PROJET PASTA

Etape 0:

1. Quelles sont les étapes clés de la méthodologie PASTA (Processus de simulation d'attaques et d'analyse des menaces) et comment contribuent-elles à identifier et à atténuer les risques de sécurité ?

- Définition des objectif
- Définition du périmètre technique
- Décomposition et analyse des applications
- Analyse des menaces
- Analyse de vulnérabilité/faiblesse
- Modélisation et simulation d'attaque
- Analyse les risque et les impact

2.En quoi la méthodologie PASTA diffère-t-elle des autres approches de modélisation des menaces,telles que STRIDE ou OCTAVE, en termes de processus et d'application ?

PASTA se distingue par son approche structurée en 7 étapes, axée sur le risque métier et la simulation d'attaques pour aligner la sécurité technique avec les objectifs stratégiques, contrairement à STRIDE, plus technique et centrée sur des catégories de menaces (Spoofing, Tampering, etc.) pour les applications logicielles, et OCTAVE, orienté gestion des risques organisationnels et actifs. PASTA intègre le contexte métier et l'impact business, ce que STRIDE néglige souvent, et offre une vision plus holistique que les cadres purement basés sur les vulnérabilités.

3Pourquoi est-il important de simuler des attaques dans la méthodologie PASTA, et comment cette simulation aide-t-elle à comprendre les vulnérabilités potentielles d'un système ?

En simulant des attaques réelles, PASTA permet aux organisations d'identifier et de corriger les failles de sécurité avant qu'elles ne puissent être exploitées. Cette approche proactive minimise le risque de violation.

4.Quel rôle joue la gestion des risques dans la méthodologie PASTA, et commentles facteurs de risque sont-ils évalués et hiérarchisés au cours du processus ?

Au cours de cette étape, l'accent est mis sur la compréhension du fonctionnement interne de l'application. L'application est divisée en composants plus petits pour comprendre l'architecture de l'application, notamment les modules, les magasins de données et les canaux de communication

5Comment les résultats de l'application de la méthodologie PASTA peuvent-ils être utilisés pour améliorer la sécurité d'un système ou d'une application, et quelles sont les prochaines étapes après l'analyse ?

Les résultats de PASTA (Processus de Simulation d'Attaque et d'Analyse des Menaces) permettent d'améliorer la sécurité en identifiant les menaces et vulnérabilités critiques (via ses 7 étapes, de la définition des objectifs à l'analyse des risques), guidant ainsi la mise en œuvre de contrôles de sécurité spécifiques, l'ajustement des exigences et la conception d'atténuations ciblées. Après l'analyse, les étapes suivantes incluent l'atténuation des risques (correction des vulnérabilités, implémentation des contrôles), la surveillance continue, le test des contre-mesures et l'itération du processus pour s'adapter aux évolutions.

Etape 1:

Business Objective	Security requirement	Compliance Requirements	Risk Profile
Enregistrement du temps de travail : les employés vont pouvoir suivre leur temps de	- Authentification forte (éviter l'usurpation d'identité) - Intégrité des données (empêcher modification frauduleuse)	- Code du travail (durée du travail, heures supplémentaires) - RGPD (protection des données personnelles des employés)	Élevé : manipulation des heures → paie erronée, litiges juridiques et syndicaux

travail quotidien et hebdomadaire	- Disponibilité de l'application 24/7		
Consolidation et validation des données c'est-à-dire que les managers pourront gérer les équipes et surveiller les heures de travail de ses équipes	- Contrôle d'accès basé sur les rôles (employé, manager, RH) - Journalisation et audit des actions - Chiffrement des données sensibles	- Normes RH et conventions collectives - ISO 27001 (sécurité des données RH)	Moyen-Élevé : absence de traçabilité = risque de fraude, contestations et perte de confiance
Fournir au directeur général une visibilité complète sur le temps de travail de tous les employés	-Accès privilégié sécurisé pour le directeur général -Ségrégation des droits d'administration -Audit trail des modifications de statut d'utilisateur	Standards d'accessibilité WCAG 2.1 (mentionné comme requis pour les handicaps visuels)	Très élevé: Abus de privilèges administratifs pourrait compromettre l'intégrité de l'ensemble du système

