International Journal of Innovative Research and Scientific Studies, 8(2) 2025, pages: 2356-2371

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

OTP security in wallet systems: A vulnerability assessment

Ahmad H. Al-Omari[1*], Ahmad Ghazi Alshanty[2], Ayoub Alsarhan[3], Saifullah A. Omari[4]

[1,2]*Cyber Security Department Faculty of Science and Information Technology Al-Zaytoonah University of Jordan*
[3]*Department of Information Technology, Faculty of Prince Al-Hussein Bin Abdallah II for Information Technology, The Hashemite University, Zarqa 13116, Jordan*
[4]*A-Secure Company Cybersecurity Technical Department Amman, Jordan*

Corresponding author: Ahmad H. Al-Omari (*Email: a.alomari@zuj.edu.jo*)

Abstract

This study investigates One-Time Password (OTP) vulnerabilities in digital wallet systems, employing penetration testing and manual security evaluations (via Burp Suite) to assess risks across authentication, fund transfers, IVR verification, and token lifecycle management. Critical gaps including OTP bypass (e.g., header manipulation, token reuse), unauthorized beneficiary additions, brute-force attacks on weak pincodes, and expired OTP exploitation, highlight systemic flaws in server-side validation and API security. Classified using CVSS and ISO/IEC 27005:2018 frameworks, these vulnerabilities demonstrate high exploitability and impact, exacerbated by poor usability-security trade-offs. The findings underscore the inadequacy of current OTP implementations against evolving threats like SIM-swapping and phishing, which jeopardize financial safety and regulatory compliance. To mitigate risks, the study proposes multi-factor authentication (MFA), cryptographic token hardening, AI-driven threat detection, and behavioral monitoring to strengthen defenses. Additionally, user education, strict token expiration policies, and adaptive authentication models are emphasized to address human-factor vulnerabilities. These strategies aim to establish scalable, user-centric frameworks that balance security with usability while aligning with industry standards. The research advocates for proactive defense mechanisms, continuous security audits, and adaptive learning systems to safeguard digital transactions, reinforcing trust in wallet ecosystems amid rising cyber threats.

Keywords: API Security, Behavioral Analysis, Cybersecurity, Digital Wallet Security, Financial Security, Mobile Payment Systems, One-Time Password, OTP Vulnerabilities, Secure Transactions, Token-Based Authentication, Two-Factor Authentication, User Education.

DOI: 10.53894/ijirss.v8i2.5691
Funding: The authors would like to thank the Deanship of scientific research and Innovation at Al-Zaytoonah University of Jordan (ZUJ).
History: Received: 12 February 2025 / **Revised:** 14 March 2025 / **Accepted:** 20 March 2025 / **Published**: 26 March 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Institutional Review Board Statement: The Ethical Committee of Al-Zaytoonah University of Jordan, has reservations not to publish this work, and the work is complied with the publication ethics and guidelines.
Publisher: Innovative Research Publishing

1. Introduction

The digital payments market has become a key part of how we handle money today, making it easy to pay through mobile wallets, online transfers, and digital currencies. Thanks to better technology, more people having internet access, and the rise of smartphones, digital payments have grown massively—reaching around $4.7 trillion by 2020 and still growing [1, 2]. But with all this progress comes new challenges, especially in cybersecurity. For example, credit cards, which banks issue, let people buy things using systems like POS terminals or online authorization. While they're super convenient, they also come with risks, like OTP vulnerabilities, which shows why we need stronger security in wallet technologies [3].

The shift from physical to digital transactions underscores the need for secure authentication mechanisms to safeguard sensitive user data. Static passwords, while convenient, have proven insufficient against evolving cyber threats such as phishing, brute-force attacks, and malware infiltration [4]. According to the Ponemon Institute, 64% of organizations have faced data breaches resulting from phishing incidents, highlighting the inadequacy of password-only systems [5]. This reality necessitates the adoption of more robust authentication methods to protect user accounts and financial transactions.

