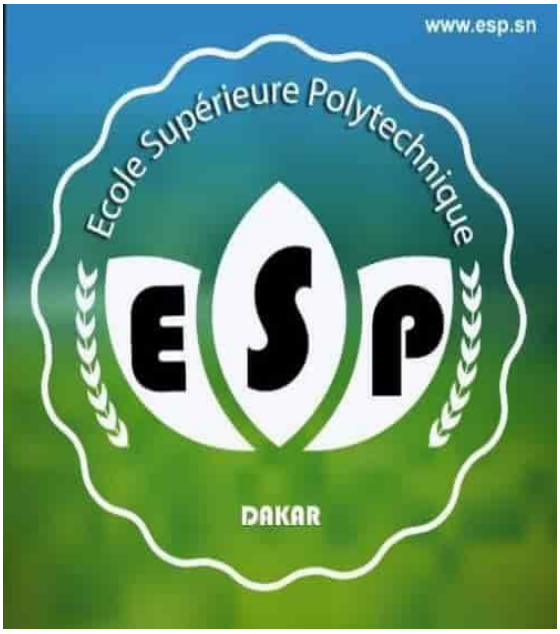
Université Cheikh Anta Diop de Dakar

Ecole Supérieure Polytechnique




Département Génie Informatique

Ingénierie Cryptographique

**Membres du groupes**

Haby DIOP

Mariama Ka

Marième AIDARA

Papa Cheikh GNINGUE

Taamba Bedel Brice THIOMBIANO

Année anniversaire : 2022/2023

- CWEs associées : le nombre de CWEs associées à une catégorie par l'équipe du Top 10.
- Taux d'incidence : le taux d'incidence est le pourcentage d'applications vulnérables à cette CWE parmi la population testée par cette organisation pour cette année.
- Couverture (Test) : Le pourcentage d'applications testées par toutes les organisations pour une CWE donnée.
- Exploitation pondérée : le sous-score Exploitation des scores CVSSv2 et CVSSv3 attribués aux CVEs associées aux CWEs, normalisés et placés sur une échelle de 10 points.
- Impact pondéré : le sous-score d'impact des scores CVSSv2 et CVSSv3 attribués aux CVEs associées aux CWEs, normalisés et placés sur une échelle de 10 points.
- Nombre total d'occurrences : nombre total d'applications trouvées pour lesquelles les CWEs sont associées à une catégorie.
- Nombre total de CVEs : nombre total de CVEs dans la base de données NVD qui ont été associées aux CWEs associées à une catégorie.

# A. Analyse

### **A01** :2021 – **Contrôle d'Accès Défaillants**

Pour cette catégorie on observe :

34 faiblesses, un taux d'incidences maximale de 55.91%, un taux d'incidences moyen de 3.81%, un sous-score Exploitation de 6.92, un sous-score d'impact de 5.93, une couverture maximale de 94.55% et une couverture moyenne de 47.72%. Et enfin un nombre total d'occurrences de 318 487 et un nombre total de CVEs de 190.13.

### **A02** :2021 – **Défaillances Cryptographiques :**

Pour cette catégorie on observe :

29 faiblesses, un taux d'incidences maximale de 46.44%, un taux d'incidences moyen de 4.49%, un sous-score Exploitation de 7.29, un sous-score d'impact est 6.81, une couverture maximale de 79.33% et une couverture moyenne de 34.85%. Et enfin un nombre total d'occurrences de 233 788 et un nombre total de CVEs de 3075.

### **A03** :2021 – **Injection :**

Pour cette catégorie on observe :

33 faiblesses, un taux d'incidences maximale de 19.09%, un taux d'incidences moyen de 3.37%, un sous-score Exploitation de 7.25, un sous-score d'impact de 7.15, une couverture maximale de 94.04% et une couverture moyenne de 47.90%. Et enfin un nombre total d'occurrences de 274 228 et un nombre total de CVEs de 32078.

