|  |
| --- |
| Pentest securebank |
| Vulnerability Report |
| undefined |

Table of Contents

[1. Introduction 3](#_Toc177396537)

[1.1. Contexte et objectifs de la mission 3](#_Toc177396538)

[1.2. Périmètre de la mission 3](#_Toc177396539)

[1.3. Méthodologie 3](#_Toc177396540)

[1.4. Déroulement des travaux 3](#_Toc177396541)

[1.5. Limites 4](#_Toc177396542)

[1.6. Remise en état 4](#_Toc177396543)

[2. Summary 5](#_Toc177396544)

[2.1. Executive summary 5](#_Toc177396545)

[2.1. Vulnérabilités et recommandations 6](#_Toc177396546)

[3. Constats détaillés 7](#_Toc177396547)

# Introduction

## Contexte et objectifs de la mission

Secure Bank a mandaté Correlia pour effectuer un test d'intrusion sur son application web dans le but d'évaluer la robustesse de celle-ci face à des attaques potentielles. L'objectif principal de cette mission est de détecter les vulnérabilités présentes au sein de l'application, de comprendre les risques associés à celles-ci et de proposer des mesures correctives pour renforcer la sécurité globale. Cette démarche proactive vise à protéger les données sensibles des utilisateurs de Secure Bank ainsi qu'à préserver l'intégrité de son système d'information.

## Périmètre de la mission

Le périmètre de cette mission couvre l'intégralité de l'application web de Secure Bank, ainsi que tous les services accessibles depuis Internet. Cela inclut, sans s'y limiter, les interfaces utilisateurs, les APIs exposées, les bases de données associées, ainsi que les mécanismes d'authentification et d'autorisation.

Les tests ont été effectués dans le respect des bonnes pratiques de sécurité et des normes éthiques, sans causer de perturbations au fonctionnement normal de l'application ni compromettre l'intégrité des données.

## Méthodologie

La méthodologie employée pour ce test d'intrusion sur l'application web de Secure Bank repose sur les meilleures pratiques en matière de sécurité des applications web. Elle comprend les phases suivantes :

**1. Collecte d'informations :** Cette phase initiale vise à rassembler toutes les informations accessibles publiquement concernant l'application. Cela inclut l'identification des noms de domaine, la découverte des sous-domaines, l'analyse des technologies utilisées, ainsi que la recherche de possibles divulgations d'informations sensibles.

**2. Analyse et Cartographie :** Un scan complet de l'application est effectué pour identifier les points d'entrée accessibles, les services exposés, les technologies web en place, ainsi que les éventuelles vulnérabilités connues associées. Cette étape permet de dresser une carte précise des vecteurs d'attaque disponibles.

**3. Test d'exploitation :** Les vulnérabilités potentielles identifiées sont testées de manière contrôlée pour vérifier leur exploitabilité. Cela inclut des tentatives d'injections (SQL, XSS), des tests d'accès direct aux objets (IDOR), ainsi que des analyses de logique applicative visant à contourner les contrôles de sécurité existants.

**4. Escalade des privilèges :** Si une vulnérabilité est exploitée avec succès, des tentatives d'escalade de privilèges sont effectuées pour évaluer la possibilité d'accéder à des données sensibles ou d'obtenir des permissions élevées au sein de l'application.

**5. Rapport et Recommandations :** Chaque vulnérabilité confirmée est documentée avec des preuves concrètes, une analyse de son impact sur la sécurité, et des recommandations spécifiques pour sa correction. L'accent est mis sur des solutions pratiques et adaptées à l'environnement de Secure Bank.

## Déroulement des travaux

Notre intervention s’est déroulée selon le calendrier établi en collaboration avec l'équipe de sécurité de Secure Bank :

* **Phase de préparation** : Une réunion de cadrage a été organisée avec les responsables de Secure Bank pour définir précisément le périmètre et les objectifs de la mission.
* **Phase de test** : Les tests d'intrusion ont été réalisés sur l'infrastructure de l'application web conformément aux directives établies. Cette phase a duré une semaine, pendant laquelle des tests automatisés et manuels ont été conduits pour identifier les vulnérabilités.
* **Phase de validation** : Les résultats des tests ont été partagés avec l'équipe sécurité de Secure Bank. Cette phase a permis de vérifier l'exactitude des informations collectées et d'évaluer l'impact des vulnérabilités identifiées.
* **Phase de rapport** : Un rapport détaillé a été rédigé et présenté aux parties prenantes de Secure Bank, incluant les conclusions de l'évaluation et les recommandations proposées

## Limites

Certaines limitations ont été rencontrées au cours de la mission. Les tests ont été réalisés exclusivement en heures creuses afin de minimiser tout risque de perturbation des services en production. De plus, certaines parties de l'application, soumises à des restrictions d'accès, n'ont pas pu être pleinement explorées

## Remise en état

À l’issue des tests, toutes les modifications temporaires apportées à l'infrastructure de test ont été annulées. Aucune altération permanente n'a été effectuée sur les systèmes testés. L'application a été restaurée à son état initial, garantissant ainsi l'intégrité et la disponibilité des services pour les utilisateurs.

# Synthèse

## Synthèse managériale

Secure Bank a sollicité Corellia pour mener des tests d'intrusion sur son application web afin d’évaluer la sécurité de son système d’information. L'objectif de cette mission était de s'assurer que l'application est suffisamment protégée contre les cyberattaques et qu'elle respecte les normes de sécurité en vigueur.

Au cours de notre évaluation, nous avons identifié une vulnérabilité de gravité critique (V005) liée à un contrôle d'accès défaillant. Cette vulnérabilité pourrait permettre à un attaquant opérant depuis Internet d’accéder de manière non autorisée à des ressources sensibles de l'application, telles que les informations des utilisateurs, et de modifier ces données sans aucune authentification préalable. Une exploitation de cette faille pourrait compromettre l'intégrité des informations stockées dans les bases de données de Secure Bank.

