

Consigner les preuves. Suivre les corrections.

La grille de travail à remplir pendant l'audit et après chaque retest.

72 fiches de contrôle interactives

Statut, preuves, fichier et ligne, risque, scénario, correction, test, résultat et suivi. Les champs sont prévus pour des synthèses ; conserver les pièces longues dans un dossier de preuves référencé.

OWASP ASVS 5.0.0 • API Security Top 10 2023
Complément LLM 2025 lorsque applicable

Téléchargement gratuit • Version datée • Sources officielles

FICHE DE CONTEXTE

Définir le dossier et son périmètre

Application / propriétaire / responsable de la décision

Code, commit ou empreinte / artefact / date de référence

Environnements, domaines et points d'entrée autorisés

Composants inclus et exclus / pièces manquantes

Accord, fenêtre, volumes, budget et seuils d'arrêt des essais

Comptes fictifs, organisations, prestataires simulés et moyens de contact

MODE D'EMPLOI

Remplir les résultats sans perdre les preuves

Utiliser un lecteur compatible formulaires

Les PDF de formulaire fonctionnent dans les lecteurs prenant en charge les champs AcroForm. Enregistrez une copie, remplissez un champ et rouvrez-la pour vérifier la conservation. Les prévisualisations intégrées n'affichent pas toujours tous les champs. Le document reste imprimable.

Quatre statuts et aucune conclusion initiale

Toutes les fiches commencent à UNKNOWN : aucun test n'est réalisé. PASS exige une preuve adaptée ; FAIL exige un écart établi ; N/A exige une justification. Distinguez une hypothèse d'exploitation d'un résultat reproduit. Un critère essentiel inconnu empêche de valider tout le contrôle.

Renseigner les emplacements

Indiquez le fichier et la ligne, le symbole et le commit, ou le service/paramètre cloud daté. Ajoutez un identifiant de preuve interne. Ne collez ni clé complète, ni cookie, ni document client. Préservez aussi le résultat avant correction.

Décrire le test et son observation

Le test proposé n'est pas un test exécuté. Renseignez procédure, attendu, observé, version et environnement. Si les champs sont trop courts, indiquez un renvoi vers une pièce expurgée. Les champs défilants ne montrent pas forcément tout leur texte à l'impression.

Lire avec le guide

Chaque fiche rappelle l'exigence ; le guide fournit le scénario fictif, la correction de principe, le test et ses références. Les deux documents partagent les mêmes identifiants C01 à C72. La date de cette édition ne remplace pas la date réelle de vos essais.

MODULE 01 • FICHES DE RÉSULTAT

Périmètre et modèle de menace

C01 Version et surface examinée

Relier les résultats à un code, un artefact et des environnements identifiés.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C02 Données et frontières de confiance

Identifier les données sensibles et leurs chemins entre navigateur, serveur, prestataires et stockage.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 01 • FICHES DE RÉSULTAT

Périmètre et modèle de menace

C03 Profils, adversaires et invariants

Définir les actions permises et les propriétés qui doivent rester vraies, même en cas d'abus.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C04 Cadre des essais actifs

Tester sur un périmètre autorisé avec un impact borné et une procédure d'arrêt.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 01 • FICHES DE RÉSULTAT

Périmètre et modèle de menace

C05 Preuves et couverture de revue

Rendre visible ce qui a été lu, exécuté, exclu ou seulement supposé.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C06 Configuration extérieure au dépôt

Inclure les protections réelles de l'hébergement, de l'identité, du stockage et de la facturation.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 02 • FICHES DE RÉSULTAT

Secrets et chaîne de livraison

C07 Secrets dans le dépôt et l'historique

Détecter les secrets exposés, y compris dans les anciennes révisions et livrables.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C08 Secrets dans le navigateur

Distinguer clés publiables prévues à cet effet et secrets donnant des privilèges.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 02 • FICHES DE RÉSULTAT

Secrets et chaîne de livraison

C09 Gestion et rotation des secrets

Limiter l'accès, la durée et l'étendue des secrets utilisés par chaque composant.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C10 Dépendances et provenance