Multifactor authentication (MFA) has emerged as a pivotal solution, with two-factor authentication (2FA) striking a balance between security and user convenience. 2FA requires users to provide two forms of verification, typically combining something they know (e.g., a password) with something they have (e.g., a device) or something they are (e.g., biometrics). One-Time Passwords (OTPs), a widely used 2FA method, enhance security by generating unique, time-sensitive codes for single-use authentication. By requiring both a static password and an OTP, these systems mitigate the risk of unauthorized access [6].

Despite their advantages, OTP-based systems are not impervious to attacks. SMS-based OTPs, in particular, are vulnerable to interception, phishing, and SIM-swapping, which allows attackers to reroute OTP messages to unauthorized devices [7, 8]. Acknowledging these risks, the National Institute of Standards and Technology (NIST) advised against SMS-based OTPs in its 2023 guidelines [9]. Nevertheless, their simplicity and broad compatibility with existing infrastructure have sustained their prevalence, particularly in regions where advanced authentication options are less accessible.

The vulnerabilities of SMS-based OTPs pose significant concerns for mobile wallet systems, which store sensitive financial information and enable real-time transactions. A compromised wallet system can lead to financial losses, erosion of user trust, and hindered adoption of digital payment solutions. Attackers exploit weaknesses such as insecure transmission channels and poor implementation practices to bypass OTP security. For example, man-in-the-middle attacks can intercept OTPs during transmission, while SIM-swapping enables attackers to hijack OTPs without the user's knowledge [10].

Implementing secure OTP protocols requires adherence to stringent standards. Secure OTP generation relies on cryptographic algorithms that produce time-sensitive, unpredictable codes. Protocols such as HMAC-based One-Time Password (HOTP) and Time-based One-Time Password (TOTP) synchronize code generation between the user's device and the server [11]. However, poor implementation practices—such as weak API configurations and improper OTP storage—can undermine these safeguards.

Researchers have proposed various methods to enhance OTP-based authentication. One approach integrates encrypted OTPs with biometric verification, such as fingerprint scans, to mitigate the risk of OTP interception and replay attacks [12]. Other methods, like QR code-based OTPs, have been introduced to reduce vulnerabilities associated with SMS-based delivery by utilizing secure and tamper-resistant transmission channels [13].

Nevertheless, challenges persist, particularly in resource-constrained environments where infrastructure limitations drive reliance on SMS-based OTPs. Advanced security measures, such as hardware tokens or biometric systems, may be impractical due to high costs and user adoption barriers. Consequently, cost-effective and scalable solutions are essential to mitigate OTP vulnerabilities in such contexts [2].

Human factors also play a crucial role in OTP security. User unawareness and the prioritization of convenience over security often undermine the effectiveness of OTP-based systems. Phishing schemes that deceive users into revealing OTPs remain prevalent, and sending OTPs as plaintext through SMS or email exacerbates the risk [14]. Addressing these issues necessitates not only technical enhancements but also user education and awareness campaigns to encourage secure practices.

Existing literature emphasizes the need for comprehensive OTP vulnerability assessments specific to wallet systems. While general OTP security has been widely studied, fewer works have examined their implementation in mobile wallets, which present unique challenges. Features such as contactless payments and loyalty program integrations introduce additional attack vectors absent in standalone systems [15].

This study aims to fill this gap by conducting an extensive vulnerability assessment of OTP-based authentication in wallet systems. The research focuses on identifying weaknesses, evaluating current mitigation strategies, and proposing actionable recommendations to enhance mobile wallet security. By leveraging real-world attack scenarios and recent research findings, this study contributes to the broader understanding of digital payment security and informs best practices for developers, financial institutions, and policymakers.

The findings of this study have broader implications beyond wallet systems. As digital payments continue to grow globally, the lessons learned from OTP vulnerabilities can inform authentication strategies across various digital platforms. By addressing both technical and human factors, this research aims to strengthen the security of digital ecosystems and foster greater trust in their usage.

2. Related Work

Numerous researchers have examined different facets of One-Time Password (OTP) implementations, including their applications and inherent vulnerabilities. The following studies offer a comprehensive overview of methodologies and findings in this domain.

