Vuln	Description	Source	Périmètre	Criticité	Reco	Recommandation	Priorité	Etat	Dates de correction prévu
V1	L'un des champs de la page de logs est vulnérable aux injections SQL	Pentest Externe	Application Web	4	R1	Il est recommandé d'utiliser des requêtes préparées (prepared statement) pour limiter les risques d'injections SQL. Par ailleurs, les champs utilisateurs doivent être encodés avant d'être utilisés par l'application. Le langage PHP propose pour répondre à ces deux cas de figure des classes et fonctions : -Les requêtes préparées peuvent être écrites à partir de la classe PDO (PHP Data Object) qui permet de ne pas manipuler directement des chaînes de caractères SQL. -La fonction « htmlspecialchars() » permet d'encoder les caractères spéciaux propres au langage SQL pour les rendre non interprétable par le moteur de base.	P1	EN COURS	CORRECTION D'ICI SEPTEMBRE 2023
V2	Certains des mots de passe utilisateurs sont stockés en clair dans la base	Pentest Externe	Application Web	4	R2	Il est nécessaire de filtrer les entrées des utilisateurs côté serveur afin de supprimer les caractères spéciaux qui peuvent entrainer une injection malveillante. En langage PHP, il est recommandé d'utiliser la fonction htmlspecialchars() pour convertir ces caractères spéciaux en entités HTML.Les mots de passe doivent être hashés et de préférence salés avant d'être insérés dans la base. La fonction "Password_bcrypt()" intégrée à PHP, combinée avec une politique de mot de passe renforcée offre un niveau de sécurité convenable	P1	CORRIGÉ	18/05/2022
ORG1	Effectuer une analyse des risques EBIOS	Entretiens techniques	Sécurité organisationnelle	4	R15	Afin d'alimenter la feuille de route de sécurité, il est recommandé d'effectuer une analyse des risques. Nous recommandons l'utilisation de la méthodologie EBIOS. Cela permettra d'identifier les risques pour Waynes Enterprises et de définir des contre-mesures pour réduire ces risques.	P1	PRÉVU	CORRECTION D'ICI SEPTEMBRE 2023
V3	L'application ne possède pas de politique pour la gestion des mots de passe	Pentest Externe	Application Web	3	R3	Les mots de passe doivent être validés côté serveur pour satisfaire une taille d'au moins 8 caractères et utiliser 3 parmi 4 types de caractère (min, maj, num, spé). En complément une liste noire de mots à ne pas utiliser peut être mise en place pour ne pas faire apparaître le nom des sociétés, de l'application, de l'utilisateur ou tout autre mot fréquemment utilisé (Top 10 des pires mots de passe).	P2	CORRIGÉ	18/05/2022
V4	La base de données est mutualisée entre toutes les sociétés utilisant BATMANAPP	Pentest Externe	Base de données	3	R4	Afin de limiter les risques en cas d'exploitation de vulnérabilité applicative, les données propres à une société ne doivent pas pouvoir être accédées par une autre. Il est préférable de créer des bases propres aux sociétés (hébergés au sein d'une même instance MySQL), l'application y accédant au travers d'un compte applicatif propre à la société et possédant des droits de lecture et écriture sur sa base et de manière extrême en lecture seule sur les données de la base BATMANAPP.	P2	EN COURS	CORRECTION D'ICI SEPTEMBRE 2023
V5	Des failles XSS sont présentent dans plusieurs pages du site	Pentest Externe	Application Web	3	R5	Il est recommandé de filtrer ou d'encoder systématiquement les entrées utilisateurs. PHP met à disposition différentes fonctions, telles que "htmlspecialchars()" pour permettre d'encoder les données utilisateurs transmises au serveur et de rendre l'utilisation de caractères spéciaux ("<", ">"…) non interprétables lors du leur affichage dans le navigateur.	P2	EN COURS	CORRECTION D'ICI SEPTEMBRE 2023
ORG2	Definir un Plan de continuité d'activité (PCA)	Entretiens techniques	Sécurité organisationnelle	3	R16	Un Plan de Continuité d'Activité (PCA) décrit une série de scénarios de catastrophes et les mesures que l'entreprise prendra dans chaque scénario pour revenir à un fonctionnement normal. Afin d'être prêt en cas de catastrophe, nous recommandons à Waynes Enterprises de développer un PCA.	P2	PRÉVU	CORRECTION D'ICI SEPTEMBRE 2023
ORG3	Définir un Plan de Reprise d'Activité (PRA)	Entretiens techniques	Sécurité organisationnelle	3	R17	Un Plan de Reprise d'Activité (PRA) est un processus documenté ou un ensemble de procédures permettant d'exécuter les processus de reprise d'activité d'une organisation et de récupérer et protéger l'infrastructure informatique d'une entreprise en cas de sinistre. Afin d'être prêt en cas de sinistre, nous recommandons à Waynes Enterprises de développer un DRP.	P2	PRÉVU	CORRECTION D'ICI SEPTEMBRE 2023
