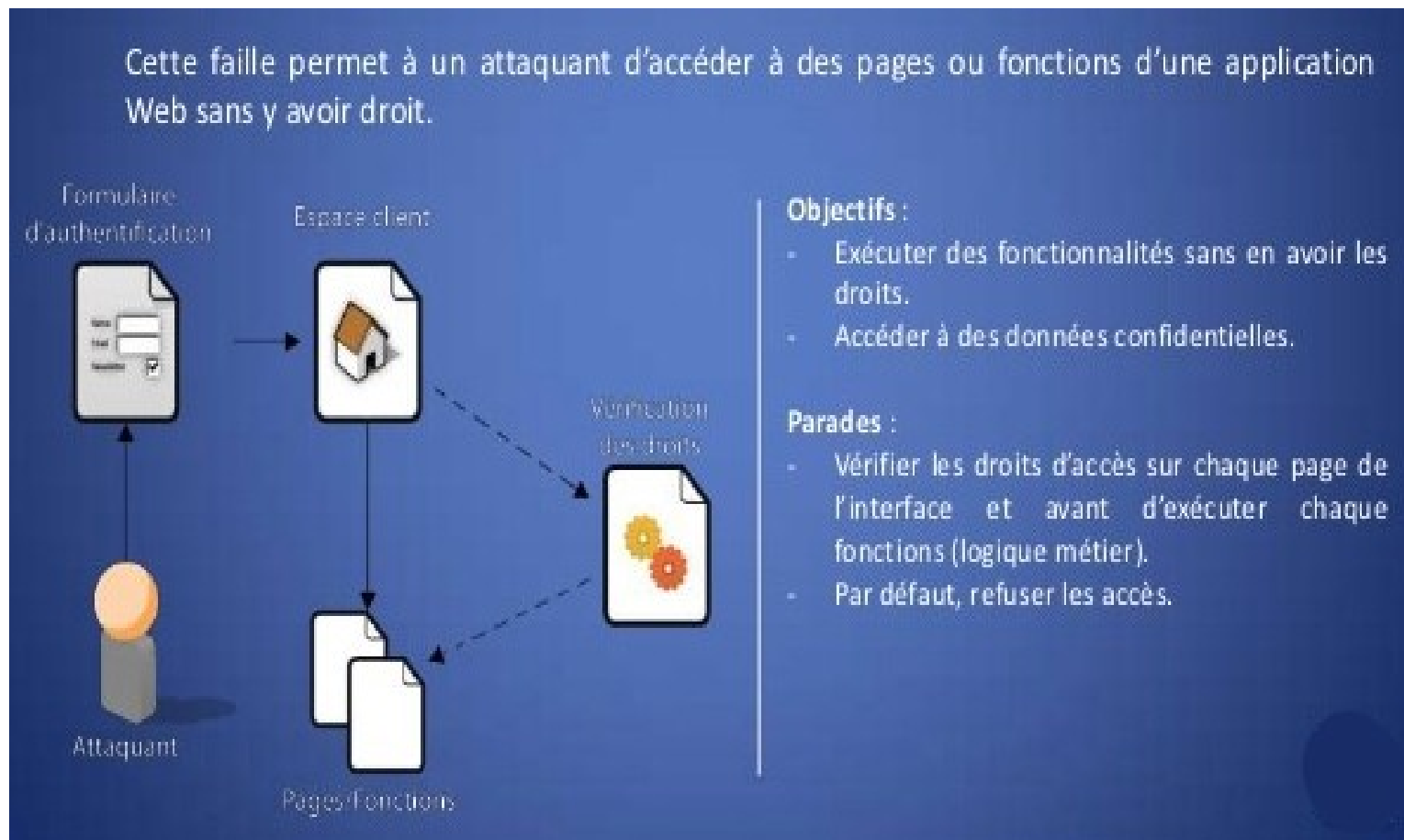
Sécurisation : limitation du nombre de connexion non valides, longueur importante des mots de passe (≥ 8), vérification de l'humain et non un « bot » (Captcha, question, etc.), vérification à double facteur...



Droits d'accès : quelle confiance à accorder ?

Type d'attaque : les utilisateurs peuvent vouloir accéder aux données d'un autre, aux fonctionnalités réservées ou payantes...