Karia, et al. [16] developed a system for securing OTP transmissions by using encryption to mitigate interception and replay attacks. Their study highlighted that while encryption enhances OTP security during transmission, the overall effectiveness depends on the correct implementation of encryption protocols. They recommended deploying robust encryption techniques to address these vulnerabilities.

Srinivas and Janaki [17] introduced a novel OTP generation approach using image-based methods to enhance randomness and mitigate brute-force attempts. Their research demonstrated that non-traditional OTP generation methods improve unpredictability but may increase resource consumption. They proposed further research into balancing security improvements with performance efficiency.

Yoo, et al. [18] conducted a case study on OTP vulnerabilities in South Korean internet banking systems. They identified significant weaknesses, including susceptibility to man-in-the-middle attacks and poorly secured APIs. Their findings emphasized that insecure API configurations and the absence of encryption exposed OTP systems to threats. The study recommended adopting end-to-end encryption and secure API configurations to mitigate these risks.

Kalaikavitha and Gnanaselvi [19] proposed a secure login framework that combines OTPs with encryption and mobile-based login techniques. Their approach involved encrypting OTPs before transmission to reduce the risks of eavesdropping and unauthorized access. The study concluded that encryption substantially improves security but may face scalability issues in large-scale deployments.

Ma, et al. [20] performed an empirical analysis of SMS-based OTP authentication in Android applications, revealing security flaws such as weak API settings and insufficient encryption. The study noted that attackers could exploit these weaknesses and recommended implementing stringent API security measures and encryption standards to fortify OTP authentication.

Yaswanth and Reddy [21] explored biometric-enhanced OTP systems that combined biometric hash codes with secret keys. This hybrid method aimed to reinforce traditional OTPs with biometric verification. Their results indicated that incorporating biometrics significantly reduced unauthorized access attempts but required advanced infrastructure. The authors suggested adopting multi-factor authentication (MFA) that integrates biometrics for environments requiring higher security.

Hariram, et al. [22] proposed an e-authentication system that incorporated QR codes with OTPs to address the vulnerabilities of SMS-based OTP delivery. Their findings showed that dynamic methods, such as QR codes, offered improved resistance against interception. However, they also noted that user familiarity with QR codes may present an adoption barrier.

Bartłomiejczyk and El Fray [23] conducted an in-depth analysis of phishing, social engineering, and SIM-swapping attacks targeting SMS OTPs. They reviewed existing countermeasures and recommended layered defense strategies, including user education and multi-factor safeguards, to mitigate social engineering risks.

Ataelfadiel [24] proposed a QR code-integrated OTP system designed to reduce reliance on mobile networks. Their research highlighted that QR-based OTPs provided a secure alternative to SMS delivery by eliminating network-based vulnerabilities. They suggested that this method be used for high-security applications but acknowledged the potential challenges in user adaptation.

Aparicio, et al. [25] focused on OTP security in banking applications, particularly highlighting issues related to insecure API configurations. The study underscored that weak APIs are a major vulnerability and proposed a set of best practices, including endpoint hardening and regular security audits, to protect against exploitation.

Yoo, et al. [26] examined the influence of user behavior and OTP message content in the context of SMS-based 2FA. Their findings emphasized that poor message design and a lack of user awareness compromised OTP security. The study advocated for enhanced message structuring and awareness campaigns to improve user compliance with security best practices.

These studies collectively underscore the critical need for secure OTP delivery mechanisms, robust encryption, fortified APIs, and the integration of biometric and dynamic authentication methods. Additionally, they highlight the importance of user education in addressing social engineering threats. The insights gained from these works contribute to advancing the security of OTP-based systems in various contexts, particularly in mobile wallets and digital banking platforms.

3. Related Work Gap Analysis

While a lot of research has been done on OTP systems, there are still some significant gaps that need attention, especially when it comes to scaling up and working efficiently in systems with limited resources. Studies like those by Karia, et al. [16] and Kalaikavitha and Gnanaselvi [19] show how encryption helps protect OTPs from being intercepted or reused in attacks. However, these studies do not fully address the challenges of using OTPs in large systems or in resource-constrained environments. Moving forward, researchers should focus on creating simpler, lightweight encryption methods that maintain security without compromising performance—something especially important for applications like mobile wallets. This ties back to the fundamentals of information security, which emphasize confidentiality, integrity, and availability [27].

