BORDEAUX
ynov
CAMPUS

RAPPORT DE STAGE

Tom Mallor

Formation : Bachelor Informatique - 2ème année

REMERCIEMENTS

Je tiens à exprimer ma gratitude à l'entreprise repply pour la confiance qu'elle m'a accordée.

Je remercie tout particulièrement :
- M. Mathieu René, Directeur Général, pour son accueil et sa confiance.
- M. Clément Bourgeois, Lead Dev, pour son accompagnement, ses conseils et le partage de son expertise.
- M. Romain Jarry, référent du pôle RGPD/Sécurité, pour nos précieux échanges.

Ce stage a constitué une expérience formatrice qui m'a permis d'affiner mes choix d'orientation professionnelle et d'aboutir à un premier bilan concret de mes compétences.

Table des matières

1. Introduction

Dans le cadre de ma deuxième année de Bachelor Informatique, j'ai réalisé un stage de six semaines au sein de l'entreprise repply, éditeur de logiciels, basée à La Rochelle.

Mon objectif principal était de consolider mes connaissances en cybersécurité et en infrastructure, tout en découvrant le fonctionnement opérationnel d'une entreprise spécialisée dans les solutions numériques.

Durant mon stage, j'ai intégré l'équipe technique, sous la supervision de Mathieu RENE, Clément BOURGEOIS et Romain JARRY.

J'ai été chaleureusement accueilli par le directeur, **Monsieur RENE**, qui m'a exposé sa vision et les valeurs de l'entreprise :

- repply a pour mission d'accompagner les entreprises et les services publics dans leur transition numérique ;
- La valeur de l'entreprise est la pleine satisfaction du client.

J'ai participé à plusieurs missions axées sur la sécurité applicative, la gestion d'infrastructure et le développement de correctifs logiciels. Cette immersion m'a permis de découvrir le quotidien d'une entreprise du numérique, tout en mettant en pratique mes connaissances acquises en formation.

2. Présentation de l'entreprise repply

2.1 Informations générales

repply est un éditeur de logiciels sur mesure travaillant avec de grands acteurs du secteur de l'énergie, tel qu'Enedis. Son expertise se concrétise à travers la suite logicielle MAIIA, composée de plusieurs applications métiers :

- **Hopii – Pilotage des opérations**
  Outil d'aide au pilotage des opérations, affaires et interventions, Hopii est né de l'expertise de repply auprès de nombreux syndicats d'énergie et gestionnaires de réseaux.
  Il centralise l'ensemble des processus liés à la conduite d'opérations (énergie, eau, éclairage public…) et propose une interface claire permettant une meilleure organisation et une mutualisation des efforts entre acteurs du secteur.

- **Assainii – Gestion des contrôles d'assainissement**
  Application destinée aux **SPANC** (Service Public d'Assainissement Non Collectif) et **SPAC** (Service Public d'Assainissement Collectif).
  Assainii centralise et dématérialise les données liées aux contrôles de conformité des installations, afin de garantir une gestion fluide, traçable et conforme à la réglementation en vigueur. Compatible sur tablette, elle facilite le travail des agents terrain grâce à une synchronisation en temps réel.

- **Géolii – Gestion des Servitudes d'Utilité Publique (SUP)**
  Application SaaS permettant aux gestionnaires de réseaux (électricité, gaz, eau) de remplir leur obligation de dépôt des SUP sur le **Géoportail de l'urbanisme**.
  Elle repose sur le standard national de dématérialisation des SUP et prend en charge les différentes catégories (I4, I5, AS1).

- **Momii – Archivage électronique sécurisé**
  Solution moderne d'archivage électronique, Momii permet de stocker tous types de fichiers de manière sécurisée, sans limite de taille, de durée ou de volume.
  Connectable via API aux autres applications métiers, Momii garantit l'intégrité des données archivées, tout en contribuant à réduire l'usage du papier et à faciliter la conservation de documents à long terme.

L'entreprise est dynamique et l'équipe se distingue par sa pédagogie, son écoute, et sa volonté d'accompagner la montée en compétences de ses collaborateurs, y compris des stagiaires. L'ambiance de travail y est conviviale, studieuse et collaborative, offrant un cadre propice à l'apprentissage et à la participation active à des projets concrets.

2.2 Organisation interne

Les équipes de l'entreprise suivent une organisation collaborative et structurée, favorisant la communication et l'efficacité dans la gestion des projets.