Nous avons également relevé trois vulnérabilités de gravité élevée (V003, V002, V001) qui représentent des menaces sérieuses pour la sécurité de l'application. La première (V003) concerne une politique de mots de passe insuffisante, qui autorise l'utilisation de mots de passe faibles et vulnérables aux attaques de force brute, permettant ainsi à un attaquant de se connecter en usurpant l’identité d’un utilisateur légitime. La deuxième vulnérabilité (V002) repose sur un IDOR (Insecure Direct Object Reference), permettant à un attaquant de manipuler des paramètres et d'accéder à des informations auxquelles il ne devrait pas avoir accès. Enfin, la troisième vulnérabilité (V001) se rapporte à une faiblesse dans la gestion des entités externes XML (XXE), susceptible de permettre à un attaquant de lire des fichiers internes au serveur ou d'exécuter des requêtes non autorisées.

De plus, nous avons identifié une vulnérabilité de gravité modérée (V004), liée à une injection XSS (Cross-Site Scripting). Cette faille permettrait à un attaquant d'exécuter des scripts malveillants dans le navigateur de l'utilisateur, ce qui pourrait conduire au vol de cookies de session ou à l'altération de l'affichage de l'application.

Les risques métiers associés à ces vulnérabilités sont conséquents :

* **Violation de la réglementation en matière de protection des données** : un attaquant pourrait accéder à des informations personnelles des utilisateurs, telles que leurs coordonnées bancaires et leurs données d'identité. Ceci pourrait exposer Secure Bank à des sanctions réglementaires et à une perte de confiance des utilisateurs.
* **Fraude et usurpation d'identité** : l’exploitation des vulnérabilités liées à la politique de mot de passe faible et à l'IDOR permettrait à un attaquant d'usurper l'identité d'un utilisateur et d'accéder à ses données sensibles, avec des conséquences potentielles de fraude.
* **Contournement des mesures de sécurité internes** : les failles identifiées permettent à un attaquant d’accéder à des informations confidentielles sans passer par les contrôles de sécurité habituels, ce qui remet en question l'efficacité des mesures de sécurité mises en place par Secure Bank.
* **Exploitation d’autres vulnérabilités** : les failles découvertes pourraient être combinées pour accentuer l'impact d'une attaque, augmentant ainsi le risque global pour l'application.

Corellia considère que ces vulnérabilités constituent une menace sérieuse pour la sécurité de l'application web de Secure Bank et recommande une correction immédiate des failles identifiées en appliquant les mesures de sécurité préconisées.

## Vulnérabilités et recommandations

Following vulnerabilities have been discovered:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Vulnérabilités | Gravité | Recommandations | Priorité |
| V005 | Injection XSS | Critical | Protection contre les attaques XSS | 3 |
| V002 | Politique de mot de passe faible | High | Renforcement de la politique de gestion des mots de passe | 4 |
| V003 | IDOR (Insecure Direct Object Reference) | High | Revue des contrôles d'accès sur l'application Secure Bank | 4 |
| V001 | Broken Access Control | High | Renforcement des contrôles d'accès | 4 |
| V004 | XXE XML External Entity | Medium | Sécurisation de la gestion des entités XML | 4 |

# Constats détaillés

The following details the vulnerabilities identified in the scope, together with an estimate of the impact of the exploitation of the vulnerability, the ease of exploitation of the vulnerability and its criticality. Also referenced are the business risks associated with the vulnerability in the context of your environment, as well as the recommendation for remediating the vulnerability and reducing the risks.

|  |  |  |
| --- | --- | --- |
| V005 | Injection XSS | Gravité |
| Critical |
| Libellé | Le site de l'application Secure Bank présente une vulnérabilité de type XSS (Cross-Site Scripting) qui permet à un attaquant d'injecter du code malveillant via les paramètres d'entrée côté client. Cette faille est due à un manque de validation et de filtrage des données entrantes, ce qui expose l'application à des risques de manipulation de contenu. Un attaquant opérant depuis un navigateur pourrait, en exploitant cette vulnérabilité, exécuter des scripts malveillants sur le navigateur des utilisateurs légitimes visitant le site.  Cette vulnérabilité pourrait être utilisée pour détourner la logique de l'application web, permettant ainsi le vol de cookies ou de jetons de session, l'altération de données ou de contenus, voire l'exécution de malwares sur les systèmes des utilisateurs affectés. L'exploitation de cette faille pourrait compromettre la confidentialité et l'intégrité des données, ainsi que la confiance des utilisateurs envers la plateforme. | |
| Périmètre |  | |

|  |  |  |
| --- | --- | --- |
| Recommandation | | |
| E005 | Protection contre les attaques XSS | Priorité |
| 3 |
| Libellé | Nous recommandons d'implémenter des mesures de protection strictes pour traiter toutes les données provenant de sources externes. Il est essentiel que tout contenu soit systématiquement filtré, validé et encodé avant d'être utilisé par l'application. Les entrées utilisateur doivent être assainies de manière rigoureuse afin d'éliminer tout caractère ou chaîne de caractères potentiellement malveillant.  De plus, il est recommandé de configurer les en-têtes de sécurité HTTP, tels que Content-Security-Policy (CSP), afin de restreindre les sources autorisées de contenu actif (scripts, styles, etc.) et d'empêcher l'exécution de code non approuvé. La mise en œuvre de ces mesures contribuera à réduire le risque d'exploitation de vulnérabilités XSS et à protéger les utilisateurs de Secure Bank contre les attaques potentielles. | |