### **A04** :2021 – **Conception non sécurisée :**

Pour cette catégorie on observe :

40 faiblesses, un taux d'incidences maximale de 24.19%, un taux d'incidences moyen de 3%, un sous-score Exploitation de 6.46%, un sous-score d'impact de 6.78%, une couverture maximale de 77.25% et une couverture moyenne de 42.51%. Et enfin un nombre total d'occurrences de 262 407 et un nombre total de CVEs de 2691.

## **A05** :2021 – **Mauvaise Configuration de Sécurité :**

20 faiblesses, un taux d'incidences maximale de 19.84%, un taux d'incidences moyen de 4.51%, un sous-score Exploitation de 8.12%, unsous-score d'impact de 6.56%, une couverture maximale de 89.58% et une couverture moyenne de 44.84%. Et enfin un nombre total d'occurrences de 208 387 et un nombre total de CVEs de 789.

## **A06** :2021 – **Composants vulnérables et obsolètes :**

Pour cette catégorie on observe :

3 faiblesses, un taux d'incidences maximale de 27.96%, un taux d'incidences moyen de 8.77%, un sous-score Exploitation de 5, un sous-score d'impact de 5, une couverture maximale de 51.78% et une couverture moyenne de 22.47%. Et enfin un nombre total d'occurrences de 30457 et un nombre total de CVEs de 0.

## **A07** :2021 – **Identification et Authentification de mauvaise qualité :**

Pour cette catégorie on observe :

22 faiblesses, un taux d'incidences maximale de 14.84%, un taux d'incidences moyen de 2.55%, un sous-score Exploitation de 7.40, un sous-score d'impact est 6.50, une couverture maximale de 79.51% et une couverture moyenne de 45.72%. Et enfin un nombre total d'occurrences de 132195 et un nombre total de CVEs de 3897.

## **A08 :2021 – Manque d'intégrité des données et du logiciel**

Pour cette catégorie on observe :

10 faiblesses, un taux d'incidences maximale de 16.67%, un taux d'incidences moyen de 2.05%, un sous-score Exploitation de 6.94, un sous-score d'impact est 7.94, une couverture maximale de 75.04% et une couverture moyenne de 45.35%. Et enfin un nombre total d'occurrences de 47 972 et un nombre total de CVEs de 1152.

## **A09 :2021 – Carence des systèmes de contrôle et de journalisation**

Pour cette catégorie on observe :

4 faiblesses, un taux d'incidences maximale de 19.23%, un taux d'incidences moyen de 6.51%, un sous-score Exploitation de 6.87, un sous-score d'impact est 4.99, une couverture maximale de 53.67% et une couverture moyenne de 39.97%. Et enfin un nombre total d'occurrences de 53615 et un nombre total de CVEs de 242.

## **A10 :2021 – A10 Falsification de requête côté serveur (SSRF)**

Pour cette catégorie on observe :

1 faiblesses, un taux d'incidences maximale de 2.72%, un taux d'incidences moyen de 2.72%, un sous-score Exploitation de 8.28, un sous-score d'impact est 6.72, une couverture maximale de 67.72% et une couverture moyenne de 67.72%. Et enfin un nombre total d'occurrences de 9503 et un nombre total de CVEs de 385.

## B. Interprétations

**Pour A01 :** Sachant que cette catégorie avait pris la **cinquième** place au niveau du Top 10 : 2017, on observe un changement de place dans la structure du top 10 : 2021 dans laquelle elle va prendre la **première** place de ce rang en soulignant que 94 % des applications ont été testées pour une forme de contrôle d'accès défaillant. Son changement de place dans le top 10 : 2021 est due au fait de l'obtention des nouveaux résultats des facteurs calculés par rapport à l'année 2021(CWEs associées, Taux d'incidence, Exploitation pondérée, Impact pondéré, Nombre total d'occurrences, Nombre total de CVEs) , qui nous a permis d'évaluer l'estimation des risque sur **les contrôles d'accès défaillants** et on remarque que l'estimation des défaillances étant plus grande que les 10 catégories du Top 10 : 2021 restant d'où ce qui justifie sa nouvelle place.

