# TOP 10 DES VULNÉRABILITÉS OWASP

#### CONTOURNEMENT DU CONTRÔLE D'ACCÈS

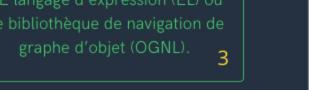
Les défaillances du contrôle d'accès entraînent généralement la divulgation, la modification ou la destruction non autorisée de toutes les données ou l'exécution d'une fonction commerciale en dehors des limites de l'utilisateur.

## DÉFAILLANCES CRYPTOGRAPHIQUES

Défaillances des outils permettant d'assurer, des fonctions de sécurité telles que la confidentialité, l'intégrité, l'authenticité et la non-répudiation. Ils sont qualifiés d'algorithmes, de primitives ou encore de mécanismes cryptographiques.

#### INJECTION

Ce sont des groupes de méthodes Les injections les plus courantes sont SQL, NoSQL, la commande OS, le mappage relationnel d'objet (ORM), LDAP et l'injection DE langage d'expression (EL) ou graphe d'objet (OGNL).



#### CONCEPTION NON SÉCURISÉE

Ce sont des défauts de peuvent être mises en lignes, c'est notion de défaut de mise en œuvre.

Lors du développement de l'application les bonnes mesures de sécurité qui devaient être appliquées n'ont pas été prises en

# CONFIGURATION DE SÉCURITÉ

outil ou d'une solution peu sécurité. Ex : le fait de ne pas automatique permettrait à un individu malveillant de perpétrer une attaque sur un environnement vulnérable de part son obsolescence (version vulnérable ou non à jour).

5

## COMPOSANTS **VULNÉRALES ET OBSOLÈTES**

Si les composants que vous

utilisez pour créer vos obsolètes ou présentent une vulnérabilité grave, vous en vos clients et utilisateurs d'applications.

## ÉCHEC **D'IDENTIFICATION** EТ D'AUTHENTIFICATION

l'authentification et de la gestion des sessions de l'utilisateur est essentielle pour se protéger contre les attaques liées à l'authentification.

La confirmation de l'identité, de

## L'INTÉGRITÉ DES LOGICIELS ET DES DONNÉES

Elles concernent le code et l'infrastructure qui ne protègent pas

DÉFAILLANCES DE

contre les violations de l'intégrité. Un pipeline CI/CD non sécurisé peut introduire un accès non autorisé, de code malveillant ou de compromission du système. Enfin, de nombreuses applications incluent désormais une fonctionnalité de mise à jour automatique, où les mises à jour sont téléchargées sans vérification d'intégrité.

8

# DE SURVEILLANCE DE LA SÉCURITÉ Il est très important d'avoir un système

de journalisation et de surveillance fonctionnel pour collecter les journaux

ÉCHECS DE

JOURNALISATION ET

et egalement donner des alertes en cas de dysfonctionnements ou d'erreurs, sinon, ceux-ci peuvent passer inaperçus durant une longue période et causer beaucoup plus de dégâts.



# SERVEUR (SSRF)

Les failles SSRF se produisent à chaque fois qu'une application Web récupère une

REQUÊTES CÔTÉ

ressource distante sans valider l'URL fournie par l'utilisateur. Il permet à un attaquant de contraindre l'application à envoyer une requête conçue à une destination inattendue, même lorsqu'elle est protégée par un pare-feu, un VPN ou un autre type de liste de contrôle d'accès réseau (ACL). 10

Cabinet de conseil, d'audit et de formation indépendant, MANIKA propose des prestations de Gouvernance SSI, de Cybersécurité, de Continuité d'Activité et de Maîtrise des Processus SI.

BESOIN D'AIDE?

Nos experts peuvent vous aider dans la définition et la mise en place de votre stratégie de cyberdéfense.

COMMERCIAL@MANIKA-CONSULTING.COM

PARIS: +33 (0)1 47 49 81 93 / ROUEN: +33 (0)2 78 77 56 89 LYON: + 33 (0) 6 84 76 42 92 / ABIDJAN: + 22 (5) 22 43 18 56

