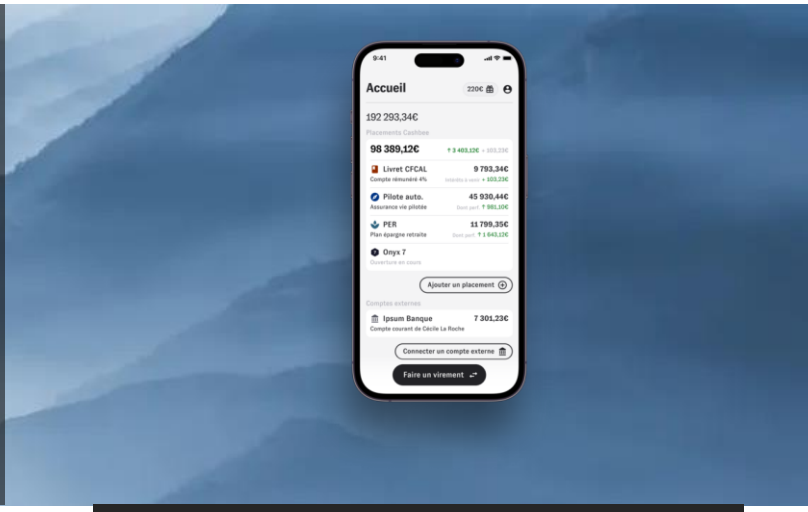
# ÉTUDE DE CAS

Comment un audit intrusif renforce la sécurité des applications et protège les données des utilisateurs ?

**ENTREPRISE :** Cashbee
**SECTEUR :** Service financier numérique




## POURQUOI ITRUST ?

ITrust a été sélectionné pour son approche complète et méthodique en matière d'audit de sécurité et pour la diversité de ses méthodes de tests d'intrusion, permettant ainsi une évaluation approfondie des vulnérabilités.
Les experts sont capables d'identifier immédiatement les vulnérabilités et de fournir des recommandations techniques précises, directement applicables.
En intégrant les référentiels de sécurité les plus stricts, tels qu'ISO 27001, RGS et OWASP, ITrust garantit une conformité rigoureuse aux standards internationaux.

### NIVEAU TECHNIQUE DU SERVICE DÉLIVRÉ

1 2 3 4 5 6 7 8 9 **10**

### QUALITÉ DU RAPPORT LIVRÉ

1 2 3 4 5 6 7 8 9 **10**

### ACCOMPAGNEMENT DE L'EQUIPE

1 2 3 4 5 6 7 8 9 **10**

### RECOMMANDATION ITRUST

1 2 3 4 5 6 7 8 9 **10**

## CONTEXTE ET ENJEUX

Cashbee propose une application mobile innovante qui permet aux utilisateurs de gérer et d'optimiser leur épargne de manière simple et sécurisée. Cet acteur majeur de la FinTech française a entrepris une démarche d'agrément auprès de l'ACPR, dont une des exigences majeures était la réalisation d'un audit de sécurité sur ses sites Internet et applications.

### ÉVALUER LA ROBUSTESSE DES ACTIFS EXPOSÉS

Estimer la robustesse des actifs de Cashbee exposés sur internet face aux différentes sources de menaces potentielles en identifiant les vulnérabilités exploitables par des acteurs.

### PROTÉGER LES DONNÉES PERSONNELLES ET FINANCIÈRES

La gestion d'épargne implique le traitement de données sensibles, telles que les informations bancaires et les identités des utilisateurs. Toute faille de sécurité pourrait avoir des conséquences graves.

### OBTENIR L'AGRÉMENT DE L'ACPR BANQUE DE FRANCE

L'agrément de l'ACPR est une étape clé pour toute entreprise opérant dans le domaine financier. Cette certification garantit que Cashbee respecte les normes bancaires et réglementaires en vigueur, un facteur essentiel pour assurer la légitimité de ses services.

# LA SOLUTION RETENUE UN AUDIT INTRUSIF EXTERNE - APPLICATIF

### BOÎTE NOIRE : TESTER LA RÉSISTANCE FACE AUX MENACES EXTÉRIEURES

Cette phase vise à reproduire les techniques qu'un attaquant totalement étranger au système pourrait employer pour s'introduire dans l'infrastructure de Cashbee. ITrust tente d'identifier et d'exploiter les failles les plus accessibles via des méthodes telles que l'ingénierie sociale, le scanning de ports et l'exploitation de vulnérabilités connues.

### BOÎTE GRISE : ÉVALUER LA SÉCURITÉ INTERNE ET LA GESTION DES ACCÈS

La phase en boîte grise permet d'analyser les failles potentielles à partir d'un accès utilisateur légitime. Cette approche permet de détecter les vulnérabilités liées aux droits d'accès excessifs, aux erreurs de configuration, ou encore aux faiblesses dans la gestion des identités et des sessions.

### UNE ÉVALUATION RIGOUREUSE DES RISQUES ET DES VULNÉRABILITÉS

**Cartographie du réseau** et identification des surfaces d'attaque pour repérer les points d'entrée.
**Recherche de vulnérabilités** via l'analyse des systèmes et tests de configuration.
**Exploitation des vulnérabilités** par simulation d'attaques pour mesurer leur impact réel.
**Analyse des résultats et recommandations**, avec une classification des risques et des mesures correctives adaptées.

Les tests sont non destructifs et encadrés pour éviter tout impact sur la production. Chaque vulnérabilité est documentée avec une procédure détaillée de détection et d'exploitation, permettant aux équipes techniques de vérifier la correction des failles.

*L'audit ITrust s'est déroulé de manière rigoureuse et efficace, avec un impact minimal sur les équipes en interne, sans pour autant négliger la rigueur des analyses.*

*Les recommandations qui ont suivi ont bien renforcé notre sécurité réseau et la protection de nos données clients. En tant qu'établissement régulé, c'est la solution qu'il nous fallait.*

**Chaker Nakhli**
Co-fondateur & CTO
Cashbee

### DES RECOMMANDATIONS PRÉCISES POUR UNE SÉCURISATION RENFORCÉE

Suite à l'audit, un rapport complet a été remis à Cashbee, comprenant :

- Une analyse des vulnérabilités classées par niveau de risque (faible, modéré, critique)
- Un plan d'actions détaillé avec des recommandations adaptées
- Une matrice de risques pour prioriser les mesures de remédiation

En appliquant ces recommandations, Cashbee réduit considérablement son exposition aux cyberattaques et renforce la sécurité de ses données financières et clients.



ITRUST.