**Pour A02 :** Sachant que cette catégorie avait pris la **troisième** place au niveau du Top 10 : 2017 sous le nom **d'*Exposition de données sensibles***, on observe un changement de place dans la structure du top 10 : 2021 dans lequel elle va prendre la **deuxième** place de ce rang sous le nom de D**éfaillances cryptographiques**. Son changement de place dans le top 10 : 2021 est due au fait de l'obtention des nouveaux résultats des facteurs calculés par rapport à l'année 2021(CWEs associées, Taux d'incidence, Exploitation pondérée, Impact pondéré, Nombre total d'occurrences, Nombre total de CVEs) , qui nous a permis d'évaluer l'estimation des risque sur **les échecs cryptographiques** et on remarque que l'estimation des défaillances étant plus grande que les 9 catégories du Top 10 : 2021 restant d'où ce qui justifie sa nouvelle place.

**Pour A03 :** Sachant que cette catégorie avait pris la **première** place au niveau du Top 10 : 2017, on observe un changement de place dans la structure du top 10 : 2021 dans lequel elle va basculer en **troisième** place de ce rang en soulignant que 94 % des applications ont été testées pour une forme d'injection. Son changement de place dans le top 10 : 2021 est due au fait avec l'obtention des nouvelles résultats des facteurs calculés par rapport à l'année 2021(CWEs associées, Taux d'incidence, Exploitation pondérée, Impact pondéré, Nombre total d'occurrences, Nombre total de CVEs) , qui nous on permit d'évaluer l'estimation des risque sur **l'injection** et on remarque que l'estimation des défaillances étant plus grande par parmis les 8 catégories du Top 10 : 2021 restant d'où ce qui justifie sa nouvelle place.

**Pour A04 :** Sachant que cette catégorie n'existait pas au niveau du Top 10 : 2017, on observe son existence dans la structure du top 10 : 2021 dans lequel elle va prendre la **quatrième** place de ce rang. Son apparition dans le top 10 : 2021 est due au fait de l'obtention des nouveaux résultats des facteurs calculés par rapport à l'année 2021(CWEs associées, Taux d'incidence, Exploitation pondérée, Impact pondéré, Nombre total d'occurrences, Nombre total de CVEs), ce qui nous a permis d'évaluer l'estimation des risques sur **la conception non sécurisée** et on remarque que l'estimation des défaillances étant plus grande que les 7 catégories du Top 10 : 2021 restant d'où ce qui justifie sa nouvelle place.

**Pour A05 :** Sachant que cette catégorie avait pris la **sixième** place au niveau du Top 10 : 2017, on observe un changement de place dans la structure du top 10 : 2021 dans laquelle elle va prendre la **cinquième** place de ce rang en soulignant que 90 % des applications ont été testées pour une forme de mauvaise configuration. Son changement de place dans le top 10 : 2021 est due au fait de l'obtention des nouveaux résultats des facteurs calculés par rapport à l'année 2021(CWEs associées, Taux d'incidence, Exploitation pondérée, Impact pondéré, Nombre total d'occurrences, Nombre total de CVEs) , qui nous a permis d'évaluer l'estimation des risque sur

**la mauvaise configuration de la sécurité** et on remarque que l'estimation des défaillances étant plus grande que les 6 catégories du Top 10 : 2021 restant d'où ce qui justifie sa nouvelle place.

**Pour A06 :** Sachant que cette catégorie avait pris la **neuvième** place au niveau du Top 10 : 2017, mais on observe un changement de place dans la structure du top 10 : 2021 dans lequel elle va prendre la **sixième** place de ce rang. Son changement de place dans le top 10 : 2021 est due au fait de l'obtention des nouveaux résultats des facteurs calculés par rapport à l'année 2021(CWEs associées, Taux d'incidence, Exploitation pondérée, Impact pondéré, Nombre total d'occurrences, Nombre total de CVEs) , qui nous on permit d'évaluer l'estimation des risque sur les **composants vulnérables et obsolètes** et on remarque que l'estimation des défaillances étant plus grande que les 5 catégories du Top 10 : 2021 restant d'où ce qui justifie sa nouvelle place.