Améliorer les conditions de travail et réduire les tensions au sein de la mairie de Gotham	-Protection contre l'utilisation non éthique de l'application -Transparence des métriques de temps de travail -Respect de la vie privée des employés	ISO 27001 pour la sécurité des informations	Moyen: Utilisation non éthique de l'application pourrait aggraver les tensions plutôt que les apaiser
Calcul et intégration avec la paie (heures normales, nuit, supplémentaires, synchronisation avec le système de paie)	- Chiffrement lors des échanges - Sécurisation des API d'intégration - Tests réguliers de vulnérabilités	- Normes de paie nationales - PCI-DSS - Protection des données personnelles (RGPD)	Élevé : erreurs de calcul ou compromission → retards/erreurs de paie, tensions sociales Amendes, poursuites judiciaires, atteinte à la réputation
Faciliter la gestion des congés pour permettre aux employés de récupérer	-Sécurité des demandes de congés -Traçabilité des approbations de congés -Protection contre la manipulation des données de congés	Réglementations sur le temps de travail applicables	Moyen: Erreurs dans la gestion des congés pourraient entraîner des problèmes de ressources humaines et de planification

Suivi, reporting et audits (consultation par employés, tableaux de bord managers, archivage pour contrôles)	- Traçabilité complète (logs inviolables) - Archivage sécurisé - Contrôles d'intégrité	- ISO 22301 (continuité et disponibilité) - Exigences syndicales et réglementaires locales	Élevé : perte de logs ou falsification = non-conformité légale, conflits syndicaux, sanctions
Améliorer la Visibilité et la Stabilité des Horaires de Travail	Contrôle d'accès aux plannings, intégrité des données d'horaires, traçabilité des modifications, disponibilité continue du système, protection contre les modifications non autorisées.	Respect du droit du travail (préavis des horaires, limites de travail de nuit), équité dans la répartition des shifts, accessibilité des informations pour tous les employés.	Changements abusifs de planning, erreurs de planification, surcharge de travail de nuit pour certains employés, conflits sociaux, stress et baisse de motivation.

Etape 2 :

Component	Acteurs	Source / Puits de Données	Services Tiers	Complétude de la Conception
Front-End App	Employés de bureau	Source : Saisie des heures, Identifiants de connexion.	Navigateurs Web	L'accessibilité pour les malvoyants est manquante. Pas de solution prévue pour les employés sans ordinateur professionnel.

Back-End API	Top Management, HR Dept, Managers (Validation).	Source : Règles de gestion (Nuit x1.5, OT x2). Puits : Logs d'activités.	Système de paie :Intégration critique requise pour les bulletins de salaire.	Une fonctionnalité cachée ("backdoor") de gestion des droits a été demandée par le Top Manager 8, introduisant une faille de sécurité majeure (Insider Threat).
Base de Données	Administrateurs Système, HR Dept.	Puits : Données personnelles, Heures travaillées, Congés maladie/vacances.		Stocke des données très sensibles (horaires des policiers, salaires). Le chiffrement n'est pas mentionné dans les specs fournies.
Module "Bat-Signal" (Intégration demandée)	Chef de la Police, Mairie, Équipes d'intervention.	Source : Signal d'urgence (Trigger). Puits : Notification aux équipes.	Le Bat-Signal (Infrastructure physique) : Connexion demandée par la Mairie pour la gestion budgétaire.	Aucune conception technique n'existe pour sécuriser ce lien physique/numérique critique. Risque élevé de spoofing (faux signal).
Module de Gestion des Shifts	Managers d'Assainissement, Police Chief Gordon.	Source : Plannings, Historique des nuits travaillées. Puits : Alertes (Manquantes).	Systèmes de géolocalisation (GPS) : Implicite pour le suivi des patrouilles/équipes mobiles.	Le système d'alerte pour prévenir l'enchaînement excessif des quarts de nuit est absent.