Plusieurs outils sont utilisés au quotidien :

- **Slack** : pour la messagerie instantanée, les échanges rapides, le partage de fichiers et la coordination en temps réel entre les membres de l'équipe.
- **Atlassian Jira** : pour la gestion de projet, le suivi des tâches et des tickets, l'attribution des missions à chaque collaborateur et la visualisation de l'avancement des projets.
- **Confluence** : pour la documentation interne, la rédaction et le partage de rapports, guides, procédures et comptes-rendus de réunions.
- **Bitbucket** : pour l'hébergement et la gestion collaborative du code source, à la manière de GitHub. Bitbucket permet de versionner les projets, de gérer les branches, de faire des pull requests et de collaborer efficacement sur le développement logiciel.

Cette méthodologie permet de fluidifier la collaboration et de garantir une traçabilité efficace des projets.
Par exemple :

- J'ai participé à des discussions sur Slack pour demander de l'aide ou valider des choix techniques ;
- J'ai suivi l'évolution de mes missions via des tickets Jira ;
- J'ai consulté ou rédigé des documents sur Confluence pour garder une trace des travaux réalisés ;
- Et j'ai collaboré sur le code source avec Bitbucket pour versionner les projets et valider les modifications via des pull requests.

Cette organisation permet à chacun de savoir précisément qui fait quoi, d'assurer la continuité des projets et de capitaliser sur les connaissances partagées au sein de l'équipe.

3. Objectifs du stage

Les objectifs fixés en début de stage étaient :

- Me conforter dans mon choix de spécialisation en cybersécurité ;
- Participer à des missions concrètes dans trois domaines clés :
  - **Sécurité** : participation à des tests d'intrusion sur les applications développées par l'entreprise, ainsi qu'à des réflexions sur la gestion et la protection des données personnelles ;
  - **Infrastructure** : gestion et automatisation des mises à jour des serveurs, réalisation d'un état des lieux et mise en place d'une organisation adaptée ;
  - **Développement** : réalisation de développements correctifs simples en C#, ainsi que le paramétrage de templates pour améliorer la productivité de l'équipe.

4. Missions et réalisations

4.1 Infrastructure et automatisation

Automatisation avec Ansible

Familiarisation et premières contributions

Ma principale mission a été de démarrer le développement de scripts d'automatisation avec **Ansible**. J'ai commencé par me familiariser avec l'outil et sa structure, en travaillant sur :

- L'architecture des rôles,
- La définition de l'inventaire,
- La configuration des tâches de base pour la mise en place de serveurs.

J'ai notamment créé un rôle Ansible pour la **gestion des utilisateurs**, qui automatise la création d'un utilisateur système et l'installation de protections comme **UFW** et **SSHGuard**. Ce rôle modulaire renforce les bonnes pratiques de sécurité de l'entreprise.

Automatisation de PostgreSQL et gestion des accès temporaires

J'ai ensuite développé un rôle Ansible complet destiné à installer et configurer **PostgreSQL** sur des serveurs Linux.

En parallèle, j'ai conçu un **playbook** permettant de créer des utilisateurs temporaires à la fois :

- Sur le serveur Linux (via ansible.builtin.user),
- Et dans PostgreSQL (via community.postgresql.postgresql_user).

Ces utilisateurs sont générés avec des **mots de passe aléatoires** créés dynamiquement dans le playbook et sont automatiquement supprimés après 24 h. Ce mécanisme améliore la sécurité des accès ponctuels (consultants, collaborateurs externes) sans intervention manuelle.

Mise en place d'une autorité de certification SSH (CA SSH)

Une autre mission importante a été la création d'un rôle Ansible permettant d'ajouter automatiquement une **Certificate Authority (CA) SSH** sur les serveurs.

Pourquoi ?
La gestion manuelle des clés SSH devient rapidement complexe dans un environnement étendu. Grâce au CA SSH, il n'est plus nécessaire de stocker chaque clé publique sur chaque serveur : seules les clés **signées** par l'autorité interne sont acceptées.

Automatisation réalisée avec Ansible :

- Ajout du fichier trusted_user_ca_keys contenant la clé publique du CA,
- Configuration de sshd_config avec la directive TrustedUserCAKeys,
- Redémarrage contrôlé du service SSH pour appliquer la configuration.

Ce rôle assure une gestion centralisée, sécurisée et évolutive des connexions SSH dans l'infrastructure.