**Pour A07 :** Sachant que cette catégorie avait pris la **deuxième** place au niveau du Top 10 : 2017 sous **le nom authentification brisée**, mais on observe un changement de place dans la structure du top 10 : 2021 dans lequel elle va basculer à la **septième** place de ce rang. Son changement de place dans le top 10 : 2021 est due au fait de l'obtention des nouveaux résultats des facteurs calculés par rapport à l'année 2021(CWEs associées, Taux d'incidence, Exploitation pondérée, Impact pondéré, Nombre total d'occurrences, Nombre total de CVEs) , qui nous a permis d'évaluer l'estimation des risque sur **les échecs d'identification et d'authentification** et on remarque que l'estimation des défaillances étant plus grande que les 4 catégories du Top 10 : 2021 restant d'où ce qui justifie sa nouvelle place.

**Pour A08 :** Sachant que cette catégorie n'existait pas au niveau du Top 10 : 2017, on observe son existence dans la structure du top 10 : 2021 dans lequel elle va prendre la **huitième** place de ce rang. Son apparition dans le top 10 : 2021 est due au fait de l'obtention des nouveaux résultats des facteurs calculés par rapport à l'année 2021(CWEs associées, Taux d'incidence, Exploitation pondérée, Impact pondéré, Nombre total d'occurrences, Nombre total de CVEs) , qui nous a permis d'évaluer l'estimation des risque sur **les défaillances d'intégrité des logiciels et des données** et on remarque que l'estimation des défaillances étant plus grande que les 3 catégories du Top 10 : 2021 restant d'où ce qui justifie sa nouvelle place.

**Pour A09 :** Sachant que cette catégorie avait pris la **dixième** place au niveau du Top 10 : 2017, mais on observe un changement de place dans la structure du top 10 : 2021 dans lequel elle va prendre la **neuvième** place de ce rang. Son changement de place dans le top 10 : 2021 est due au fait de l'obtention des nouveaux résultats des facteurs calculés par rapport à l'année 2021(CWEs associées, Taux d'incidence, Exploitation pondérée, Impact pondéré, Nombre total d'occurrences, Nombre total de CVEs) , qui nous a permis d'évaluer l'estimation des risque sur **les échecs de journalisation et de surveillance de la sécurité** et on remarque que l'estimation des défaillances étant plus grande que les 2 catégories du Top 10 : 2021 restant d'où ce qui justifie sa nouvelle place.

**Pour A10 :** Sachant que cette catégorie n'existait pas au niveau du Top 10 : 2017, mais on observe son existence dans la structure du top 10 : 2021 dans lequel elle va prendre la **dixième** place de ce rang. Son apparition dans le top 10 : 2021 est due au fait de l'obtention des nouveaux résultats des facteurs calculés par rapport à l'année 2021(CWEs associées, Taux d'incidence, Exploitation pondérée, Impact pondéré, Nombre total d'occurrences, Nombre total de CVEs) , qui nous a permis d'évaluer l'estimation des risque sur **la contrefaçon de demande coté**

**serveur** et on remarque que l'estimation des défaillances étant plus fiable par rapport au Top 10 : 2021 d'où ce qui justifie sa nouvelle place.

## Tache 2 : Choix du sujet et illustration avec via un scénario

**Sujet : A07:2021 – Identification et authentification de mauvaise qualité**

**Scénario 3** : Les timeouts de session d'application ne sont pas paramétrés correctement. Un utilisateur utilise un ordinateur public pour accéder à une application. À la place de se déconnecter correctement, l'utilisateur ferme le navigateur et quitte l'ordinateur. Un attaquant utilise ensuite le même navigateur quelque temps après et l'utilisateur est toujours authentifié.

**Illustration du scénario :**

Pour illustrer ce scénario, nous allons prendre les applications telles Facebook et Gmail. Après s'être connecté sur ces dernières via un navigateur. Si on ferme l'application sans se déconnecter, il est tout à fait possible de recharger la page sans pour autant se reconnecter même après plusieurs jours d'inactivité. Cela entraine que toute personne utilisant ce même navigateur peut avoir accès à notre compte. De plus, si la personne connectée à enregistrer ses identifiants (username et mot de passe), il est possible de les récupérer via les paramètres du navigateur et de les utiliser pour nuire, sachant qu'une personne peut utiliser les mêmes identifiants pour plusieurs applications.