Innovative OTP generation methods, such as image-based techniques [17] provide enhanced randomness and resistance to brute-force attacks. However, their feasibility remains underexplored in mobile environments where computational resources are constrained. Further studies are needed to evaluate the real-world performance of these methods and determine how they can be integrated into existing authentication frameworks without imposing significant processing overhead.

API security has been consistently identified as a critical vulnerability in OTP implementations [18, 20, 25]. Although these studies recommend encrypting API communications and strengthening API configurations, they lack comprehensive frameworks that address OTP-specific threats. Additionally, the dynamic nature of attack patterns, such as automated API exploitation, necessitates ongoing research to develop adaptive security strategies and OTP-specific API protection guidelines.

The integration of biometrics with OTP systems shows considerable potential for reducing unauthorized access risks [21]. However, the associated costs, privacy concerns, and infrastructural requirements have not been thoroughly addressed. Further research should focus on the feasibility of biometric-OTP integration across diverse environments, especially in resource-constrained settings, and explore potential vulnerabilities, such as biometric spoofing and data breaches.

QR code-based OTP delivery methods provide a secure alternative to SMS-based OTPs [13, 22]. However, these studies fall short of addressing the usability challenges associated with QR codes, particularly for less tech-savvy users. Research is needed to design user-friendly QR code-based systems and assess their effectiveness across various demographics to ensure widespread adoption and usability.

While studies have highlighted the vulnerabilities of SMS OTPs—such as phishing, SIM-swapping, and social engineering attacks [23] most research has focused on mitigation rather than alternatives. There is a need to explore alternative OTP delivery mechanisms, such as app-based OTPs or blockchain-secured authentication, which can eliminate reliance on SMS while maintaining scalability and security.

The role of user behavior and OTP message design in securing OTP systems has been explored Yoo, et al. [26] but existing research provides limited guidance on implementing large-scale user education initiatives. The influence of cultural and linguistic factors on user adherence to security best practices also remains underexamined. Future research should prioritize the development of tailored awareness programs to promote secure behaviors among diverse user groups.

A notable gap in the literature is the lack of empirical studies examining OTP vulnerabilities specific to mobile wallet systems. While some research Ma, et al. [20] and Aparicio, et al. [25] investigates OTP implementations in banking and Android applications, it does not fully address the unique challenges of mobile wallets. These systems often feature contactless payments and loyalty program integrations, which introduce additional attack vectors. Research should focus on identifying these unique vulnerabilities and proposing tailored security solutions for mobile wallets.

Emerging threats, such as AI-driven phishing attacks and automated OTP exploitation, have received minimal attention in the current literature. Additionally, decentralized authentication technologies, such as blockchain, remain underexplored despite their potential to enhance OTP security. Future studies should investigate these emerging threats and evaluate how advanced technologies can strengthen OTP implementations.

Finally, most studies concentrate on isolated aspects of OTP security, such as encryption or API protection, without considering comprehensive frameworks that integrate technical, organizational, and user-centric measures. Developing holistic security frameworks that address these dimensions cohesively could significantly improve the resilience of OTP systems across various digital platforms.

4. Methodology

The assessment involved testing OTP functionalities through a systematic penetration testing approach. Each OTP function was evaluated for potential bypass mechanisms, token validation errors, and timeout handling. The key functionalities analyzed include:

1. Login OTP
2. Adding Beneficiaries
3. Fund Transfer to Contacts
4. Adding Bills
5. IVR Verification
6. OTP Timeout and Expiration
7. OTP-Pincode

One-Time Passwords (OTPs) are a common security mechanism in digital wallet systems, providing user authentication and transaction validation. However, these systems, being pivotal to real-time financial transactions, are prone to OTP-related security flaws that can endanger user data and facilitate financial fraud [20, 26]. This study offers an in-depth assessment of OTP implementations within wallet systems, focusing on their resilience against various exploitation attempts. Through a detailed analysis of OTP mechanisms, we identify security vulnerabilities and present actionable strategies to improve the overall robustness of wallet systems.

