Actifs	Vulnérabilités	Mesures correctives	Services Conservés	Statut
- https://sineb.bj - http://administration.sineb.bj/	- La requête de téléchargement des document sélectionner utilise une methode GET - L'accès au jar backend-service.jar est ouvert - Les Identifiants du SMTP dans le code - La clé de signature des tokens au format JWT est exposé dans le code - L'accès de la base de donnée est exposé dans le code - La non vérification du nom des fichiers avant le téléversement - L'accès non sécurisé aux informations de l'utilisateur à savoir : Id - Falsification de requête côté serveur, au niveau de son api - Insuffisance de contrôle d'accès a été identifiée sur la plateforme permettant à un utilisateur n'ayant pas les droits appropriés, déffectuer les mêmes actions qu'un administrateur	- Effectuer une validation et un filtrage des noms afin d'empêcher l'accès à des chemins de fichiers non autorisés; - Configurer le serveur et les permissions des fichiers de manière sécurisée de sorte à restreindre l'accès à des répertoires spécifiques; - Mettre en place des contôles d'accès renforcés, y compris l'utilisation de mécanismes d'authentification et autorisation appropriés pour les utilisateurs et les processus accédant aux fichiers et répertoires; - Changer tous les identifiants exposés; - Valider les chemins de destination des fichiers afin d'empêcher les téléversements dans les répertoires non autorisés et éviter l'écrasement de fichiers critiques; - Restreindre l'accès aux répertoires de téléversement afin que les fichiers ne puissent être stockés que dans des répertoires spécifiques et sécurisés; - Utiliser un système de vérification des types de fichiers pour accepter uniquement les fichiers avec des exrensions ou types préalablement autorisés et sécurisés - Mettre en place des mécanismes de contrôle d'accès strict pour garantir que seules les personnes autorisées et authentifiées puissent accéder aux informations de la plateform; - Opter pour l'utilisation d'identifiants opaques ou faire recours au chiffrement des identifiants transmis dans les requêtes afin d'éviter que ces derniers soint manipulés ou prédictibles - Valider les URL de redirection en utilisant une liste blanche (witelist) des destinations autorisées; - Encoder correctement les urls afin d'éviter l'insertion de caractères malveillants ou l'évasion de paramètres - Mettre en place des mécanismes de restriction pour garantir que seuls les profils autorisés puissent accéder aux resources ou effectuer des actions attribuées; - utiliser le principe du moindre privilège sur toutes les routes API; - Effectuer une vérification stricte des autorisations côtés serveur avant d'exécuter des actions sensibles ou d'accéder à des informations confidentielles	- sineb-frontoffice - sineb-backoffice	Résolu
- backend.sineb.bj	La route https://backend.sineb.bj/rc/rbdd/document-sineb/download/?refdocument= de l'API permet aux utilisateurs du SINEB de télécharger des fichiers en spécifiant le chemin sur le serveur. En modifiant le paramètre refdocument , un acteur malveillant pourrait accéder à des répertoires ou à des fichiers sensibles, compromettant ainsi la sécurité des données.	- Limiter l'accès aux fichiers à un répertoire spécifique -Nettoyer et valider le paramètre refdocument -Utiliser une identification des fichiers plutôt que des chemins - Implémenter des contrôles d'accès basés sur les rôles pour garantir que seules les personnes autorisées puissent accéder aux ressources de l'API et à la documentation Swagger - Implémenter une authentification et une autorisation appropriées pour toutes les routes de l'API - Implémenter des validations et des vérifications approfondies des entrées utilisateur pour prévenir les tentives d'accès non autorisé ou de manipulation de fichiers sensibles - Filtrer et valider les entrées utilisateur pour prévenir les tentives d'accès non autorisé ou de manipulation de fichiers sensibles - Changer les mots de passe exposés (Système et dev) - Ajouter les en-têtes HTTP suivants : - X-XSS-Protection - XFrame-Options - X-Content-Type-Options - Strinct - Transport - Security - Expires - Cache-Control - Set-Cookie - Content-Security-Policy (Système et dev) - Implémenter les exigences du référentiel de sécurité pour la protection des services en ligne; - Mettre en place un principe de moindre privilège impliquant l'attribution de droits d'accès strictement nécessaire pour les activités associés à chaque utilisateur - suivre des directives de codage sécurisé et d'utiliser des bibliotèques de sécurités reconnues ou recommandées par l'ASIN du Bénin	- sineb-backend	Résolu
- ged.sineb.bj	- L'accès au swagger est ouvert sans autorisation et authentification	- Mettre en place des mécanismes de restriction pour garantir que seules les personnes autorisées et authentifiées puissent accéderaux informations sensibles de la plateforme - Restreindre l'accès au swagger ou à l'interface API si ces outils sont indispensables, ou les supprimer si leur utilisation n'est pas nécessaire - Ajouter les en-têtes HTTP suivants : - X-XSS-Protection - XFrame-Options - X-Content-Type-Options - Strinct - Transport - Security - Expires - Cache-Control - Set-Cookie - Content-Security-Policy - Implémenter les exigences du référentiel de sécurité pour la protection des services en ligne; - Mettre en place un principe de moindre privilège impliquant l'attribution de droits d'accès strictement nécessaire pour les activités associés à chaque utilisateur - suivre des directives de codage sécurisé et d'utiliser des bibliotèques de sécurités reconnues ou recommandées par l'ASIN du Bénin	- mayan-app	En cours