Connaître les versions réellement livrées et traiter les avis qui les concernent.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 02 • FICHES DE RÉSULTAT

Secrets et chaîne de livraison

C11 Droits de livraison et environnements

Empêcher une contribution non approuvée de lire des secrets ou de déployer en production.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C12 Fichiers et interfaces techniques exposés

Exclure secrets, dépôts, sauvegardes, diagnostics et consoles du périmètre public.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 03 • FICHES DE RÉSULTAT

Authentification et comptes

C13 Stockage des mots de passe

Rendre une fuite de la base difficile à convertir en mots de passe utilisables.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C14 Politique de mot de passe et énumération

Écarter les secrets triviaux sans révéler les comptes existants ni gêner les gestionnaires.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 03 • FICHES DE RÉSULTAT

Authentification et comptes

C15 Brute force et inscriptions abusives

Limiter les tentatives et créations automatisées sans blocage permanent facile d'un compte tiers.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C16 Authentification renforcée et secours

Protéger les comptes privilégiés et empêcher le contournement par la récupération.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 03 • FICHES DE RÉSULTAT

Authentification et comptes

C17 Récupération, invitations et changement d'adresse

Lier chaque lien sensible au bon compte, au bon usage et à une durée limitée.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C18 Connexion déléguée OAuth et OIDC

Accepter seulement une réponse liée au parcours initié et à l'identité attendue.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 04 • FICHES DE RÉSULTAT

Sessions et jetons

C19 Cookies et stockage des jetons

Limiter le vol des jetons et leur transmission hors du contexte prévu.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis	Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C20 Validation des JWT et assertions

Ne jamais confondre décodage du contenu et validation cryptographique.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis	Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 04 • FICHES DE RÉSULTAT

Sessions et jetons

C21 Création, rotation et fixation de session

Renouveler l'identité de session lors de l'authentification et des transitions sensibles.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis	Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C22 Expiration et réauthentification

Borner la durée d'accès et vérifier à nouveau l'identité pour les actions à enjeu.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis	Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 04 • FICHES DE RÉSULTAT

Sessions et jetons

C23 Déconnexion et retrait des droits

Faire cesser les accès retirés, y compris avec un jeton précédemment émis.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C24 Renouvellement et rejeu des refresh tokens

Empêcher un jeton de renouvellement ancien de recréer indéfiniment des accès.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 05 • FICHES DE RÉSULTAT

Autorisations et séparation des clients

C25 Accès aux objets d'un autre utilisateur

Vérifier la propriété ou le droit explicite sur chaque ressource, pour chaque opération.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C26 Rôles, administration et champs sensibles

Contrôler à la fois les fonctions accessibles et les propriétés modifiables.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 05 • FICHES DE RÉSULTAT

Autorisations et séparation des clients

C27 Séparation des organisations et des caches

Conserver l'isolation dans les requêtes, les fichiers, les tâches et les résultats mis en cache.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C28 Permissions de base et politiques par ligne

Vérifier les politiques avec le rôle réellement employé par chaque parcours.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 05 • FICHES DE RÉSULTAT

Autorisations et séparation des clients

C29 Services, tâches et accès internes

Authentifier les appels techniques et restreindre leurs droits au besoin réel.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C30 Défaillance des contrôles et accès obsolètes

Refuser une opération sensible lorsque son autorisation ne peut pas être établie.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 06 • FICHES DE RÉSULTAT

Entrées et navigateur

C31 Schémas et limites des entrées

Valider au serveur types, tailles, formats et cohérence métier.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C32 Injections SQL et requêtes de données

Séparer les données utilisateur de la structure exécutée par le moteur.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 06 • FICHES DE RÉSULTAT

Entrées et navigateur

C33 XSS et rendu HTML ou Markdown

Traiter textes, imports et sorties IA comme des données non fiables.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis	Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C34 CSRF et actions déclenchées par le navigateur

Empêcher un site tiers de déclencher une action protégée à l'insu du visiteur.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis	Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 06 • FICHES DE RÉSULTAT