4.1. Research Environment

The assessment was conducted in a real production environment for one of the industry's well-known digital wallet systems, handling live transactions and sensitive user data. This environment reflected the authentic operational setup, ensuring that the findings were not simulated but based on actual system interactions and live security mechanisms. The production system included critical features such as user authentication, financial operations, and beneficiary management, each protected by various security layers, including One-Time Password (OTP) verification. Conducting the assessment in such a high-stakes environment allowed for an accurate evaluation of vulnerabilities that could have a direct impact on real users. Additionally, the production nature of the system mandated rigorous compliance with regulatory standards and the need to minimize any operational impact during testing, necessitating a careful and controlled approach to avoid service disruptions while capturing genuine security insights.

The assessment was carried out as a comprehensive and manual security evaluation to ensure in-depth coverage of potential vulnerabilities. The primary tool employed during this process was Burp Suite, an industry-standard web vulnerability scanner and proxy tool used to intercept and analyze web traffic. Burp Suite facilitated the manual inspection of requests and responses, enabling us to identify flaws in the business logic and to exploit gaps discovered within the source code. This methodology allowed for a thorough examination of the OTP mechanisms to identify and validate the associated vulnerabilities.

4.2. Objectives

Our research study assessment focuses on evaluating the security of OTP functionalities across various processes to identify weaknesses and recommend mitigation strategies to achieve the following objectives:

- Assess the security of OTP functionalities across various processes, including login, beneficiary management, fund transfers, bill additions, IVR verification, and OTP-Pincode usage.
- Identify potential vulnerabilities that attackers could exploit in OTP-related processes.
- Provide targeted recommendations to mitigate identified security risks.

4.3. Classification of Severity Levels

The severity levels for each identified vulnerability were classified based on the following criteria:

Impact: The potential damage or consequence of exploiting the vulnerability (e.g., unauthorized access, financial loss, data exposure).

Exploitability: The ease with which an attacker can exploit the vulnerability (e.g., requires special tools or can be exploited using basic tools).

Scope: The extent of users or systems affected by the vulnerability.

Regulatory Implications: Compliance risks associated with data protection regulations or industry standards.

These criteria align with established security frameworks such as the Common Vulnerability Scoring System (CVSS) [1] and international standards like ISO/IEC 27005:2018, which provide structured methodologies for risk assessment and severity classification [2].

The vulnerabilities identified in this study include:

- Login OTP
- Adding Beneficiaries
- Fund Transfer to Contacts
- Adding Bills
- IVR Verification (Interactive Voice Response)
- OTP Timeout and Expiration
- OTP-Pincode

The chosen methodology and classification of severity levels are pivotal to ensuring a structured and accurate evaluation of vulnerabilities. By employing a systematic penetration testing approach, the research identifies weaknesses in OTP implementations through practical and repeatable techniques. Furthermore, classifying vulnerabilities based on impact, exploitability, scope, and regulatory implications provides a clear framework for prioritizing mitigation efforts. This approach aligns with established security standards, ensuring consistency and scientific rigor in the analysis [1, 2].

5. Results

5.1. OTP Evaluation Mechanisms

We perform intensive evaluation on the different OTPs to understand the weakness in OTP implementations. The following sections explain the findings.

5.2. Login OTP

Login OTPs (One-Time Passwords) are dynamic, single-use passwords used to verify user identity during login attempts. By requiring an additional factor beyond static passwords, they enhance security against unauthorized access [3]. However, vulnerabilities such as interception and phishing necessitate secure delivery and implementation [4].

Table 1.
Vulnerabilities Identified in Login OTP.