Déploiement d'un registre OCI avec Zot

J'ai également travaillé sur un rôle Ansible pour déployer **Zot**, un registre d'images OCI (alternative légère à Harbor ou Docker Registry).

Atouts de Zot :

- Léger et rapide à déployer,
- Exécutable en mode *rootless* pour plus de sécurité,
- Support natif de la signature, des scans de vulnérabilités et de l'authentification,
- Intégration fluide dans des pipelines CI/CD modernes (GitLab, GitHub Actions).

Objectif du rôle Ansible :

- Téléchargement et configuration du binaire Zot,
- Création d'un service systemd pour l'exécution persistante,
- Paramétrage des options (authentification, TLS, stockage),
- Intégration au SI pour héberger et tester des images locales.

Ce rôle m'a permis de renforcer mes compétences en gestion de services Linux et en intégration d'outils DevOps modernes.

Travaux en production

Enfin, j'ai poursuivi mes travaux d'automatisation sur un **serveur en production**, destiné à l'un des prochains clients de l'entreprise, pour les applications **Assainii** et **Hopii**.

Ce travail s'est appuyé sur les rôles Ansible développés en amont (socle de base, rôles applicatifs, configurations spécifiques), afin de **normaliser et fiabiliser** les installations.

4.2 Cybersécurité et conformité RGPD

En parallèle de mes missions sur ansible, j'ai eu l'opportunité de collaborer avec l'équipe du pôle RGPD/sécurité. Ces expériences, en lien direct avec ma future spécialisation en cybersécurité, m'ont permis d'aborder la sécurité des systèmes d'information sous plusieurs angles : technique, organisationnel et réglementaire.

Audit de sécurité de l'application Assainii

J'ai conduit un audit de cybersécurité sur l'application web **Assainii**, développée par repply pour la gestion des contrôles d'assainissement.
L'objectif était de tester la robustesse de l'application et de son infrastructure face aux menaces. Pour cela, j'ai appliqué une méthodologie structurée :

- **Prise en main** : analyse des fonctionnalités et identification des zones sensibles (formulaires, endpoints, entrées utilisateurs…).
- **Scan technique** : reconnaissance de l'environnement (serveurs, versions, services ouverts) avec des outils comme **Nmap**.
- **Phase offensive** : détection de vulnérabilités potentielles (XSS, injections, erreurs de configuration…).
- **Rédaction d'un rapport** : documentation détaillée des failles et recommandations de correction.

Outils mobilisés :

- **BurpSuite** : interception et modification de requêtes HTTP, tests de sécurité applicative.
- **Registre RGPD** : apprentissage de la documentation des traitements de données personnelles (finalité, durée, sous-traitants, mesures de protection).

Ce travail m'a permis de développer des compétences techniques en pentest tout en intégrant la **dimension légale et réglementaire** (protection des données personnelles).

Réunions et management du risque

J'ai participé à plusieurs réunions stratégiques centrées sur l'analyse et la gestion des risques, avec notamment l'utilisation de la **méthode EBIOS** de l'ANSSI.
Ces échanges m'ont permis de :

- Comprendre l'importance de la **prise de recul en cybersécurité**,
- Analyser des scénarios de menace réalistes (intrusions, fuites de données, erreurs humaines),
- Évaluer la gravité et la vraisemblance des risques,
- Réfléchir à des **mesures de prévention et de réaction** adaptées.

J'ai ainsi découvert comment la cybersécurité s'intègre dans une **vision globale d'entreprise**, mêlant technique, organisation et gouvernance.

Études et rapports de sensibilisation

Au cours du stage, j'ai également produit plusieurs rapports de veille et de sensibilisation :

- **IA et protection des données personnelles** : analyse des risques liés à l'utilisation de l'IA en entreprise, avec un focus sur la conformité RGPD et la gouvernance responsable.
- **Proposition d'architecture de supervision de sécurité** : comparaison des solutions (NIDS, SIEM, EDR, XDR) selon leur détection, leur complexité, leur coût et leur pertinence pour repply.
- **MaletteCyber (ANSSI & ACYMA)** : synthèse du kit de sensibilisation destiné aux PME (guides pratiques, outils, modules de formation, assistance cyber).
- **Guide d'hygiène informatique de l'ANSSI** : résumé des 42 règles de sécurité (séparation des privilèges, sauvegardes, blocage périphériques amovibles, authentification forte, limitation des accès par besoin métier).

