Vuln	Description	Source	Périmètre	Criticité	Reco	Recommandation	Priorité	Etat	Dates de correction prévu
V1	Téléversement de fichiers sans restriction de type	Pentest Applicatif	Application Web	4	R1	Cette vulnérabilité réside dans le fait que l'API `/api/dropzone` n'effectue aucune vérification du type de contenu téléversé. Pour y remédier, il est recommandé, comme l'indique la documentation de Laravel, de valider systématiquement le type de fichier avant d'autoriser le téléversement. Cette validation doit être systématiquement effectuée pour chaque téléversement. Il est à noter que l'absence d'une telle validation sur un seul téléversement est suffisant pour exposer l'application, et donc le serveur l'hébergeant, à toutes les conséquences décrites dans la partie impact.	P1	EN COURS	CORRECTION D'ICI SEPTEMBRE 2025
V2	Pages administrateurs accessibles aux utilisateurs peu privilégiés	Pentest Applicatif	Application Web	4	R2	Il est recommandé de mettre en place une vérification systématique des permissions d'accès aux différentes pages, en particulier dans le cas de requêtes normalement réservées aux administrateurs.	P1	CORRIGÉ	18/11/2024
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. Pour ce faire, il est recommandé d'utiliser 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 2025
V3	Absence de neutralisation des éléments spéciaux SQL (SQLi)	Pentest Applicatif	Application Web	4	R3	Il est recommandé de systématiquement utiliser des requêtes préparées pour interagir avec votre base de données afin de prévenir les attaques par injection SQL (SQLi). Pour ce faire, il est conseillé d'utiliser les fonctionnalités de PDO (PHP Data Objects) ou MySQLi, qui permettent de lier les paramètres de manière sécurisée (requêtes préparées). Cela garantira que les entrées utilisateur sont traitées comme des données et non comme des instructions SQL.	P2	CORRIGÉ	18/11/2024
V4	Absence de neutralisation des entrées (XSS)	Pentest Applicatif	Base de données	4	R4	Il est recommandé de systématiquement encoder les caractères spéciaux dans les entrées utilisateur afin de les rendre inoffensives côté client. Pour ce faire, il est recommandé d'utiliser la fonction PHP htmlspecialchars().	P2	EN COURS	CORRECTION D'ICI SEPTEMBRE 2025
V5	Les attributs de sécurité des cookies ne sont pas configurés	Pentest Applicatif	Application Web	3	R5	Il est recommandé de modifier le fichier de configuration PHP (php.ini) de sorte que le cookie de session dispose des attributs Secure et httpOnly.	P2	EN COURS	CORRECTION D'ICI SEPTEMBRE 2025
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, il est recommandé à Waynes Enterprises de développer un PCA.	P2	PRÉVU	CORRECTION D'ICI SEPTEMBRE 2025
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, il est recommandé à Waynes Enterprises de développer un DRP.	P2	PRÉVU	CORRECTION D'ICI SEPTEMBRE 2025
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/@muditha dul/little-things-if-world-need-it-4862e68453e0	P2	PRÉVU	CORRECTION D'ICI SEPTEMBRE 2025
V6	Absence de restrictions en cas de tentatives d'authentification excessives	Pentest Applicatif	Application Web	3	R6	Il est recommandé de mettre en place un verrouillage du compte qui empêche toute nouvelle tentative de connexion pendant une certaine période après un certain nombre d'échecs. Le compteur de tentatives de connexion infructueuses devrait être lié au compte plutôt qu'à l'adresse IP source afin de contrecarrer les adversaires qui tentent de se connecter à partir de plusieurs adresses IP. Voici une proposition : - Le nombre de tentatives infructueuses avant que le compte ne soit verrouillé, également appelé seuil de verrouillage, devrait être de 5 tentatives. - La période pendant laquelle