ORG4	Configurer un serveur d'authentification pour les connexions aux services d'administration (SSH)	Entretiens techniques	Sécurité organisationnelle	3	R18	Il est recommandé de mettre en place un système de double authentification afin de se connecter aux services d'administration SSH des machines. Pour cela, le serveur SSO Keycloak peut être utilisé : https://medium.com/@mudithadul/little-things-if-world-need-it-4862e68453e0	P2	PRÉVU	CORRECTION D'ICI SEPTEMBRE 2023
V6	Aucune analyse antivirale n'est effectuée lors de l'importation de fichiers par l'administrateur	Pentest Externe	Application Web	2	R6	Il est recommandé de protéger les utilisateurs en intégrant une analyse antivirale des fichiers uploadés contre d'éventuelles attaques virales. Ce mécanisme peut être effectué en amont (brique de filtrage sécurité type Firewall Applicatif WAF) ou directement à l'aide d'un antivirus type ClamAV sous Linux. Par ailleurs, la détection de pièce jointe malveillante doit faire l'objet d'une alerte de sécurité.	P3	EN COURS	CORRECTION D'ICI SEPTEMBRE 2023
V7	En cas d'inactivité, la session reste active pendant plus d'une heure	Pentest Externe	Application Web	2	R7	Il est recommandé de diminuer la durée des sessions utilisateurs afin de respecter la politique de sécurité Waynes Enterprises. Habituellement ce paramètre est positionné pour une valeur inférieure à 30 minutes. PHP met à disposition les fonctions "ini_set('session.gc_maxlifetime', 1800)", pour la durée des sessions côté serveur, et "session_set_cookie_params(1800)", pour la durée des cookies de sessions utilisateurs.	P3	EN COURS	CORRECTION D'ICI SEPTEMBRE 2023
V8	Plusieurs utilisateurs peuvent se connecter simultanément avec un même compte	Pentest Externe	Application Web	2	R8	L'accès à un compte doit être limité à un seul utilisateur simultanément. La connexion à l'application doit détruire les autres sessions existantes pour cet utilisateur.	P3	EN COURS	CORRECTION D'ICI SEPTEMBRE 2023
V9	Lors de la génération des graphiques en image/pdf, "highcharts" récupère les données via canal non chiffré	Pentest Externe	Application Web	2	R9	Les fonctionnalités d'export mises à disposition par highcharts doivent être revues afin d'être executées dans la mesure du possible en local (backend BATMANAPP). Dans le cas ou ce n'est pas réalisable, il est nécessaire d'envoyer les données à minima sur un canal chiffré (HTTPS). Par ailleurs, il est recommandé d'informer les utilisateurs que l'application utilise les services d'une entreprise tierce (non francaise) pour la génération des graphes et PDF.	P3	EN COURS	CORRECTION D'ICI SEPTEMBRE 2023
ORG5	Définir un plan de gestion de crise	Entretiens techniques	Sécurité organisationnelle	2	R20	Un plan de gestion de crise décrit comment répondre à une situation critique qui affecterait négativement la rentabilité, la réputation ou la capacité de fonctionnement d'une organisation. Afin d'être prêt en cas de crise, nous recommandons à Waynes Enterprises de développer un plan de gestion de crise.	P3	PRÉVU	CORRECTION D'ICI SEPTEMBRE 2023
ORG6	Rédiger une politique de sécurité du développement	Entretiens techniques	Sécurité organisationnelle	2	R21	Afin de formaliser ses bonnes pratiques de développement, nous recommandons à Waynes Enterprises de rédiger une politique de sécurité du développement.	P3	PRÉVU	CORRECTION D'ICI SEPTEMBRE 2023
V10	Notre utilisateur de moindre privilège à pu se connecter à la messagerie "admin/messages"	Pentest Externe	Application Web	1	R10	Il est nécessaire de vérifier qu'un utilisateur à faible privilège n'a pas la possibilité d'accéder aux messages de l'administrateur	P3	EN COURS	CORRECTION D'ICI SEPTEMBRE 2023
V11	Un utilisateur peut, lors d'une commande, manipuler des quantités négatives pour obtenir des montants négatifs	Pentest Externe	Application Web	1	R11	Les valeurs envoyées par l'utilisateur doivent être vérifiées du côté serveur. Cette fonction doit être revue avant le passage en production de l'application.	P3	EN COURS	CORRECTION D'ICI SEPTEMBRE 2023
V12	Une page intitulée "/tests" est présente dans l'application	Pentest Externe	Application Web	1	R12	Cette page doit être retirée lors du passage en production de l'application	P3	EN COURS	CORRECTION D'ICI SEPTEMBRE 2023
ORG7	Réaliser un pré-audit ISO27001 pour définir le travail à faire avant l'audit de certification	Entretiens techniques	Sécurité organisationnelle	1	R22	Comme Waynes Enterprises a l'ambition d'être certifié ISO 27001, nous recommandons un pré-audit pour évaluer le travail restant.	P3	PRÉVU	CORRECTION D'ICI SEPTEMBRE 2023