Groupe 8 :

Bocar DIALLO
Elhadj Moussa COULIBALY
El Hadji Malick SY
Mouhamed FALL
Alexandre Adiouma NDENE

I. Explication des concepts

❖ CWE cartographiés

Common Weakness Enumeration (CWE) est un dictionnaire universel en ligne des faiblesses trouvées dans les logiciels informatiques . Le dictionnaire est maintenu par MITRE Corporation et peut être consulté gratuitement dans le monde entier. Le but de CWE est de faciliter l'utilisation efficace d'outils capables d'identifier, de trouver et de résoudre les bogues , les vulnérabilités et les expositions dans les logiciels informatiques avant que les programmes ne soient distribués ou vendus publiquement.

❖ Taux d'incidence maximal

Le taux d'incidence demande quel pourcentage de la population d'applications avait au moins une instance d'un type de vulnérabilité. Peu nous importe si c'était ponctuel ou systémique. Ce n'est pas pertinent pour nos fins ; nous avons seulement besoin de savoir combien d'applications ont eu au moins une instance, ce qui permet de fournir une vue plus claire des résultats des tests sur plusieurs types de tests sans noyer les données dans des résultats à haute fréquence. Cela correspond à une vue liée au risque, car un attaquant n'a besoin que d'une seule instance pour attaquer une application avec succès via la catégorie.

❖ Taux d'incidence moyen

La moyenne pondérée est un calcul qui prend en compte les différents degrés d'importance des nombres dans un ensemble de données. Lors du calcul d'une moyenne pondérée, chaque nombre de l'ensemble de données est multiplié par un poids prédéterminé avant que le calcul final ne soit effectué. Une moyenne pondérée est le plus souvent calculée pour égaliser la fréquence des valeurs dans un ensemble de données.

- **Exploit moyen pondéré**

- **Impact moyen pondéré**

La méthode de la moyenne pondérée est un outil utilisé dans les salles de classe, l'analyse statistique et les bureaux de comptabilité, entre autres. Une moyenne pondérée aide l'utilisateur à obtenir un aperçu plus précis d'un ensemble de données que la moyenne normale seule. La précision des chiffres que vous obtenez avec cette méthode est déterminée par le poids que vous attribuez à des variables spécifiques dans l'ensemble de données.

- **Couverture maximale**

Pour chaque CWE donné, c'est le taux maximal applications testées au niveau d' une organisation.

- **Couverture moyenne**

c’est la moyenne de couverture pour des applications CWE. il est entre la couverture maximale et la couverture minimale des données

- **Nombre total d'occurrences**

Une occurrence est une instance de quelque chose ou un moment où quelque chose se produit

Total des CVE

CVE, abréviation de Common Vulnerabilities and Exposures, est une liste de failles de sécurité informatique divulguées publiquement.

II. Interpretation des Resultats de chaque CWE

1) A01: 2021 - Contrôle d'accès cassé

Pour le controle d’acces casse a une couverture maximale de 94.55% ce qui veut dire l’ensemble des 94% des applications ont été testées pour une forme de contrôle d'accès cassé avec un taux d'incidence moyen de 3,81 % avec plus d'occurrence dans l’ensemble des données fournies soit 318 487 . CWE cartographiés est faible dans ce type d’attaque donc les informations peuvent être exploitées par une

personne non autorisée. Donc tout type de modification est possible (insertion d'information ,falsification de requêtes) .

2) A02 Échecs cryptographiques

Dans les Échecs cryptographique le CWE cartographiés est faible (29) ce qui entraîne un problème d'intégrité des données. Taux d'incidence maximal a une valeur de 46.44% qui est lié à la défaillance liée à la crytographie . Le Taux d'incidence moyen très faible soit 4.49% ce qui réduit la confidentialité des données. La couverture maximale et la couverture moyenne 79,33% et 43,85% ce qui veut dire environ 30% des données ont une défaillance liée à la cryptographie qui conduit souvent à l'exposition de données sensibles ou à la compromission du système.

3) A03:2021-INJECTION

l'injection occupe l'avant dernière place au niveau des faiblesses exploitables elle a un CWE de 33 dû à l'utilisation massive et permanente des bases de données.l'injection a été testée sur 94,04% qui est le taux maximal d'applications testées au niveau d'une entreprise et 19,09% de la population ont été recensées comme ayant une instance de ce type de failles.Ce résultat est assez élevé pour des applications d'entreprises.L'application est vulnérable lorsque les données de l'utilisateur ne sont pas contrôlées par l'application,les données hostiles sont directement utilisées ou concaténées .Ceci montre que 19,09% des apps d'entreprises testées ne réalisent pas les tests et ne séparent pas les données non fiables des commandes et requêtes.
Un taux d'incidence moyen de 3% qui montre que la plupart des données envoyées ne sont pas utile c'est l'essence même de l'injection qui correspond a ajouter des données malveillantes aux données utilisateurs.Le nombre total de CVE qui est de 32078 montre qu' avec l'injection on peut exploiter plusieurs failles.De meme que le nombre d'occurences qui est de 274 228 montre que l'injection est utilisée massivement car il occupe la 3e place du classement.