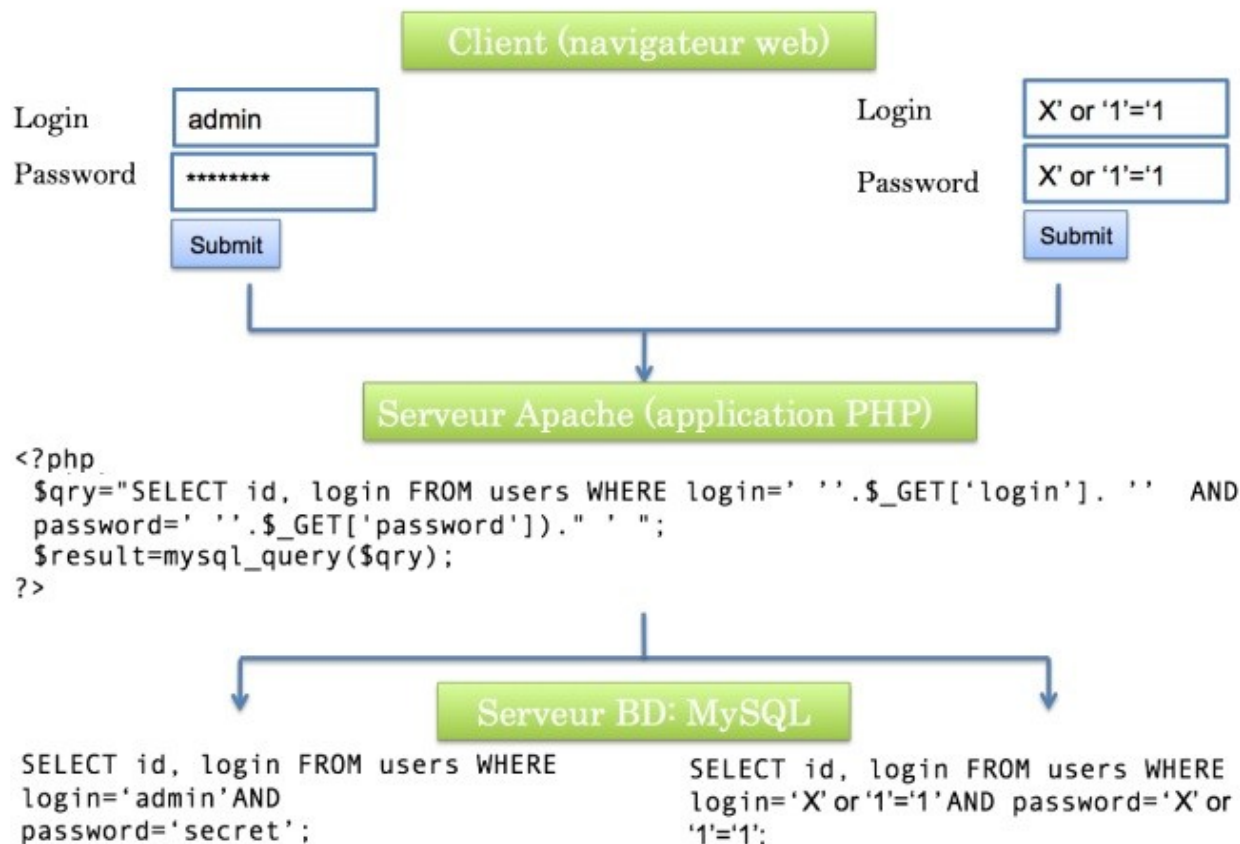
Sécurisation : vérifier la fiabilité des privilèges accordés, lecture et surveillance des logs, test d'intrusion.



Injection : contrôle et fiabilité des flux entrants

Type d'attaque : fréquentes, la plus connue étant l'injection SQL modifiant ou récupérant des données, il existe aussi l'injection de commandes systèmes, de traitements non autorisés, etc.