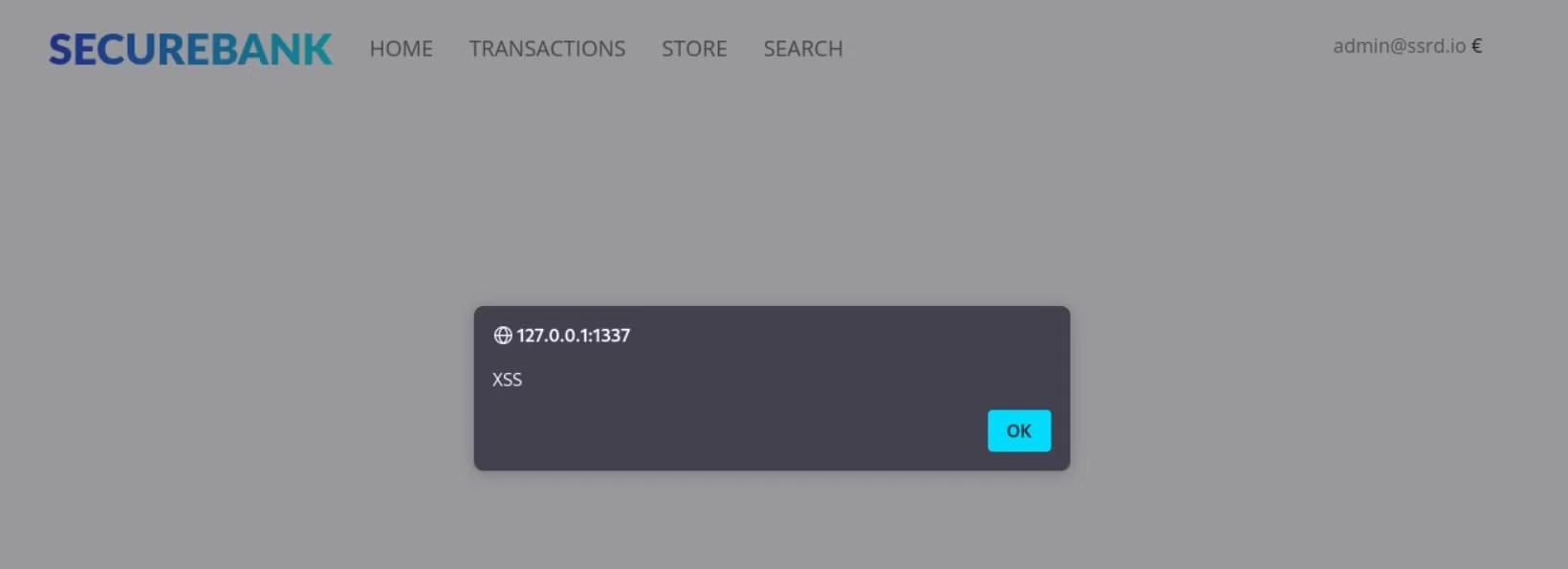


Image **1** – Exécution réussie d'une attaque XSS sur Secure Bank

|  |  |  |
| --- | --- | --- |
| V002 | Politique de mot de passe faible | Gravité |
| High |
| Libellé | Le compte administrateur de l'application Secure Bank utilise un mot de passe faible, "admin". Ce mot de passe a pu être facilement deviné, permettant à un attaquant d'accéder au compte administrateur avec des privilèges élevés. Cette faiblesse pourrait être exploitée par un individu malveillant opérant depuis l'extérieur ou l'intérieur du réseau, compromettant ainsi la sécurité de l'application et des données sensibles des utilisateurs.  En raison de la simplicité du mot de passe, un attaquant pourrait aisément réaliser une attaque par force brute ou par devinette pour accéder à ce compte. Une fois connecté, il serait en mesure de manipuler les paramètres de l'application, d'accéder aux informations confidentielles des utilisateurs, et potentiellement de compromettre d'autres services connectés. Cela expose l'organisation à un risque de perte de données et d'accès non autorisé à des informations critiques. | |
| Périmètre |  | |

|  |  |  |
| --- | --- | --- |
| Recommandation | | |
| E002 | Renforcement de la politique de gestion des mots de passe | Priorité |
| 4 |
| Libellé | Nous vous recommandons de revoir la politique de gestion des mots de passe en imposant l'utilisation de mots de passe forts, comprenant au minimum huit caractères avec une combinaison de majuscules, minuscules, chiffres et caractères spéciaux. De plus, l'implémentation d'une authentification multi-facteurs (MFA) est préconisée afin de renforcer la sécurité des comptes administratifs, même en cas de compromission du mot de passe. L'adoption de ces mesures réduirait considérablement le risque d'accès non autorisé aux informations sensibles et aux fonctions critiques de l'application. | |