Etape 3:

1.Énumérer tous les cas d'utilisation de l'application employé:

a. s’authentifier dans l'application pour y accéder
b. enregistrer son temps de travail quotidien sur l’application
c. modifier son l’heure de pointage avant la validation
d. consulter ses heure de nuit supplémentaire
e. consulter ses horaires et plannings
f. soumettre les demande de congés
g. recevoir des notifications de changement d’horaires

Manager:

a. s’authentifier avec le rôle de manager
b. consulter les pointages de son équipe
c. valider les heures déclarées
d. modifier les plannings et les shifts
e. gérer les equipes
f. recevoir des alertes
g. traiter les contestation des employés
h. Visualiser les rapports d’équipe

Ressources Humaines:

a. consulter tous les pointages
b. gérer les régles de calcul
c. valider les congés

d. préparer les données pour la paie
e. générer des rapports RH
f. accéder aux journaux d'audit

Directeur Général:

a. Accéder au tableau de bord global
b. Consulter le temps de travail de tous les employés
c. Visualiser les indicateurs clés (KPI)
d. Télécharger des rapports stratégiques
e. Auditer l'utilisation du système

Administrateur Système:

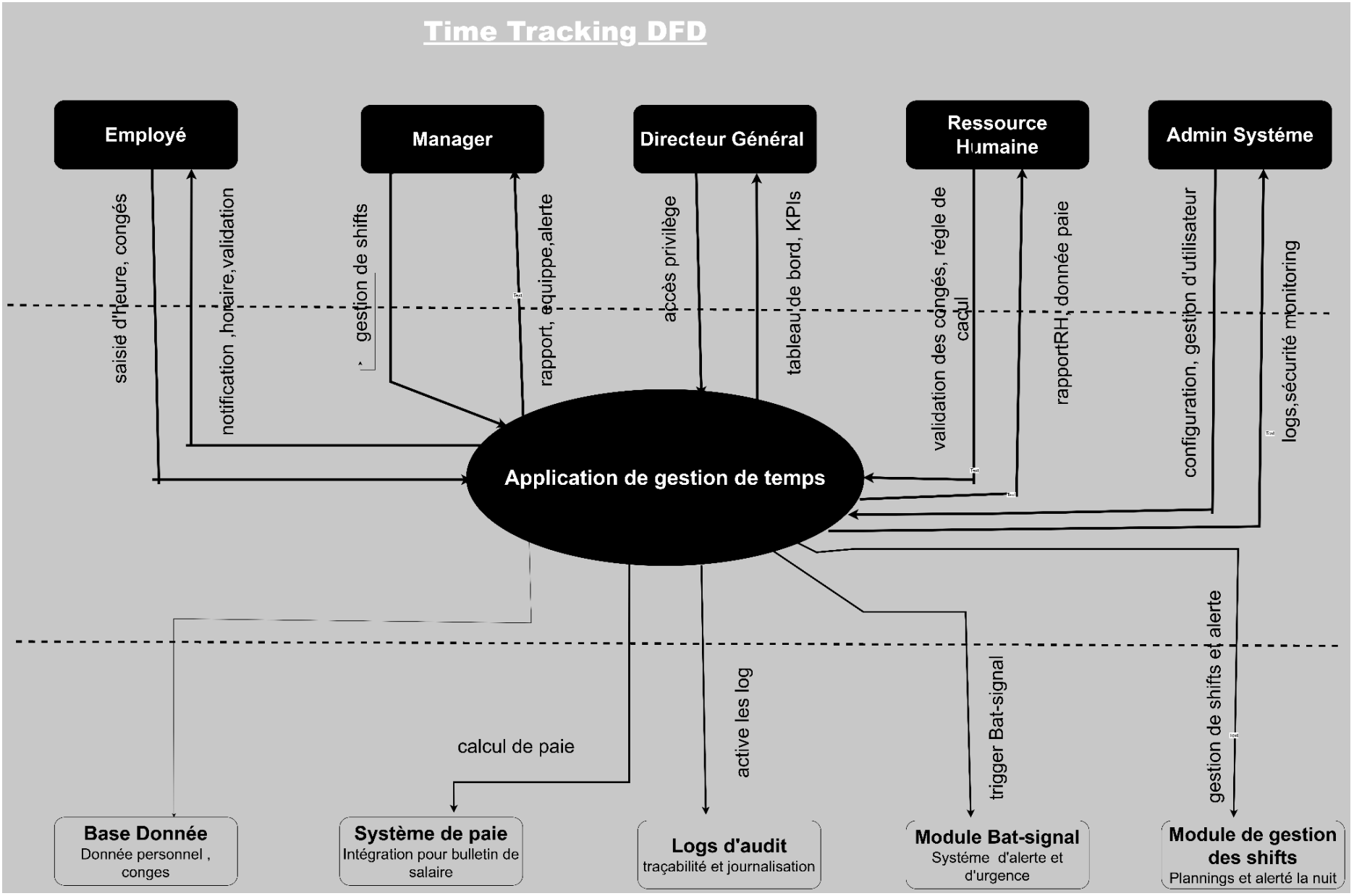
a. gérer les comptes utilisateurs
b. gérer les rôles et permissions
c. surveille les performances du système
d. consulter les logs de sécurité
e. configurer les intégration
f. sauvegarder et restaurer les donnnées