ces tentatives doivent avoir lieu, aussi appelée fenêtre d'observation, devrait être de 5 minutes. - La durée durant laquelle le compte est bloqué, c'est-à-dire la durée du blocage, devrait être de 10 minutes. Lors de la création d'un système de verrouillage de compte, il est essentiel de s'assurer qu'il ne peut pas être exploité pour provoquer un déni de service en verrouillant des comptes appartenant à d'autres utilisateurs. Une précaution possible consiste à permettre aux utilisateurs de se connecter en utilisant la fonction de mot de passe oublié, même si leur compte est actuellement verrouillé. De plus, il est recommandé d'utiliser un système CAPTCHA robuste pour contrecarrer les tentatives de connexion automatique aux comptes utilisateurs. Néanmoins, de nombreuses implémentations de	P2	EN COURS	CORRECTION D'ICI SEPTEMBRE 2025
V7	L'authentification repose sur un facteur unique	Pentest Applicatif	Application Web	2	R7	Il est recommandé de permettre aux utilisateurs de configurer une authentification à facteur multiple s'ils le désirent. Pour se faire, il est recommandé de vous baser sur un algorithme permettant de générer un mot de passe à usage unique comme le TOTP (Time based One Time Password en anglais) celui-ci étant largement supportés par les appareils mobiles. Dans l'idéal, pour les utilisateurs les plus privilégiés, comme les administrateurs par exemple, cette configuration devrait être obligatoire.	P2	EN COURS	CORRECTION D'ICI SEPTEMBRE 2025
V8	Disparité de réponse observable entre les requêtes d'authentification	Pentest Applicatif	Application Web	2	R8	Il est recommandé de faire en sorte que pour tous les mécanismes d'authentification (connexion, réinitialisation du mot de passe ou récupération du mot de passe), l'application réponde par un message d'erreur générique, indépendamment du fait que le nom d'utilisateur ou le mot de passe soient incorrect ou non. L'objectif est d'empêcher la création d'un facteur de divergence, permettant à un attaquant n'énumérer des utilisateurs sur l'application.	P3	EN COURS	CORRECTION D'ICI SEPTEMBRE 2025
V9	Exigences insuffisantes en matière de mot de passe	Pentest Applicatif	Application Web	2	R9	Il est recommandé d'augmenter la longueur minimale des mots de passe pour atteindre à minima 10 caractères. Dans l'idéal, cette longueur devrait atteindre 12 caractères afin de garantir une sécurité optimale. De la même manière, il est recommandé d'exiger que les mots de passe soient complexes, c'est-à-dire qu'ils comportent au moins 3 types de caractères parmi les 4 que sont les majuscules, les minuscules, les chiffres et les caractères spéciaux.	P3	EN COURS	CORRECTION D'ICI SEPTEMBRE 2025
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, il est recommandé à Waynes Enterprises de développer un plan de gestion de crise.	P3	PRÉVU	CORRECTION D'ICI SEPTEMBRE 2025
ORG6	Rédiger une politique de sécurité du développement	Entretiens techniques	Sécurité organisationnelle	2	R21	Afin de formaliser ses bonnes pratiques de développement, il est recommandé à Waynes Enterprises de rédiger une politique de sécurité du développement.	P3	PRÉVU	CORRECTION D'ICI SEPTEMBRE 2025