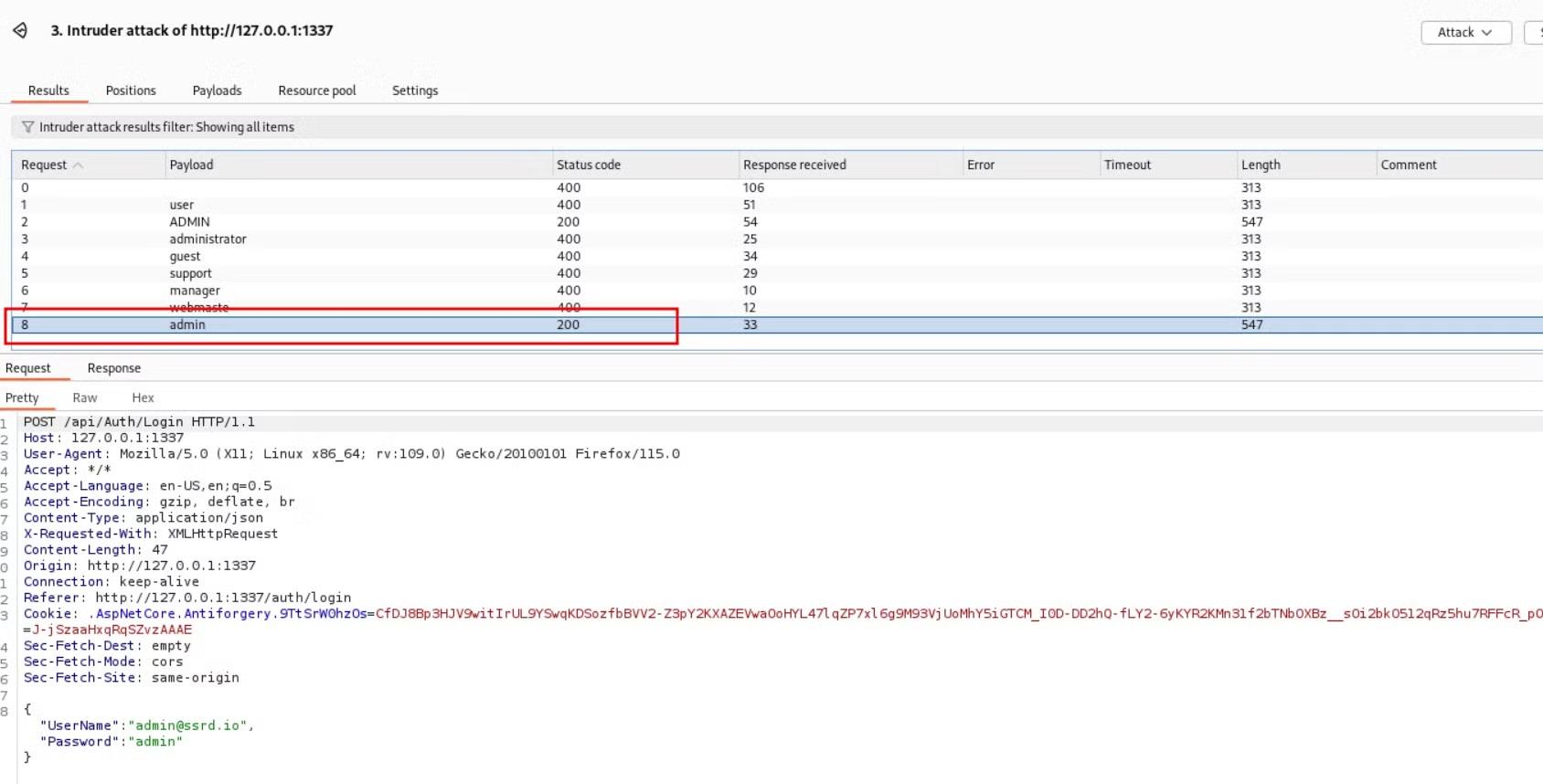


Image **2** – Tentative de connexion sur le compte admin

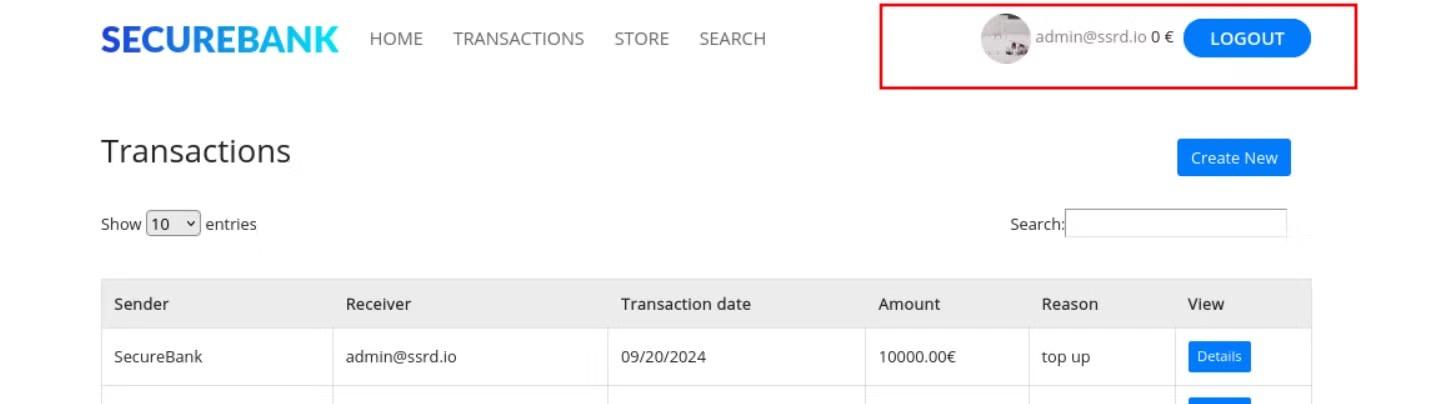


Image **3** – Tentative de connexion sur le compte admin réussie

|  |  |  |
| --- | --- | --- |
| V003 | IDOR (Insecure Direct Object Reference) | Gravité |
| High |
| Libellé | Une vulnérabilité de type IDOR (Insecure Direct Object Reference) est présente sur le site de l'application de Secure Bank. Cette faille permet à un utilisateur avec des privilèges limités d'accéder aux informations confidentielles des transactions bancaires effectuées par d'autres collaborateurs. Cette exposition de données sensibles inclut des informations telles que le montant des transactions, les détails des bénéficiaires, et les dates de transfert. L'exploitation de cette vulnérabilité constitue un risque majeur en termes de sécurité, car elle pourrait être utilisée par un attaquant pour collecter des informations financières sensibles et les utiliser à des fins malveillantes, telles que le chantage ou la fraude. La capacité de contourner les contrôles d'accès et d'accéder à des informations auxquelles un utilisateur ne devrait pas avoir accès compromet la confidentialité des données et pourrait avoir des conséquences juridiques et financières pour l'organisation | |
| Périmètre |  | |

|  |  |  |
| --- | --- | --- |
| Recommandation | | |
| E003 | Revue des contrôles d'accès sur l'application Secure Bank | Priorité |
| 4 |
| Libellé | Nous vous recommandons de :   * Revoir les mécanismes de gestion des droits d'accès au sein de l'application Secure Bank afin de s'assurer que seuls les utilisateurs autorisés puissent accéder aux informations relatives aux transactions. * Mettre en place une vérification rigoureuse des autorisations utilisateur à chaque requête de récupération de données, en utilisant des mécanismes d'autorisation contextuelle basés sur les rôles et les attributs de l'utilisateur. * Aappliquer le principe du moindre privilège, en s'assurant que les utilisateurs ne puissent accéder qu'aux informations strictement nécessaires à l'exercice de leurs fonctions. * Auditer régulierement des logs d'accès et des transactions pour détecter toute tentative d'accès non autorisé et répondre rapidement en cas d'incident. | |