Ces travaux m'ont permis de relier **veille technologique**, **cybersécurité opérationnelle** et **conformité réglementaire**.

Audit OSINT sur repply

J'ai aussi mené un audit **OSINT (Open Source Intelligence)** pour identifier les informations publiques concernant repply.
Sources utilisées : Google Dorking, réseaux sociaux (LinkedIn), archives, caches et forums.

Résultats :

- Aucune faille technique ni donnée sensible sur l'infrastructure.
- Présence de **données personnelles accessibles librement** (adresses e-mail, profils LinkedIn, photos), ce qui expose les collaborateurs à du **phishing ciblé**.

Bilan sécurité

Ces missions m'ont apporté une vision complète de la cybersécurité, mêlant :

- **Techniques d'audit** (pentest, OSINT, scans).
- **Pratiques organisationnelles** (analyse de risques, méthode EBIOS).
- **Approche réglementaire** (RGPD, hygiène informatique).
- **Sensibilisation et gouvernance** (rapports, veille, outils pédagogiques).

Elles ont constitué une **expérience déterminante** pour confirmer mon intérêt et mes compétences dans le domaine de la cybersécurité.

4.3 Développement – Sécurisation du code

Dans la partie développement, mes missions ont principalement porté sur la sécurisation du code. J'ai notamment travaillé sur l'évaluation et la comparaison de plusieurs logiciels spécialisés dans l'analyse de code source.

Rédaction de rapports techniques en cybersécurité

En milieu de semaine, j'ai rédigé un rapport comparatif d'outils d'analyse de code sécurisé. L'objectif était d'accompagner l'équipe de développement dans la mise en

place d'une production logicielle plus robuste, en identifiant les solutions capables de :

- Détecter automatiquement les vulnérabilités (XSS, injections, erreurs de logique…),
- S'intégrer efficacement dans leur pipeline CI/CD,
- Proposer une couverture adaptée au contexte de repply.

Outils étudiés

- **SonarQube** (Plateforme d'analyse de code statique qui détecte les bugs, vulnérabilités et problèmes de qualité. Elle s'intègre bien aux pipelines CI/CD et offre des tableaux de bord détaillés pour le suivi de la dette technique.)
- **SemgrepOutil** (open source d'analyse statique basé sur des règles personnalisables. Il est léger, rapide et particulièrement adapté à la recherche de patterns de sécurité ou de conformité dans le code.)
- **Snyk Code** (Solution SaaS qui analyse le code source et les dépendances pour identifier des vulnérabilités connues. Elle met l'accent sur la remédiation avec des suggestions de corrections intégrées.)
- **CodeQLMoteur** (d'analyse développé par GitHub qui permet d'interroger le code comme une base de données. Il est puissant pour détecter des vulnérabilités complexes grâce à des requêtes personnalisées.)

Axes d'analyse

Pour chaque outil, j'ai étudié :

- La facilité d'intégration,
- Les fonctionnalités de détection,
- Le type de licence (open source ou propriétaire),
- La pertinence dans le contexte spécifique de l'entreprise.

Résultats et impact

Ce travail a permis de poser les bases d'une stratégie de revue de code automatique plus rigoureuse et réactive. À terme, cette démarche vise à renforcer la qualité logicielle et à réduire les risques de vulnérabilités dans les applications développées.

5. Compétences acquises

Au cours de ces missions, j'ai pu développer et consolider plusieurs compétences clés dans le domaine du DevOps et de l'automatisation :

- **Maîtrise d'Ansible** : création de rôles et playbooks modulaires pour la gestion d'utilisateurs, de services et de configurations complexes.
- **Sécurisation des systèmes** : mise en place d'utilisateurs temporaires, intégration d'un CA SSH et configuration d'outils de protection (UFW, SSHGuard).
- **Administration de bases de données** : automatisation de l'installation et de la configuration de PostgreSQL, ainsi que de la gestion des comptes et droits d'accès.
- **Gestion de services Linux** : déploiement d'outils modernes comme Zot via systemd, avec une intégration dans les pipelines CI/CD.

Compétences acquises en cybersécurité

Au fil de ces missions, j'ai renforcé mes compétences techniques, méthodologiques et juridiques dans le domaine de la cybersécurité :

- **Audit de sécurité d'applications web** : mise en œuvre d'une méthodologie complète (reconnaissance, scans techniques, exploitation de failles, rédaction de rapports).
- **Utilisation d'outils spécialisés** : maîtrise accrue de BurpSuite, Nmap, et techniques d'OSINT (Google Dorking, veille réseaux sociaux).