Systéme Bat-Signal (service externe):

a. Déclencher une alerte d'urgence

b. Transmettre le signal aux équipes
c. Enregistrer l’événement dans le système
d. Notifier la direction et la pol

2. Représenter les interactions et les flux de données entre les composants identifiés de l'application à l'aide d'un ou plusieurs diagrammes de flux de données (DFD) pour mettre en évidence les aspects pertinents de son architecture globale.


Time Tracking DFD
Employé
Manager
Directeur Général
Ressource Humaine
Admin Système
saisie d'heure, congés
notification ,horaire,validation
gestion de shifts
rapport, equippe,alerte
accès privilège
tableau de bord, KPIs
validation des congés, régle de calcul
rapportRH, donnée paie
configuration, gestion d'utilisateur
logs,sécurité monitoring
Application de gestion de temps
calcul de paie
active les log
trigger Bat-signal
gestion de shifts et alerte
Base Donnée
Donnée personnel , conges
Système de paie
Intégration pour bulletin de salaire
Logs d'audit
traçabilité et journalisation
Module Bat-signal
Systéme d'alerte et d'urgence
Module de gestion des shifts
Plannings et alerté la nuit

3.Analyse fonctionnelle de la sécurité et utilisation des limites de confiance

a. Quelles sont les différentes limites de confiance et leur impact sur la sécurité ?

Dans le diagramme, le système est divisé en **plusieurs zones de confiance**, chacune ayant un **niveau de sécurité différent**.

1. Zone Externe / Internet

Éléments concernés :

- Employés
- Navigateurs
- Système de paie (tiers)
- Connexions Internet

Impact sécurité :

- Zone non fiable
- Exposée aux attaques externes (vol d'identifiants, MITM, injection)
- Risque élevé d'usurpation d'identité

2. Zone Interne – Réseau de la Mairie de Gotham

Éléments concernés :

- Application de pointage
- Managers
- RH
- Directeur Général

Impact sécurité :

- Zone plus fiable, mais pas totalement sûre
- Risques internes (erreurs, abus de privilèges, insider threats)

3. Zone Backend / Données sensibles

Éléments concernés :

- Base de données RH
- Logs & audits
- Moteur de calcul de paie

Impact sécurité :

- Zone hautement critique
- Contient données personnelles, horaires, salaires, police
- Cible prioritaire en cas d’attaque

4. Zone Critique Spécifique – Bat-Signal

Éléments concernés :

- Infrastructure Bat-Signal
- Déclenchement d'alertes d'urgence

Impact sécurité :

- Impact direct sur la sécurité publique
- Risque de spoofing (faux signal)
- Impact opérationnel immédiat

b. Comment interagissent les zones de confiance et quelles implications de sécurité ?