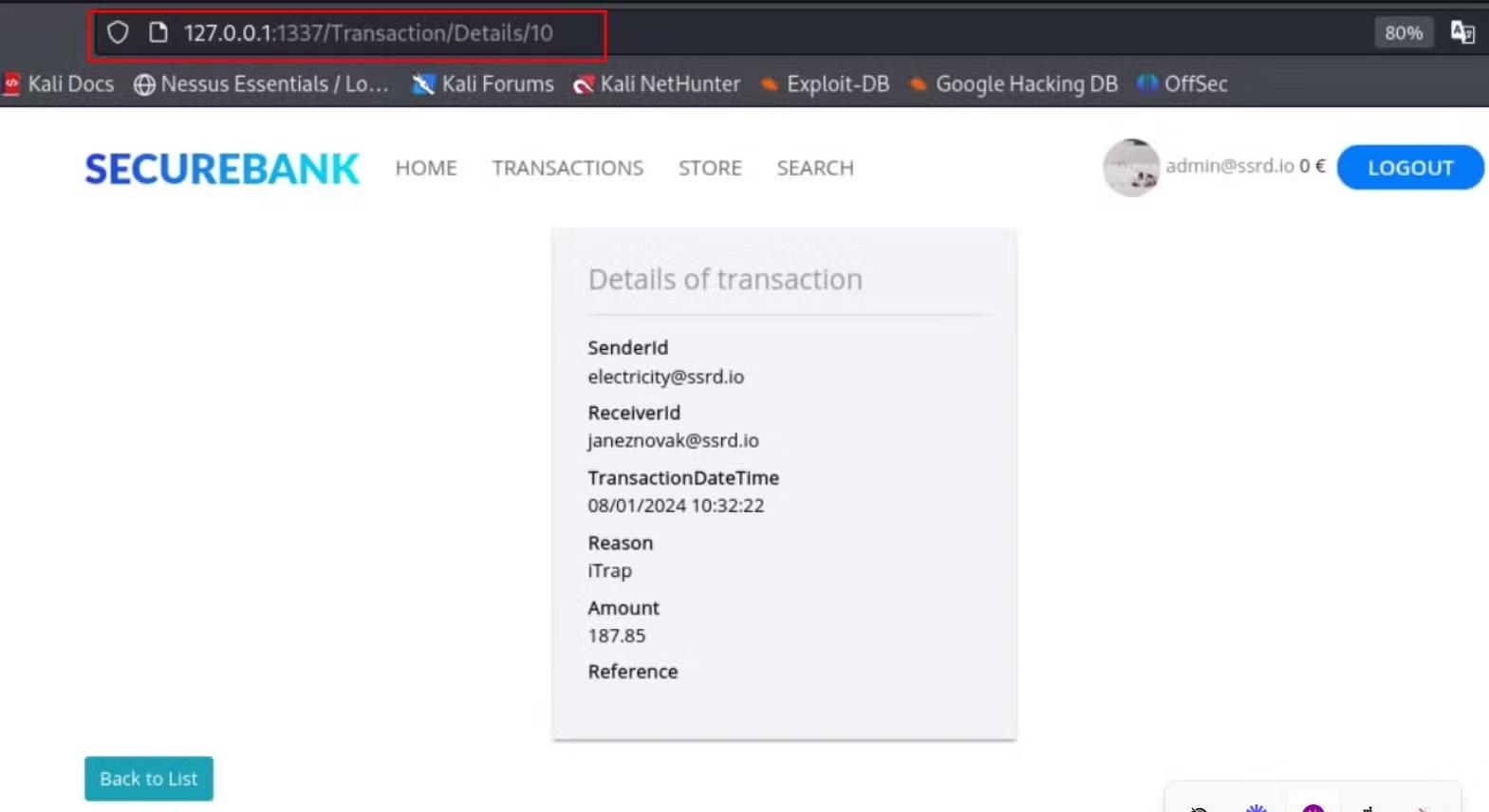


Image **4** – Accès non autorisé aux détails des transactions d'un utilisateur tiers

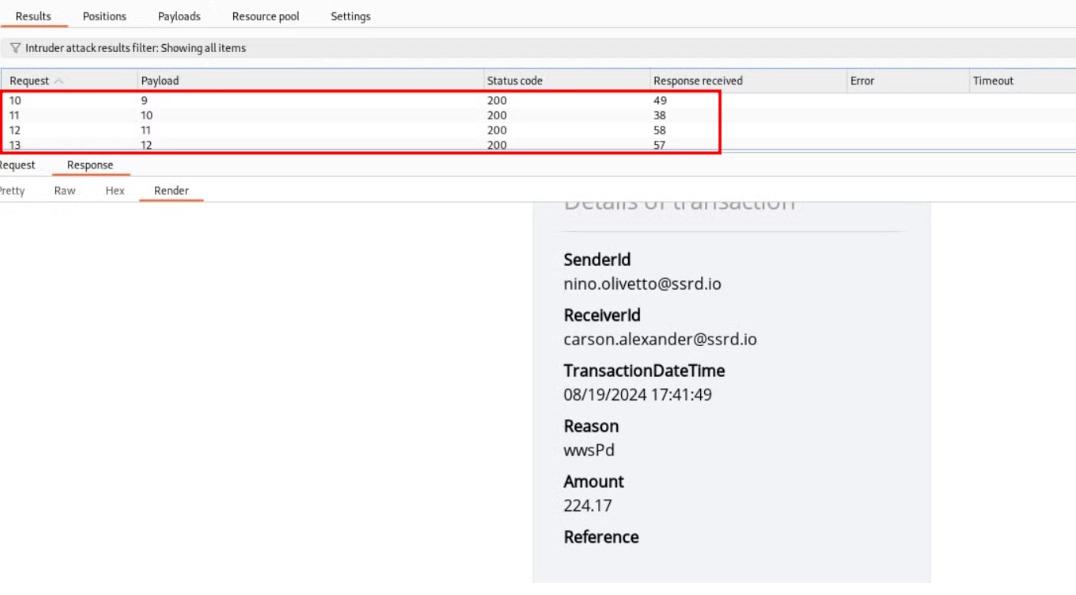


Image **5** – Accès non autorisé aux détails des transactions d'un utilisateur tiers