Entrées et navigateur

C35 Commandes, modèles, XML et désérialisation

Éviter qu'un contenu reçu commande le système, un moteur de modèle ou un parseur.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C36 Protections du navigateur et ressources tierces

Réduire les conséquences d'un contenu injecté ou d'une dépendance chargée à distance.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 07 • FICHES DE RÉSULTAT

API et communications

C37 CORS et origines autorisées

N'autoriser les lectures interorigines privées que pour les clients prévus.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C38 SSRF et récupération d'URL

Restreindre les destinations réellement jointes, après résolution et redirection.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 07 • FICHES DE RÉSULTAT

API et communications

C39 TLS, certificats et en-têtes de proxy

Protéger le transport et ne croire que les informations ajoutées par les intermédiaires approuvés.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C40 Routes, méthodes et versions d'API

Appliquer les mêmes exigences aux routes alternatives et aux opérations par lots.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 07 • FICHES DE RÉSULTAT

API et communications

C41 GraphQL, WebSocket et flux longs

Contrôler complexité, messages et autorisations tout au long de la connexion.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C42 Réponses et intégrations de services tiers

Valider les données reçues sans leur accorder une confiance implicite.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 08 • FICHES DE RÉSULTAT

Fichiers et cycle de vie des données

C43 Validation des fichiers reçus

Contrôler formats et volumes avant les étapes coûteuses.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C44 Archives, chemins et traitement des fichiers

Borner le volume décompressé et empêcher l'écriture hors de la zone prévue.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 08 • FICHES DE RÉSULTAT

Fichiers et cycle de vie des données

C45 Stockage privé, partage et téléchargement

Conserver les droits jusqu'au téléchargement et neutraliser le contenu actif.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C46 Chiffrement et protection des clés

Adapter la protection aux données, y compris les sauvegardes et les métadonnées.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 08 • FICHES DE RÉSULTAT

Fichiers et cycle de vie des données

C47 Rétention, effacement et prestataires

Définir les copies conservées, leurs destinataires et leur suppression vérifiable.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C48 Brouillons, exports et poste partagé

Éviter les fuites après déconnexion et les interprétations actives lors des exports.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 09 • FICHES DE RÉSULTAT

Intégrité et paiements

C49 Transitions et règles métier

Imposer l'ordre et les conditions des opérations au serveur.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis	Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C50 Écritures concurrentes et cohérence

Éviter pertes de mises à jour et dépassements lors d'opérations simultanées.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis	Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 09 • FICHES DE RÉSULTAT

Intégrité et paiements

C51 Idempotence et réponse perdue

Reconnaître une répétition de la même opération sans en doubler les effets.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C52 Prix, paiement et activation

Calculer le montant au serveur et activer le droit seulement après vérification fiable.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 09 • FICHES DE RÉSULTAT

Intégrité et paiements

C53 Webhooks signés, rejoués ou désordonnés

Authentifier la notification et appliquer une seule transition métier cohérente.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Responsable / échéance / retest et version corrigée / état de déploiement

C54 Enregistrement, conflits et états d'interface

Ne confirmer que les résultats connus et préserver la cohérence des reprises.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 10 • FICHES DE RÉSULTAT

IA, outils et dépenses

C55 Injection de prompt directe et indirecte

Empêcher les contenus non fiables de décider des droits ou des actions de l'application.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C56 Outils et actions des agents

Limiter les actions à des capacités explicitement autorisées pour le compte courant.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 10 • FICHES DE RÉSULTAT

IA, outils et dépenses

C57 RAG, index et séparation documentaire

Filtrer les documents selon les droits avant leur entrée dans le contexte du modèle.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C58 Sorties IA, confidentialité et décisions

Valider le résultat avant affichage, exécution, stockage ou décision sensible.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 10 • FICHES DE RÉSULTAT

IA, outils et dépenses

C59 Quotas, concurrence et budget atomique

Vérifier l'abonnement et réserver un coût borné avant de déclencher la dépense.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Responsable / échéance / retest et version corrigée / état de déploiement