- **Cybersécurité et conformité légale** : participation à la rédaction d'un registre RGPD, étude de la gouvernance des IA et de leur conformité à la protection des données personnelles.
- **Analyse et gestion des risques** : contribution à des ateliers EBIOS, compréhension des menaces (intrusions, phishing, erreurs humaines) et des mesures préventives adaptées.
- **Architecture de supervision de sécurité** : étude et comparaison de solutions (NIDS, SIEM, EDR, XDR), proposition d'un plan de surveillance scalable pour l'entreprise.
- **Veille et sensibilisation** : synthèses sur la MaletteCyber et le Guide d'hygiène informatique de l'ANSSI, afin de diffuser les bonnes pratiques et d'améliorer la posture de sécurité globale.

6. Conclusion et perspectives

Mon stage de six semaines chez repply a été une expérience d'apprentissage intense et extrêmement formatrice. Les objectifs que je m'étais fixés au début du stage, à savoir consolider mes connaissances en matière de cybersécurité et d'infrastructure tout en découvrant le fonctionnement d'une entreprise du secteur numérique, ont été pleinement atteints.
Ce stage m'a permis de mettre en pratique les concepts théoriques appris en formation, tout en travaillant sur des projets concrets et opérationnels. L'équipe m'a fait confiance et m'a donné l'opportunité de travailler sur diverses missions, allant de l'automatisation des infrastructures avec ansible à l'audit de sécurité d'une application web, en passant par la gestion des risques et la veille technologique.
J'ai pu constater l'impact direct de mon travail, notamment avec l'intégration de certains rôles Ansible en production.
Ce stage a été une expérience déterminante qui a non seulement confirmé mon choix de spécialisation en cybersécurité, mais m'a également montré la complémentarité des domaines de l'infrastructure et du développement dans le contexte d'une entreprise moderne. Je me sens maintenant plus confiant pour la suite de mon parcours.

Définitions – Annexes (appréciations repply fin de stage)

Cette partie regroupe toutes les définitions importantes pour bien comprendre les missions réalisées pendant le stage.
À noter que le rapport/blog est également disponible à cette adresse : https://tom-mallor.com/
Deux documents externes sont également à consulter : il s'agit de mails de remerciement concernant le travail que j'ai effectué.

Application SaaS : Une application SaaS (Software as a Service, ou *logiciel en tant que service*) est un logiciel hébergé sur des serveurs distants (dans le cloud) et accessible via Internet, généralement avec un simple navigateur web. Documentation

Ansible : Outil open-source permettant d'automatiser le déploiement de logiciels, la configuration de serveurs ou la gestion de tâches système, à l'aide de fichiers YAML appelés playbooks. Documentation

Rôle Ansible : Un ensemble structuré de fichiers contenant des tâches, variables, handlers, templates, etc., permettant de réutiliser facilement un ensemble de configurations dans plusieurs playbooks. Documentation

Playbook Ansible : Un fichier YAML décrivant des tâches à exécuter sur des machines distantes. C'est l'unité principale d'exécution dans Ansible, utilisée pour déployer, configurer ou gérer des serveurs. Documentation

OSINT (Open Source Intelligence) : Démarche consistant à rechercher toutes les informations disponibles publiquement sur Internet à propos d'une cible, pour évaluer les risques liés à la divulgation non contrôlée d'informations. Documentation

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) : Méthode développée par l'ANSSI pour identifier, évaluer et hiérarchiser les risques pesant sur le système d'information d'une organisation. Documentation

RGPD (Règlement Général sur la Protection des Données) : Règlement européen visant à protéger les données personnelles des citoyens de l'UE. Documentation

PostgreSQL : Système de gestion de base de données relationnelle open-source, reconnu pour sa robustesse, sa conformité aux standards SQL et ses fonctionnalités avancées (transactions, extensibilité, sécurité). Documentation

NIDS (Network Intrusion Detection System) : Analyse le trafic réseau pour détecter des comportements suspects ou des intrusions potentielles (ex : Snort, Suricata). Documentation

SIEM (Security Information and Event Management) : Centralise les logs et événements de sécurité, permettant leur corrélation, leur visualisation et la détection d'incidents (ex : Wazuh, ELK, Splunk). Documentation