|  |  |  |
| --- | --- | --- |
| V001 | Broken Access Control | Gravité |
| High |
| Libellé | Le site de l'application Secure Bank présente une faille de type "Broken Access Control". Cette vulnérabilité permet à un attaquant opérant depuis l'interface utilisateur de contourner les contrôles d'accès en place et d'effectuer des actions non autorisées. En exploitant cette faille, un attaquant pourrait, par exemple, transférer des fonds depuis un compte vers un autre, sans disposer des droits d'accès requis pour le compte source. Cette faiblesse dans le système de gestion des permissions pourrait conduire à des conséquences graves, notamment la perte financière des clients ou la compromission de l'intégrité des données bancaires. | |
| Périmètre |  | |

|  |  |  |
| --- | --- | --- |
| Recommandation | | |
| E001 | Renforcement des contrôles d'accès | Priorité |
| 4 |
| Libellé | Nous recommandons de revoir et de renforcer les mécanismes de gestion des droits d'accès au sein de l'application Secure Bank. Les contrôles d'accès doivent être strictement appliqués à chaque niveau de l'application pour s'assurer que les utilisateurs ne peuvent effectuer que les actions pour lesquelles ils disposent des autorisations nécessaires. Il est également crucial de mettre en place des vérifications systématiques des droits d'accès avant toute opération sensible, comme le transfert de fonds, afin d'empêcher toute tentative de contournement des contrôles d'accès en place. | |