Interaction 1 : Internet → Application Gotham

Flux :

- Identifiants
- Saisie des heures
- Demandes de congés

Implications sécurité :

- Risque d’interception
- Risque d’usurpation
- Risque d’injection

Zone externe → interne = frontière critique

Interaction 2 : Application → Backend (Base de données)

Flux :

- Heures travaillées
- Données personnelles
- Congés

Implications sécurité :

- Toute compromission de l’application donne accès aux données sensibles
- Risque RGPD majeur

Interaction interne → backend = **zone à protéger fortement**

Interaction 3 : Application → Système de paie (tiers)

Flux :

- Heures validées

- Heures de nuit et supplémentaires

Implications sécurité :

- Dépendance externe
- Risque de fuite de données
- Erreurs de synchronisation

Interaction inter-organisation = risque juridique et financier

Interaction 4 : Bat-Signal → Application

Flux :

- Signal d'urgence

Implications sécurité :

- Faux signal = panique + mauvaise allocation des ressources
- Risque critique pour Gotham

Interaction physique / numérique = surface d'attaque inhabituelle

c. Quels contrôles de sécurité sont nécessaires entre les zones ?

1. Entre Internet et Application

- Authentification forte (MFA)
- Chiffrement TLS
- Validation des entrées
- Protection contre brute force
- Journalisation des accès

2. Entre Application et Backend

- Chiffrement des données au repos
- Comptes de service dédiés
- Séparation des privilèges
- Monitoring et alertes
- Contrôles d’intégrité

3. Entre Application et Systèmes tiers (Paie)

- API sécurisées (OAuth2, clés)

  Chiffrement des échanges

- Journalisation des synchronisations
- Tests réguliers

4. Pour la zone Bat-Signal

- Authentification forte des signaux
- Validation cryptographique
- Isolation réseau
- Procédure de confirmation humaine
- Audit systématique

Step 4 :

voir image : step4.jpg step4.png

Step 5

ID	Host / IP	Port	Service	Vulnerability	CVE	CVSS Score	Severity	Description	Solution / Remediation	Status	Detected by NESSUS	Detected by OpenVAS
V01	3.125.102.39	443	tcp	Deprecated TLSv1.0 / v1.1	CVE-2014-3566	**4.3**	**Medium**	Utilisation de protocoles de chiffrement obsolètes vulnérables aux interceptions.	Désactiver TLS 1.0/1.1 et forcer TLS 1.2 ou 1.3 sur le proxy/tunnel.	Open	FALSE	TRUE

V02	18.192.31.165	Any	tcp	TCP Timestamps Disclosure	CVE-1999-0524	**2.6**	**Low**	Le serveur révèle son uptime, facilitant la reconnaissance.	Désactiver les timestamps TCP dans les paramètres du noyau (sysctl).	Open	FALSE	TRUE
V03	3.125.223.134	Any	icmp	ICMP Timestamp Reply	N/A	**2.1**	**Low**	Réponse aux requêtes de temps ICMP, aidant à la synchronisation d'attaque.	Configurer le pare-feu pour bloquer les messages ICMP Timestamp (Type 13 & 14).	Open	FALSE	TRUE
V01	3.125.209.94	443	tcp	HSTS Missing From HTTPS Server 2	RFC 6797	6.5 3	Medium 4	Le serveur n'impose pas de connexion HTTPS via le header HSTS, permettant des attaques par "SSL-stripping"5.	Configurer le serveur web pour envoyer le	Open	TRUE	FALSE