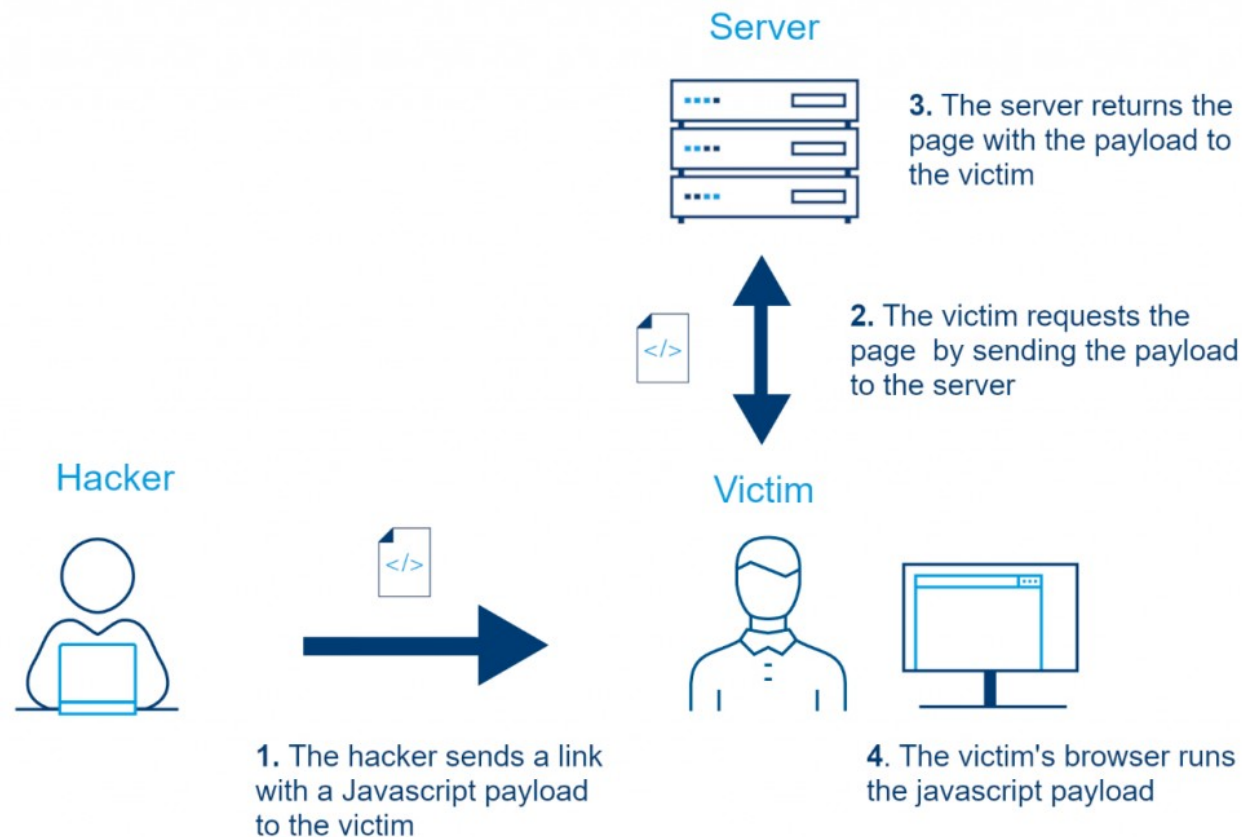
Sécurisation : utilisation de frameworks connus et fiables (pas de framework « maison », respect des mises à jour.



Failles XSS : attaque par le code JavaScript

Type d'attaque : faille XSS ou dite « Cross Site Scripting » (stockée dans la BDD ou non persistante), l'injection se fait par du code JavaScript par Front Office via les sessions, les comptes, l'upload, etc.

Sécurisation : utiliser des frameworks récents, les mieux classés, ceux disposant d'une forte communauté pour les informations.



Faible d'un service tiers : vérification de la coopération

Type d'attaque : faible des services utilisés par les applications comme les Web services ou les API (par exemple les systèmes tiers de paiement en ligne ou sans contact).

Sécurisation : recensement et contrôle périodique des services tiers, vérification des mises à jour par la veille technologique, tests de fiabilité.

