RAPPORT N° 2 D'INGÉNIERIE DE LA CRYPTOGRAPHIE

<u>Groupe 4</u> :

Sira NDIAYE

Ndeye Maty TEUW

Adja Rokhaya NDOYE

Yakhya DIALLO

Ndeye Fagnan BEYE

24/11/2022

DIC 3 Informatique/ Télécom

PHASE I : PRÉSENTATION DE LA CATÉGORIE CHOISIE

Passée première dans le classement des 10 vulnérabilités les plus communes en 2021 de l'Open Web Application Security Project (OWASP), le Broken Access Control désigne le scénario dans lequel les attaquants peuvent accéder, modifier, supprimer ou effectuer des actions en dehors des autorisations prévues pour une application ou un système. Selon l'organisation, trente-quatre (34) vulnérabilités appelés Common Vulnerabilities Enumerations (CWEs) peuvent être classées comme une forme de violation du contrôle d'accès, par exemple lorsque des utilisateurs normaux peuvent accéder à des fonctions réservées aux administrateurs en modifiant les paramètres d'une URL, en visualisant ou en modifiant les données d'un autre utilisateur ou en procédant à une escalade des privilèges (CWE-275) . La vulnérabilité Broken Access Control peut être divisée en trois (3) catégories et concerne différents niveaux d'accès aux privilèges qui sont :

- L'accès vertical: Lorsque des utilisateurs peuvent accéder aux données d'autres utilisateurs qui ont le même niveau de permissions qu'eux.
- L'accès horizontal : Lorsque les utilisateurs peuvent accéder aux données des utilisateurs qui ont des autorisations pour effectuer certaines actions que les utilisateurs normaux ne peuvent pas effectuer, avec les contrôles d'accès verticaux, différents types d'utilisateurs ont accès à différentes fonctions de l'application.
- L'accès en fonction du contexte : Lorsqu'un utilisateur est autorisé à effectuer des actions dans le mauvais ordre. Par exemple, après avoir acheté des articles sur un site de commerce électronique, un utilisateur ne devrait pas être autorisé à modifier son panier. Le contrôle d'accès dépendant du contexte ne permet pas à un utilisateur de modifier les articles après le paiement, mais s'il est cassé, alors l'utilisateur sera autorisé à faire des modifications.

La cryptographie est un ensemble de procédés visant à crypter des informations afin de garantir les quatre (4) services fondamentaux de la sécurité des informations que sont la confidentialité, l'intégrité des données, l'authentification et la non-répudiation. La faille qui est l'objet de notre étude impacte tous ces services comme suit:

- Confidentialité

  Des CWEs comme la CWE-863 (Incorrect Authorization) et la CWE-352 (Cross-Site Request Forgery) impactent techniquement ce principe de la sécurité à travers la

lecture de données d'application, la lecture de fichiers ou de répertoires, l'obtention de privilèges ou l'usurpation d'identité, le contournement du mécanisme de protection, etc. Un attaquant pourrait lire des données sensibles, soit en lisant les données directement à partir d'une source de données qui n'est pas correctement restreinte, soit en accédant à une fonctionnalité privilégiée insuffisamment protégée pour lire les données.

Référence: CVE-2008-6123, CVE-2008-3424

- Intégrité

Impact technique : Modification des données de l'application ; modification des fichiers ou des répertoires.

Un attaquant pourrait modifier des données sensibles, soit en écrivant les données directement dans un magasin de données dont l'accès n'est pas correctement limité, soit en accédant à une fonctionnalité privilégiée insuffisamment protégée pour écrire les données.

Référence : CVE-2005-2801

- Contrôle d'accès

Impact technique : obtention de privilèges ou usurpation d'identité ; contournement du mécanisme de protection.

Un attaquant pourrait obtenir des privilèges en modifiant ou en lisant directement des données critiques, ou en accédant à une fonctionnalité privilégiée.

Par exemple, la CWE-639 a des impacts qui ne portent que sur ce principe à travers le mécanisme de protection de contournement, l'obtention des privilèges ou la prise d' identité. Référence: CVE-2001-1155, CVE-2008-3424, CVE-2008-7109

Le contrôle d'accès implique , entre autres, la vérification d'un utilisateur, c'est-à-dire vérifier si le dit utilisateur est connecté, ou s'il est autorisé à passer (ses identifiants de connexion sont corrects). Il existe cependant une troisième vérification à faire qui consiste à s'assurer que les informations de connexion ne sont pas falsifiées et cela se produit lorsqu'un jeton JWT (Json Web Token) est contrefait, par exemple si l'algorithme de cryptage n'est pas correctement défini. C'est dans ce cas précis, que le choix d'algorithmes de chiffrement, tels que le chiffrement RSA, intervient afin de contourner ce problème.