4) A04-CONCEPTION NON SÉCURISÉE

Conception non sécurisée est une vaste catégorie représentant différentes insuffisances, exprimées par « contrôles de conception manquants ou inefficaces ». La conception non sécurisée n'est pas la source de toutes les autres catégories de risques du Top 10. Il existe une différence entre une conception non sécurisée et une implémentation non sécurisée.Les tests pour la conception non sécurisée couvre une population d'applications de 77,25 %, dépassant largement la moitiés de la population. Le taux d'incidence s'élève à 3 %, ce qui est pratiquement faible.

L’impact sur la population est faible et justifié par le **Avg Weighted Impact** qui est égal à 6.78.

5) A05 Security Misconfiguration

Malgré une couverture maximale élevée de 89,5%, nous avons constaté que le taux d'incidence maximal (27,96%) n’est pas très élevé. Autrement, cette vulnérabilité n’est pas très répandue comparé à l'édition précédente. Avec un total CVEs nulle, on peut dire que cette faille n’est pas connue du grand public. Actuellement, elle est à plus de 208 000 d'occurrence mais avec l'évolution vers des logiciels hautement configurables, il n'est pas surprenant de voir cette catégorie monter en puissance

6) A06 Composants vulnérables et obsolètes

Avec une couverture moyenne faible comparée à la couverture maximale qui est de 51, 78%, nous avons constaté que les Taux d'incidence moyen et maximal (8,77% et 27,96%) sont relativement faibles. Autrement, cette vulnérabilité n’est pas très répandue comparé à l'édition précédente. Son total CVEs nulle et nombre d'occurrence faible sont dus au fait que les composants vulnérables sont un problème connu pour lequel nous avons du mal à tester et à évaluer les risques.

7) A07 Identification et authentification de mauvaise qualité

Cette catégorie était auparavant n°1 sous le nom de *Broken Authentication* . Cela inclut des péchés courants tels que la mauvaise gestion des mots de passe, l'absence de limitation de débit pour empêcher le bourrage d'informations d'identification, la gestion de session non sécurisée et l'utilisation de mécanismes d'authentification pouvant être contournés. Alors que les données de l'OWASP suggèrent un taux d'incidence plus faible 2,32%, ce qui explique vraisemblablement le classement inférieur dans cette édition, les attaques liées à l'authentification peuvent être extrêmement dangereuses lorsqu'elles sont automatisées pour extraire les informations d'identification à grande échelle. Selon le Verizon DBIR pour 2021 , 47,54% % de toutes les violations de données impliquent des identifiants volés, donc cette catégorie est là pour rester.

8) A08:2021-Manque d'intégrité des données et du logiciel

Une nouvelle catégorie cette année, les échecs d'intégrité des logiciels et des données font référence au code et à l'infrastructure qui ne parviennent pas à protéger contre les violations d'intégrité. Cela inclut les mises à jour logicielles, les

données critiques et les pipelines CI/CD qui sont mis en œuvre sans vérification. Un exemple de ceci inclut des objets ou des données encodés ou sérialisés dans une structure qu'un attaquant peut modifier. Un autre exemple est une application qui s'appuie sur des plugins, des bibliothèques ou des modules provenant de sources non fiables. Les pipelines CI/CD non sécurisés qui peuvent introduire un potentiel d'accès non autorisé, de code malveillant ou de compromission du système entrent également dans cette catégorie. Enfin, les applications dotées d'une fonctionnalité de mise à jour automatique, dans lesquelles les mises à jour sont téléchargées sans vérification d'intégrité suffisante et appliquées à une application précédemment approuvée, sont considérées comme des défaillances de l'intégrité des logiciels et des données, car les attaquants pourraient s'infiltrer dans la chaîne d'approvisionnement pour distribuer leurs propres mises à jour malveillantes. La désérialisation non sécurisée du Top 10 2017 a été classée dans cette catégorie.

9) A09:2021- Échecs de journalisation et de surveillance de la sécurité

Sans journalisation ni surveillance, les violations ne peuvent pas être détectées. Une journalisation, une détection, une surveillance et une réponse active insuffisantes se produisent à tout moment. Les échecs de journalisation et de surveillance de la sécurité présentent un taux maximal d'incidence de 19.23%. Cela signifie que sur 100 applications testées, plus de 19 d'entre elles ont une instance de cette vulnérabilité, ce qui est un peu moins élevé. Cependant la moyenne tourne autour de 6.5 %. Les tests ont couvert 53.67 % de la population d'applications pour une moyenne de 39.97%, accentuant ainsi l'impact de cette vulnérabilité. D'ailleurs le **Avg Weighted Impact** s'élève à 4.99.

10) A10:2021- Contrefaçon de demande côté serveur

Les failles SSRF se produisent chaque fois qu'une application Web récupère une ressource distante sans valider l'URL fournie par l'utilisateur. Il permet à un attaquant de contraindre l'application à envoyer une requête spécialement conçue vers une destination inattendue. Les tests pour la contrefaçon de demande côté serveur couvrent une population d'applications de 67.72 %, dépassant largement la moitiés de la population. Et pour plus de 67 % testées, le taux d'incidence s'élève à 2.72 %, ce qui est pratiquement faible. L'impact sur la population est faible et justifié par le **Avg Weighted Impact** qui est égal à 6.72.