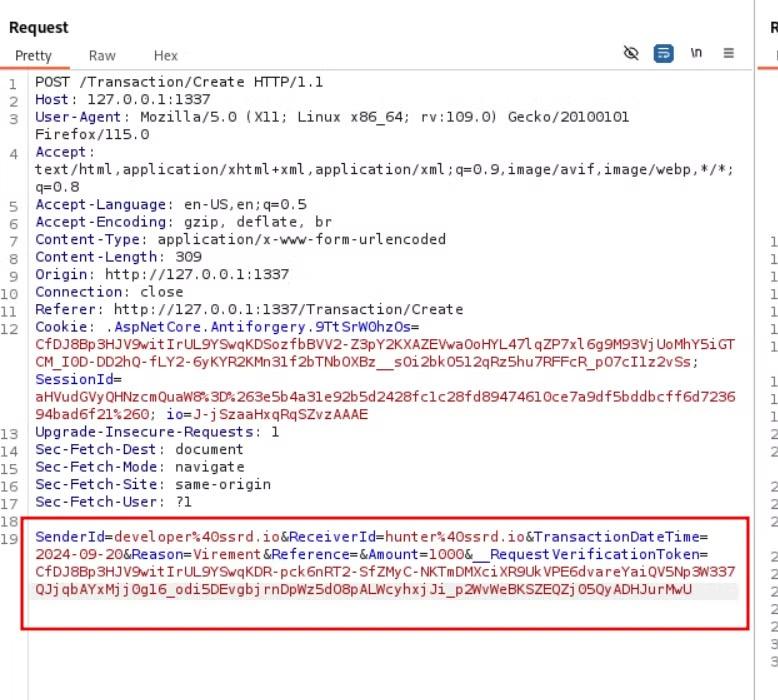


Image **6** – Transférer des fonds depuis un compte

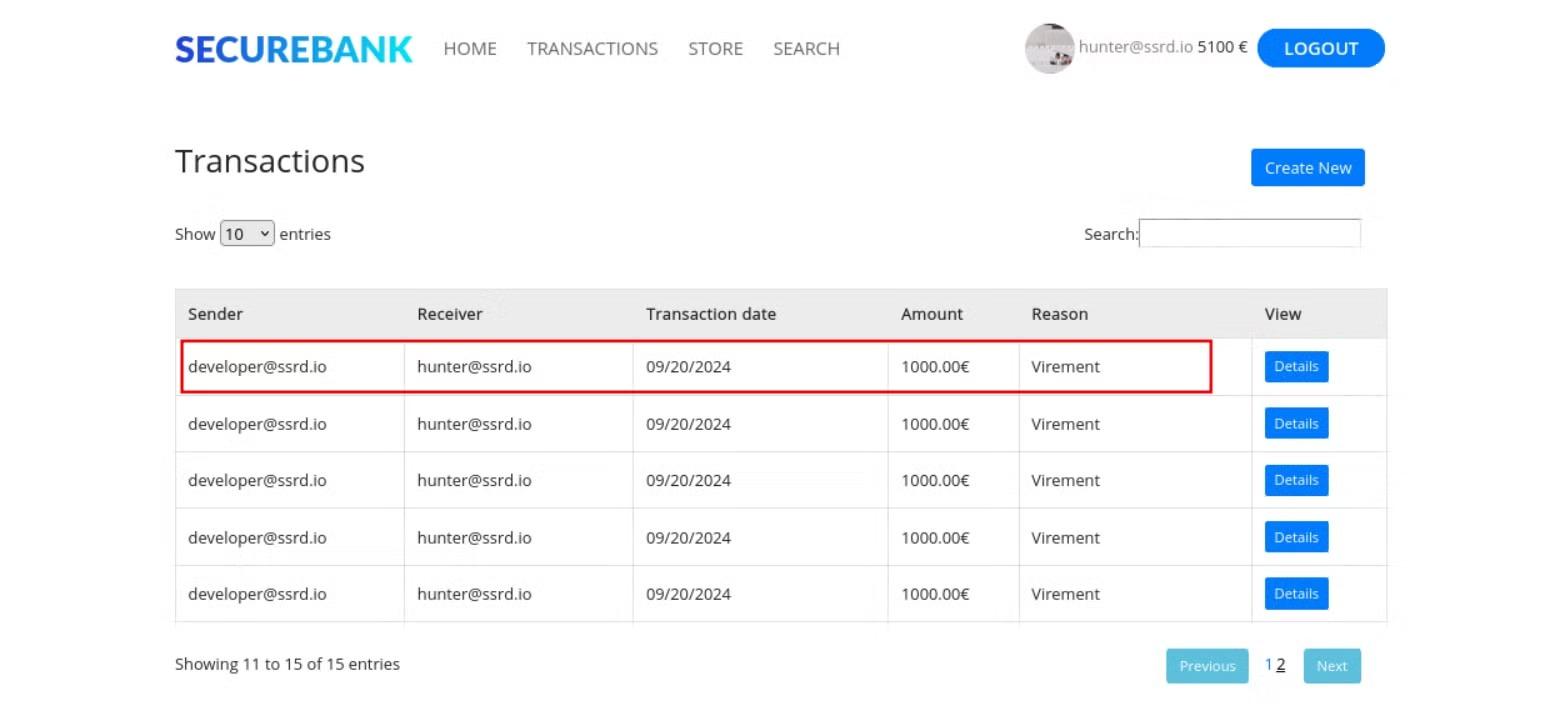


Image **7** – Transférer des fonds depuis un compte réussi

|  |  |  |
| --- | --- | --- |
| V004 | XXE XML External Entity | Gravité |
| Medium |
| Libellé | L'application de Secure Bank présente une vulnérabilité de type "XML External Entity" (XXE). Cette faille permet à un attaquant, opérant depuis l'extérieur ou depuis le réseau interne, de soumettre une requête XML spécialement conçue pour accéder à des fichiers sensibles sur le serveur. En exploitant cette vulnérabilité, un attaquant peut lire des fichiers contenant des informations sur les utilisateurs, y compris leurs mots de passe, ce qui constitue un risque majeur en termes de sécurité des données.  Ce type d'attaque permet de contourner les mécanismes de sécurité de l'application et peut conduire à une compromission totale du système. L'attaquant pourrait également utiliser cette vulnérabilité pour accéder à des informations critiques sur la configuration du serveur ou exfiltrer des données sensibles, compromettant ainsi la confidentialité et l'intégrité des données de l'application. | |
| Périmètre |  | |

|  |  |  |
| --- | --- | --- |
| Recommandation | | |
| E004 | Sécurisation de la gestion des entités XML | Priorité |
| 4 |
| Libellé | Nous vous recommandons de désactiver le traitement des entités externes dans les parseurs XML utilisés par l'application. Cette configuration empêche l'inclusion d'entités externes dans les requêtes XML, réduisant ainsi la surface d'attaque exploitée par cette vulnérabilité. De plus, il est essentiel de mettre en place une validation stricte des entrées et de s'assurer que les parseurs XML utilisés ne permettent pas le chargement de fichiers externes non autorisés.  Il est également conseillé d'effectuer une revue de sécurité approfondie de l'application pour identifier et corriger toutes les instances de traitement des entités XML. Enfin, la mise en œuvre d'un modèle de sécurité renforcé, comprenant la segmentation des droits d'accès et le chiffrement des données sensibles, contribuera à réduire l'impact potentiel de ce type d'attaque sur l'intégrité et la confidentialité des informations de l'application. | |