Contacts Gestion de stock Paiements Rapports ? 6 Rechercher Paramètres

Modes de paiement Paramètres Notifications par email E-commerce

Pour tester le paiement, vous avez besoin d'ajouter un nouveau produit et d'activer la fonction Vente en ligne

- ☐ Virement bancaire manuel
- ☐ Paiement instantané via Braintree: carte bancaire
- ☒ Paiement instantané via PayPal: carte bancaire ou compte PayPal

Nom d'utilisateur API * Mot de passe API *

Signature *

- ☐ Paiement instantané via BitPay: Bitcoins
- ☐ Paiement instantané via Stripe : carte bancaire
- ☐ Paiement instantané via PayZen : carte bancaire
- ☐ Paiement instantané via Ingenico (carte achat et carte bancaire)

Paramètres du compte
Compagnies/Départements
Paiements en ligne
Utilisateurs
Catégories
Codes promotionnels
Historique des activités
API
Importation
Anglais
Polonais
Français
Espagnol
Allemand
Tchèque
Parrainage/Partenariat
Assistance

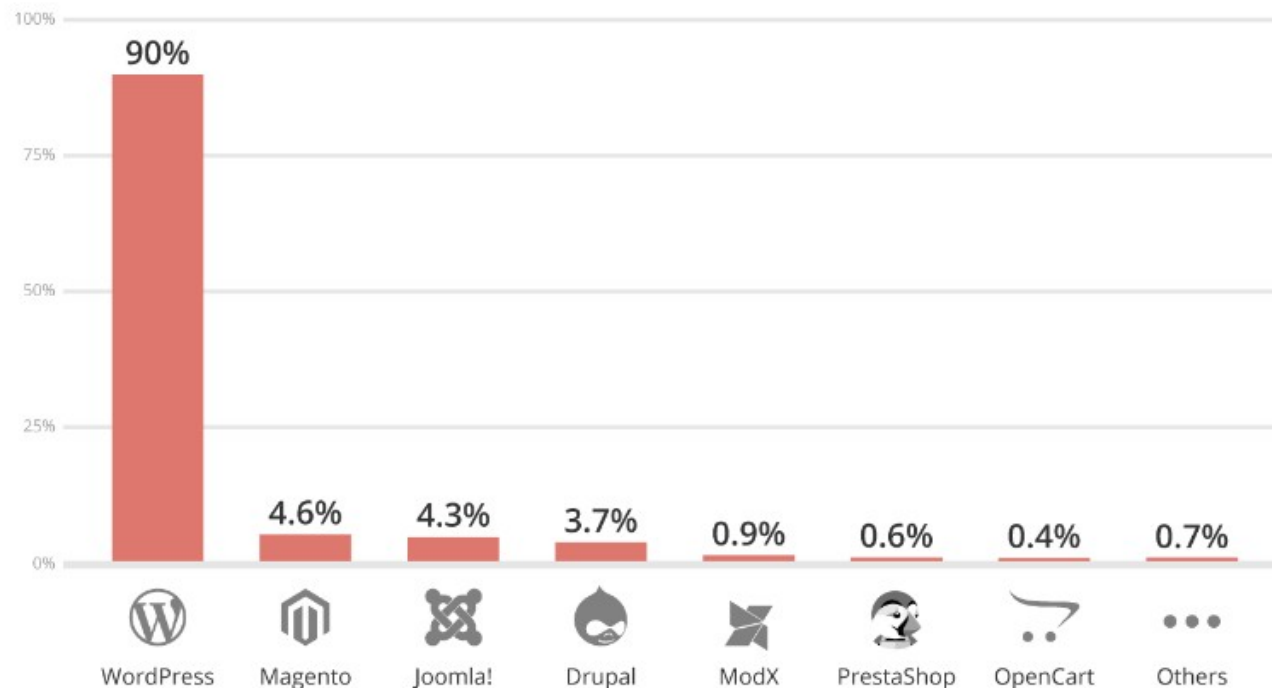
Aide

Faible d'un composant tiers : attaques de l'intérieur

Type d'attaque : exploitation des failles sur des librairies, composants, intégrant un framework, un CMS ou toutes parties internes d'un programme mais reposant sur le développement d'un tiers.

Sécurisation : limitation du nombre des composants tiers, vérification des mises à jour par la veille technologique, tests de fiabilité.

Infected Websites Platform Distribution - 2018



Problèmes de configuration : respect de la méthode

Type d'attaque : exploitation d'un défaut de paramétrage de librairies, frameworks, BDD, services, etc...

Sécurisation : vérifier et respecter les procédures, surveiller les documentations officielles, s'informer des mises à jour, etc.