C60 Coupe-circuit financier et plafonds fournisseur

Arrêter les nouvelles dépenses avant une dérive incontrôlée.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 11 • FICHES DE RÉSULTAT

Disponibilité et maîtrise de la charge

C61 Débit et automatisisation des parcours

Limiter les abus par opération sans se contenter d'un compteur IP global.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C62 Files, traitements et surcharge

Limiter les tâches en attente et en cours ; préserver les parcours essentiels.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 11 • FICHES DE RÉSULTAT

Disponibilité et maîtrise de la charge

C63 Délais, flux et annulation

Donner une fin à chaque attente et libérer les ressources devenues inutiles.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C64 Reprises et propagation des pannes

Éviter de multiplier erreurs, effets métier et dépenses en cas de panne.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis

Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 11 • FICHES DE RÉSULTAT

Disponibilité et maîtrise de la charge

C65 Saturation de la base et du stockage

Borner connexions, requêtes et volumes pour éviter l'épuisement partagé.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C66 Charge, pics et récupération

Mesurer un niveau de service et ses limites sur une charge explicitement définie.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 12 • FICHES DE RÉSULTAT

Production, détection et reprise

C67 Journaux utiles et non divulguants

Tracer les événements nécessaires sans fabriquer un nouveau dépôt de secrets.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis	Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C68 Erreurs publiques et comportement sûr

Fournir un message utile sans exposer les détails internes ni transformer une panne en succès.

Statut	Gravité si établie	Date / version examinée
UNKNOWN	Non evaluee	

Preuve précise / fichier et ligne / configuration / référence de pièce

Risque / impact et prérequis	Scénario observé ou hypothétique (préciser)

Correction proposée / justification N/A si concerné

Test / attendu / observé / exécution ou Non exécuté (renvoi possible)

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 12 • FICHES DE RÉSULTAT

Production, détection et reprise

C69 Monitoring et alertes reçues

Détecter panne, abus et dérive financière avec une personne en mesure d'agir.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C70 Sauvegarde et restauration démontrée

Récupérer un ensemble cohérent dans les délais de perte et de reprise acceptés.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

MODULE 12 • FICHES DE RÉSULTAT

Production, détection et reprise

C71 Artefact, migrations et retour arrière

Livrer la version testée et savoir retrouver un état exploitable après échec.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

C72 Incident, clôture et réévaluation

Désigner qui décide, intervient et confirme les corrections sur la version cible.

Statut

UNKNOWN

Gravité si établie

Non evaluee

Date / version examinée**Preuve précise / fichier et ligne / configuration / référence de pièce****Risque / impact et prérequis****Scénario observé ou hypothétique (préciser)****Correction proposée / justification N/A si concerné****Test / attendu / observé / exécution ou Non exécuté (renvoi possible)**

Non exécuté

Responsable / échéance / retest et version corrigée / état de déploiement

SYNTHÈSE

Hiérarchiser les constats et les inconnues

Critical — identifiants des constats, impact, preuve et action

High — identifiants des constats, impact, preuve et action

Medium — identifiants, priorité et responsable

Low — identifiants et suivi

UNKNOWN déterminants — information manquante, preuve attendue, responsable et échéance

Couverture réelle — surfaces non examinées, tests non exécutés et limites des simulations

MISE EN LIGNE

Acter la décision et programmer la suite

Règle de décision

Ne pas calculer une moyenne de sécurité. Un UNKNOWN déterminant reste à résoudre. Un défaut corrigé dans le code doit encore être retesté et son déploiement vérifié.

Décision dans le périmètre examiné

A décider

Blocages restants et conditions précises de levée

Risques résiduels / mesures temporaires / fonctions retirées ou restreintes

Décideur / relecteur / date / version et environnement concernés

Prochaine revue / déclencheurs / responsables / références des preuves finales

Contacts incident / arrêt des dépenses / révocation / restauration

Référentiel du dossier : ASVS 5.0.0, API Security Top 10 2023, complément LLM 2025. Sélection pédagogique, sans certification. Sources et méthode : document 01. © IN DATA VERITAS • CC BY-SA 4.0.