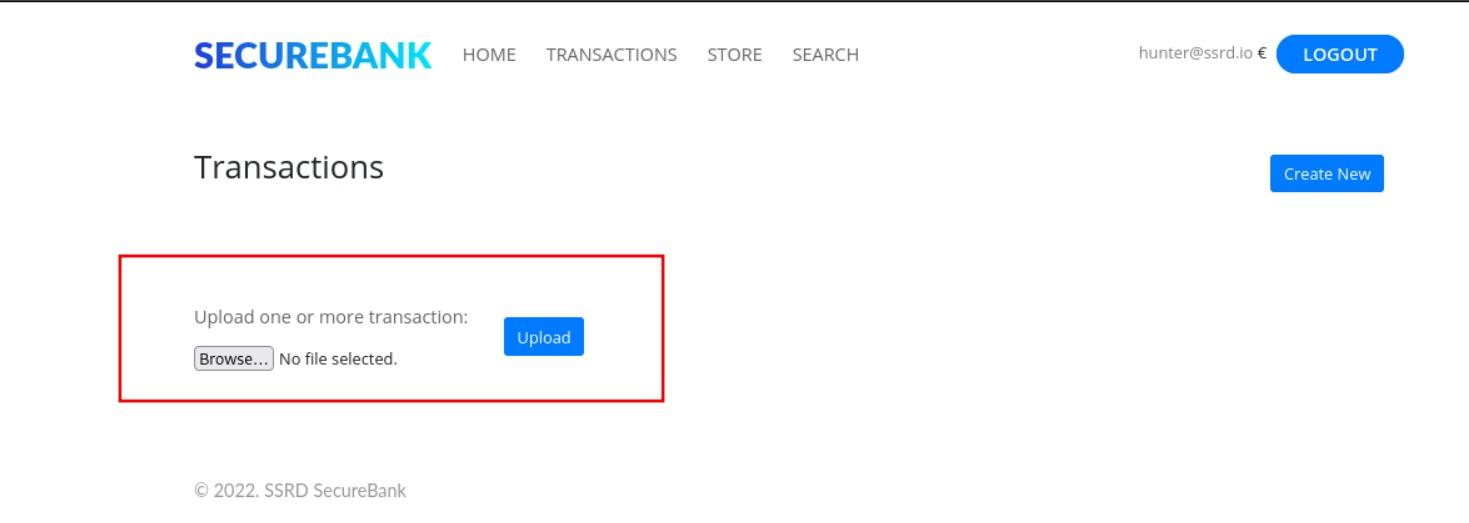


Image **8** – Exploitation de la faille XXE

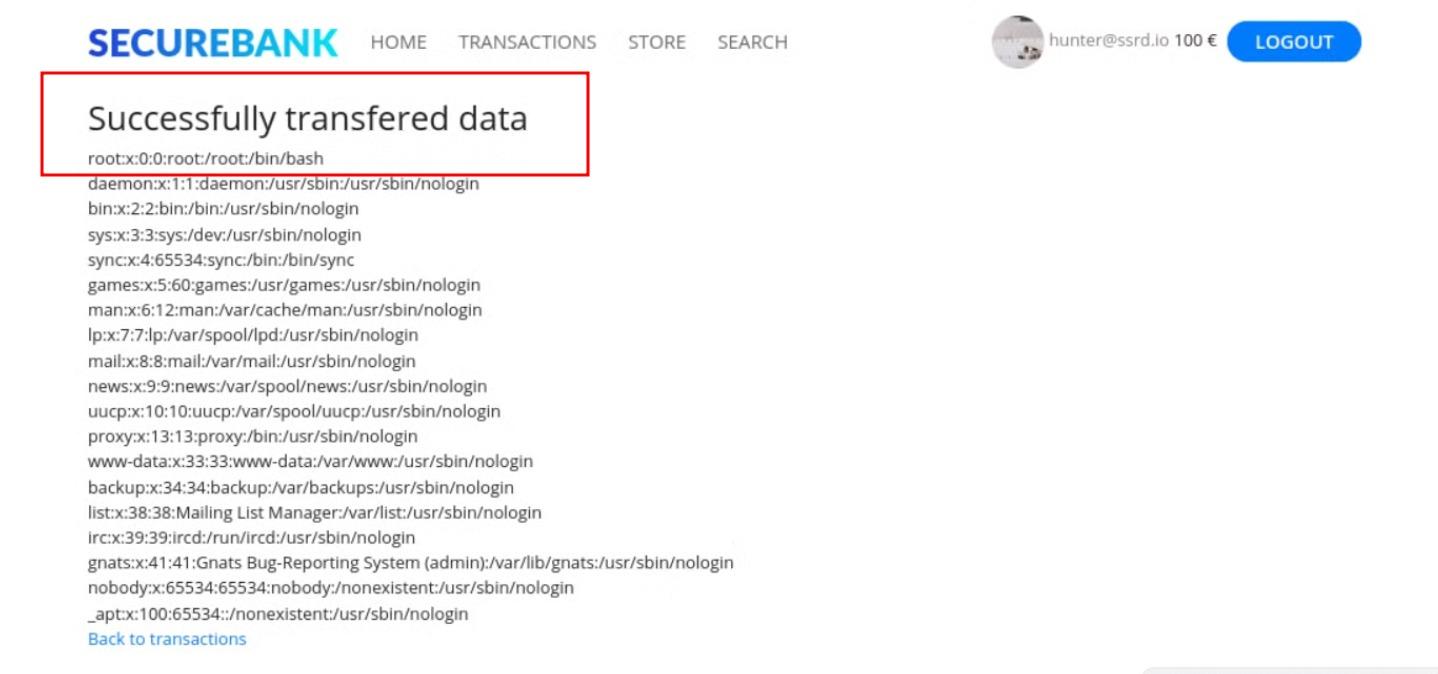


Image **9** – Accès aux noms d'utilisateurs

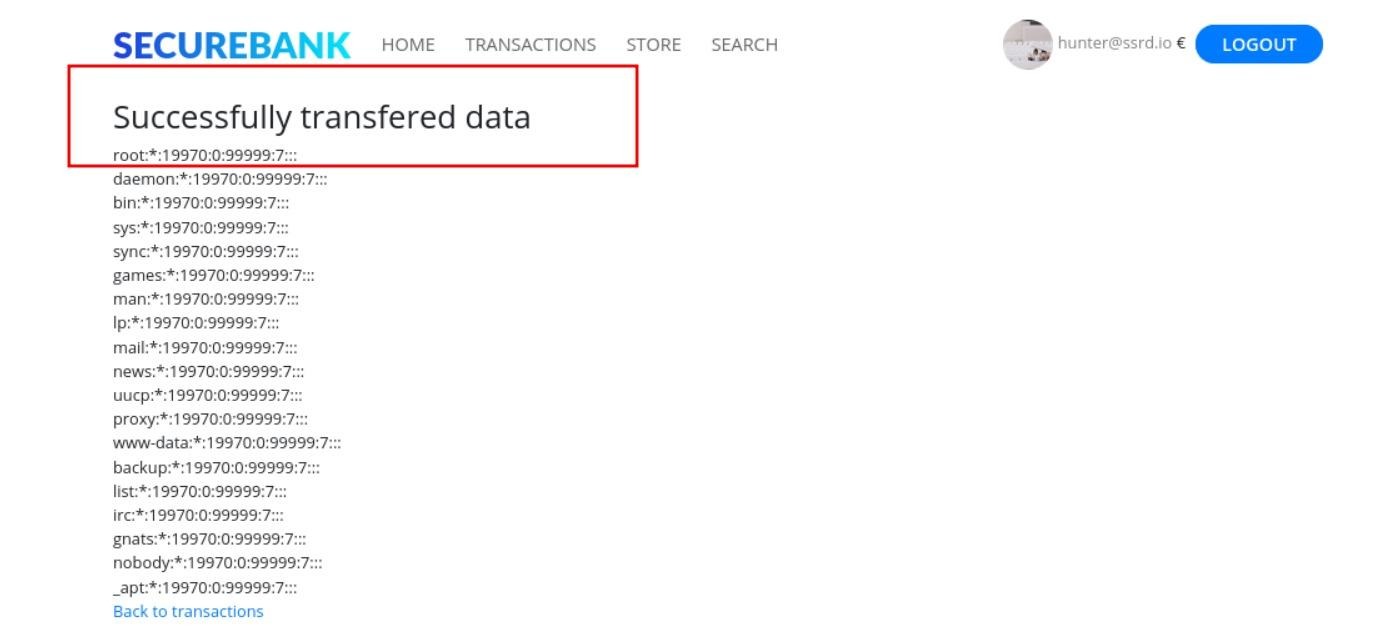


Image **10** – Accès aux mots de passe utilisateurs