Documentation Administrative pour le Débogage de l'API de Vérification des Liens Phishing

Introduction : L'API de vérification des liens phishing est un composant essentiel de notre système de sécurité. Elle permet de détecter les liens malveillants et de protéger nos utilisateurs contre les attaques en ligne. Cependant, comme pour tout logiciel, il peut y avoir des moments où des problèmes surviennent. Cette documentation vise à guider les administrateurs à travers le processus de débogage de l'API en cas de dysfonctionnement.

Étapes de Débogage :

1. Redémarrer les Services :

Lorsque des problèmes surviennent, la première étape consiste souvent à redémarrer les services liés à l'API de vérification des liens phishing. Cela peut aider à résoudre les problèmes mineurs liés à la disponibilité des services.

Sudo service apache2 restart

// // mariadb //

// // php //

Puis on verifie les logs Less /var/log/apache2/error.log

Si l'erreur persiste, passer à l'étape suivante

2. Téléchargement et remplacement de la Base de Données :

La base de données utilisée par l'API pour la détection des liens phishing doit être à jour. Pour cela, nous utilisons une base de données disponible sur GitHub.

Utilisez la commande suivante pour télécharger la base de données :

Wget https://github.com/mitchellkrogza/Phishing.Database/blob/master/ALL-phishing-links.tar.gz

Assurez-vous que l'emplacement de téléchargement est situé dans le même répertoire que le programme create_db.sh.

Une fois que la base de données a été téléchargée, vous devez la décompresser et la préparer pour une utilisation par l'API tar -xzf ALL-phishing-links.tar.gz.

Utilisez la commande create_db.sh pour créer ou mettre à jour la base de données avec les nouvelles informations téléchargées, puis assurez-vous que cette commande est exécutée dans le répertoire approprié où la base de données a été téléchargée de façons a supprimé l'ancienne qui est potentiellement corrompue.

3. Vérification du Bon Fonctionnement :

Après avoir redémarré les services, téléchargé et préparé la base de données, il est temps de vérifier si l'API fonctionne correctement.

Testez l'API en utilisant différents liens, y compris des liens suspects connus, pour vérifier si elle détecte correctement les liens phishing.

Surveillez les journaux d'activité de l'API pour détecter d'éventuels messages d'erreur ou avertissements qui pourraient indiquer des problèmes résiduels.

Conclusion : En suivant ces étapes, vous devriez être en mesure de déboguer efficacement l'API de vérification des liens phishing. Si des problèmes persistent après avoir suivi ces étapes, veuillez consulter la documentation supplémentaire ou contacter le support technique pour obtenir de l'aide supplémentaire. La maintenance régulière et la surveillance de l'API sont essentielles pour assurer son bon fonctionnement et garantir la sécurité de nos utilisateurs.