EDR (Endpoint Detection and Response) : Agent installé sur les postes de travail/serveurs, capable de détecter des comportements anormaux, d'analyser les menaces et parfois de réagir automatiquement (ex : CrowdStrike, Microsoft Defender for Endpoint). Documentation

XDR (Extended Detection and Response) : Solution intégrée combinant les capacités des EDR, NIDS et SIEM pour une supervision centralisée et intelligente sur tout le système d'information. Documentation

CA SSH (Certificate Authority SSH) : Autorité de certification permettant de signer des clés SSH pour centraliser et sécuriser la gestion des accès aux serveurs. Documentation

Zot : Registre 100 % OCI-compliant, développé en Go, permettant d'héberger des images container de manière sécurisée, rapide et sans dépendance excessive. Documentation

OCI (Open Container Initiative) : Standard pour les images de conteneurs, garantissant l'interopérabilité entre différents outils et registres de conteneurs. Documentation

Gmail tom <tom.mallor@gmail.com>

Fin du stage de Tom MALLOR

1 message

Clément BOURGEOIS <clement.bourgeois@repply.fr> 8 août 2025 à 08:25
À : Charles VILLEMONAIS <charles.villemonais@repply.fr>, Anne-Sophie DIONISI <anso.dionisi@repply.fr>, Mathieu RENE <mathieu.rene@repply.fr>, Astrid GAUTERON <astrid.gauteron@repply.fr>
Cci : tom@repply.fr

Hello,

Le stage de Tom touche à sa fin et je suis très content de ce qu'il a accompli pour le pôle infra, il s'est montré curieux, a posé des questions pertinentes, pris quelques très bonnes initiatives en fin de stage et a travaillé en autonomie sur les sujets que je lui ai confié.

Il a en particulier travaillé à reverse engineerer les installations manuelles qui avaient été faites vers des rôles Ansible maintenus sur git :

1. socle de base pour les machines
2. rôle nginx
3. rôle postgresql + gestion de comptes temporaires pour les connexions de dev sur les production
4. rôle typesense
5. rôle zot (notre nouveau registry de containers)
6. rôle pour le port (gestion-fluides), déploiement intégral avec podman
7. rôle hopii (qui sera utile bientot pour les environnements de démo)
8. rôle assainii

Son travail est visible sur https://bitbucket.org/amcreations/infra-ansible/src/develop/ et actuellement tourne en production chez nous.

Il a aussi fait un POC de connexion SSH avec une autorité de certification centralisée. Tout le travail effectué sera complété et amélioré dans le futur. Le rôle gestion des fluides sera déployé en recette au port courant août nous faisant gagner un temps précieux.

--

repply
Clément Bourgeois
Infrastructure / DevOps
clement.bourgeois@repply.fr
05 46 45 14 10

Gmail **tom <tom.mallor@gmail.com>**

Veille OSINT - entreprise

2 messages

Romain JARRY <romain.jarry@repply.fr> 25 juillet 2025 à 10:41
À : Charles VILLEMONAIS <charles.villemonais@repply.fr>, Mathieu RENE <mathieu.rene@repply.fr>, Anne-Sophie DIONISI <anso.dionisi@repply.fr>
Cc : tom <tom@repply.fr>

Bonjour,

Une veille OSINT de l'entreprise a été réalisée par Tom, afin de relever de possibles failles provenant des données publiques. L'analyse est positive, elle n'a pas remontée de failles critiques, mais elle permet aussi de se rendre compte de l'exposition que l'entreprise a sur internet. Je ne sais pas si vous avez auparavant déjà fait ce genre d'analyse mais je vous la partage afin que vous en ayez connaissance : OSINT - Veille entreprise - repply - Pôle Sécurité/RGPD - Confluence

Cordialement,

repply | **Romain JARRY**
Développeur
romain.jarry@repply.fr

Mathieu RENE <mathieu.rene@repply.fr> 25 juillet 2025 à 13:20
À : Romain JARRY <romain.jarry@repply.fr>
Cc : Charles VILLEMONAIS <charles.villemonais@repply.fr>, Anne-Sophie DIONISI <anso.dionisi@repply.fr>, tom <tom@repply.fr>

Merci pour le travail !
J'avais déjà fait le travail mais de manière moins poussée.
Bonne nouvelle en tout cas, pas de fuite de données non maîtrisée.

Cordialement

repply | **Mathieu RENE**
Directeur Général
mathieu.rene@repply.fr
07 60 32 49 07