V10	Utilisation d'un algorithme de hachage faible pour stocker les mots de passe	Pentest Applicatif	Application Web	2	R10	Il est recommandé de mettre à jour l'algorithme de hachage de mot de passe de votre application vers bcrypt, un algorithme de hachage moderne et sûr. Pour se faire, il est recommandé d'utiliser la fonction PHP password_hash($password, PASSWORD_DEFAULT), la valeur de PASSWORD_DEFAULT étant définie à bcrypt par défaut depuis PHP 5.5.0. En ce qui concerne le processus de mise à niveau, et comme indiqué dans la CheatSheet de l'OWASP, lorsque les utilisateurs s'authentifient, leurs mots de passe doivent être recalculés à l'aide du nouvel algorithme. Pour gérer la transition en douceur, vous pouvez adopter l'une des deux approches suivantes : - Première méthode de mise à niveau : expirez et supprimez les hachages de mots de passe des utilisateurs inactifs, en les invitant à réinitialiser leurs mots de passe lorsqu'ils se connectent à nouveau. Bien que sûre, cette approche peut gêner les utilisateurs et poser des problèmes au personnel d'assistance. - Deuxième méthode de mise à niveau : ajouter un algorithme plus sûr aux hachages de mots de passe existants. Par exemple, vous pourriez passer de md5($password) à bcrypt(md5($password)). Notez toutefois que cette approche pourrait rendre les hachages plus faciles à décrypter. D'après l'expérience de l'auditeur, la première méthode est généralement préférée car elle garantit la sécurité la plus forte et ne nécessite que des modifications marginales du code.	P3	EN COURS	CORRECTION D'ICI SEPTEMBRE 2025
V11	Absence de l'en-tête HSTS	Pentest Applicatif	Application Web	2	R11	Il est recommandé d'activer cet en-tête sur tous les sous-domaines afin de garantir que toute tentative d'accès au serveur via HTTP sera convertie en HTTPS par les navigateurs clients. Les valeurs suivantes sont recommandées : Strict-Transport-Security: max-age=31536000; includeSubDomains; Il convient de noter qu'une fois qu'un site web a activé HSTS et que le navigateur a mis en cache la politique HSTS, il peut être difficile de revenir à des connexions non-HTTPS jusqu'à ce que la durée spécifiée de la politique expire. Il s'agit là d'une volonté de garantir aux utilisateurs une expérience de navigation cohérente et sûre. En outre, et comme le suggère l'OWASP CheatSheet associé et lié ci-dessous, il est recommandé d'essayer d'abord de fixer un âge maximum très court en cas d'erreurs lors du déploiement initial avant de mettre en œuvre un âge maximum de 1 ou 2 ans.	P3	EN COURS	CORRECTION D'ICI SEPTEMBRE 2025
V12	Absence de l'en-tête CSP	Pentest Applicatif	Application Web	2	R12	Comme le recommande l'évaluateur CSP de Google, l'application web doit appliquer la politique de sécurité de contenu la plus stricte possible. Voici une proposition tirée de l'exemple de règles de sécurité de Google : script-src 'strict-dynamic' 'nonce-rAnd0m123' 'unsafe-inline' http: https:; object-src 'none'; base-uri 'none'; require-trusted-types-for 'script'; frame-ancestors 'self';	P3	EN COURS	CORRECTION D'ICI SEPTEMBRE 2025
ORG7	Réaliser un pré-audit ISO27001 pour définir le travail à faire avant l'audit de certification	Entretiens techniques	Sécurité organisationnelle	1	R22	Waynes Enterprises ayant pour ambition d'être certifié ISO 27001, il est recommandé de réaliser un pré-audit afin d'évaluer le travail restant.	P3	PRÉVU	CORRECTION D'ICI SEPTEMBRE 2025
V13	La fonctionnalité de déconnexion n'invalide pas le cookie de session	Pentest Applicatif	Application Web	1	R13	Comme conseillé dans la documentation de PHP, il est recommandé d'utiliser la méthode session-destroy() afin de supprimer les informations d'authentification de la session de l'utilisateur, de sorte que les demandes ultérieures ne soient pas authentifiées.	P3	EN COURS	CORRECTION D'ICI SEPTEMBRE 2025
V14	L'en-tête Server divulgue la version d'Apache utilisée	Pentest Applicatif	Application Web	1	R14	Dans un premier temps, il est recommandé de mettre à jour Apache vers sa dernière version, soit la 2.4.61 au moment de la rédaction du présent rapport. Par ailleurs, il est également recommandé de configurer la directive ServerTokens à la valeur Prod dans le fichier de configuration Apache2.	P4	EN COURS	CORRECTION D'ICI SEPTEMBRE 2025