									header Strict-Transport-Security6666.			
V02	3.125.209.94	80/443	tcp	HTTP Methods Allowed 7	N/A	Informational	Info 8	Détermination des méthodes HTTP autorisées (GET, POST, OPTIONS, etc.) par répertoire9999.	Désactiver les méthodes HTTP non nécessaires ou risquées comme PUT ou DELETE10101010.	Open	TRUE	FALSE
V03	3.125.209.94	443	tcp	Missing CSP frame-ancestors 11	N/A	Informational	Info 12	Absence de politique de sécurité de contenu pour prévenir le clickjacking13.	Configurer un header Content-Security-Policy avec la directive frame-ancestors14.	Open	TRUE	FALSE

V04	3.125.209.94	443	tcp	Missing X-Frame-Options Header 15	N/A	Informational	Info 16	Le serveur ne définit pas de header X-Frame-Options, facilitant les attaques de type clickjacking17.	Ajouter le header X-Frame-Options (DENY ou SAMEORIGIN) dans les réponses HTTP1818.	Open	TRUE	FALSE
V05	3.125.209.94	443	tcp	Web Server No 404 Error Code 19	N/A	Informational	Info 20	Le serveur ne renvoie pas de code d'erreur 404 standard pour les fichiers inexistants21.	Configurer le serveur pour qu'il réponde avec un code 404 standard en cas de ressource manquante22.	Open	TRUE	FALSE

L'audit réalisé par **Nessus** et **OpenVAS** n'a révélé aucune vulnérabilité classée comme « Critique ». Il est important de préciser que les alertes concernant le chiffrement, notamment l'absence de **HSTS** et les faiblesses **TLS**, sont considérées comme « normales » dans ce contexte de test. En effet, l'application étant hébergée localement et exposée via un tunnel **Ngrok**, les scanners analysent les serveurs de relais de Ngrok et non la configuration finale de la ville de Gotham.

Cependant, l'absence de vulnérabilités connues ne signifie pas que le système est invulnérable. Le risque réel est ici **logique et applicatif**. Les outils automatisés ne peuvent pas détecter les failles de conception spécifiques à notre code Elixir, comme les variables d'ID ignorées ou les vérifications de rôles incomplètes constatées lors de l'analyse des logs du serveur. Un attaquant ne cherchera pas à briser le chiffrement, mais à exploiter ces erreurs de logique métier pour manipuler les données de paie ou usurper des identités. C'est sur cette **simulation d'attaque ciblée** que se concentrera l'étape suivante de notre méthodologie PASTA.

STEP 6

Scénario d'attaque	Interne / Externe	Prérequis pour l'attaque
Hacker externe (sans compte, sans connaissance) attaquant l'application pour des faiblesses communes.	Externe	Aucun prérequis. L'attaquant cible l'URL publique cdfe77791688.ngrok-free.app et exploite l'absence de HSTS pour tenter une interception de données par "SSL Stripping".
Hacker externe (avec compte, sans connaissance) attaquant l'application pour des faiblesses de logique.	Externe	Possession d'un compte "Employé" standard. L'attaquant utilise sa session pour tester des failles de type IDOR en modifiant les IDs dans les URLs afin d'accéder aux profils d'autres agents .

Initié malveillant (Employé) cherchant à manipuler la paie ou les heures de travail.	Interne	Un compte utilisateur valide. L'attaquant profite de l'absence de vérification de propriété sur les points d'accès /api/workingtimes pour modifier ses propres relevés ou ceux de ses collègues (V2.2).
Voleur d'identifiants ciblant un accès administratif.	Externe	Interception d'un flux réseau. L'attaquant utilise le fait que le hachage est réalisé côté client (V1.1) pour capturer et réutiliser directement le hash sans avoir à déchiffrer le mot de passe réel.