Vulnerability Reference	Vulnerability Description	Impact	Exploitability	Recommendations
OTP-01	Unauthenticated Account Access via OTP Bypass	High	Moderate	Validate mobile numbers server-side
OTP-02	Reused OTP Token Allows Unauthorized Login	Medium	Moderate	Enforce strict token expiration policies

Table 1 Vulnerabilities Identified in Login OTP details the vulnerabilities identified in Login OTP, focusing on bypass techniques and token reuse, highlighting the need for robust server-side validation and token management. For example, "OTP Bypass" demonstrates higher levels of both impact and exploitability compared to "Token Reuse," indicating a more critical priority for mitigation.

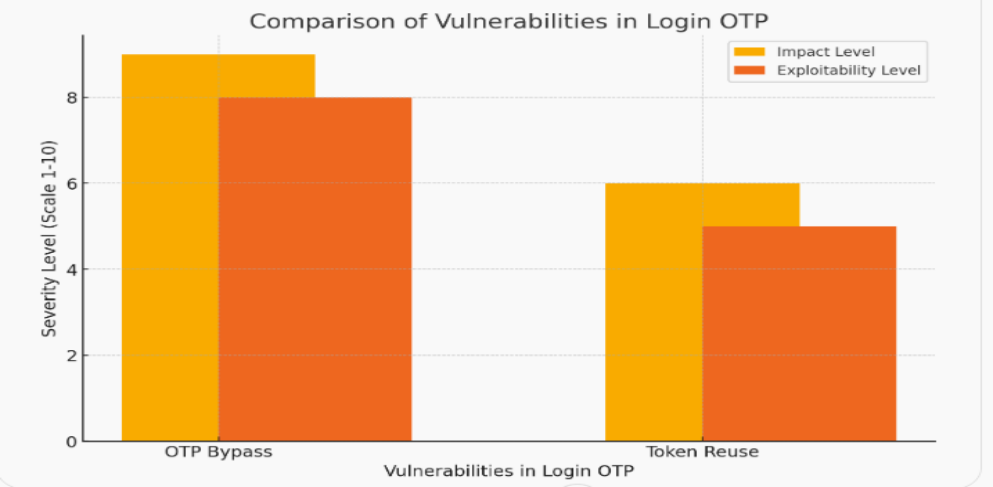

Figure 1.
Vulnerabilities in the Login OTP

Figure 1.

Vulnerabilities in the Login OTP, visually compares the vulnerabilities identified in the Login OTP functionality, focusing on their impact and exploitability levels, the figure highlights:

1. Impact Level: The severity of consequences if the vulnerability is exploited.
2. Exploitability Level: The effort required for an attacker to exploit the vulnerability.

For example, "OTP Bypass" demonstrates higher levels of both impact and exploitability compared to "Token Reuse," indicating a more critical priority for mitigation.

Vulnerability 1: Unauthenticated Account Access via OTP Bypass

- Description: Attackers intercepted and manipulated mobile number fields in OTP requests to bypass verification and gain unauthorized access.
- Impact: High risk of unauthorized account access.
- Recommendations: Implement strict server-side validation of mobile numbers and session tokens.

Vulnerability 2: Reused OTP Tokens

- Description: Expired OTP tokens were accepted, allowing attackers to bypass verification.
- Impact: Medium risk of account hijacking.
- Recommendations: Enforce strict token expiration policies and invalidate tokens after a single use.

5.3. Adding Beneficiaries

The OTP process for adding beneficiaries in digital wallets ensures that only authorized users can create or modify recipient details. This critical security step prevents unauthorized additions, but flaws such as token reuse or insecure delivery can expose the system to risks [5].

Table 1.
Vulnerabilities in the Adding Beneficiaries.

Vulnerability Reference	Vulnerability Description	Impact	Exploitability	Recommendations
OTP-03	Unauthorized Beneficiary Addition	High	High	Validate beneficiary addition requests server-side
OTP-04	Bypassed OTP Process via Header Manipulation	High	High	Require header verification for OTP processes
OTP-05	Multiple Beneficiaries Added with	Medium	Moderate	Limit OTP validity to a single

Vulnerability Reference	Vulnerability Description	Impact	Exploitability	Recommendations
	Single OTP			transaction

Table 1.

Vulnerabilities in the Adding Beneficiaries, emphasizing risks like unauthorized additions and header manipulation, requiring strict validations.

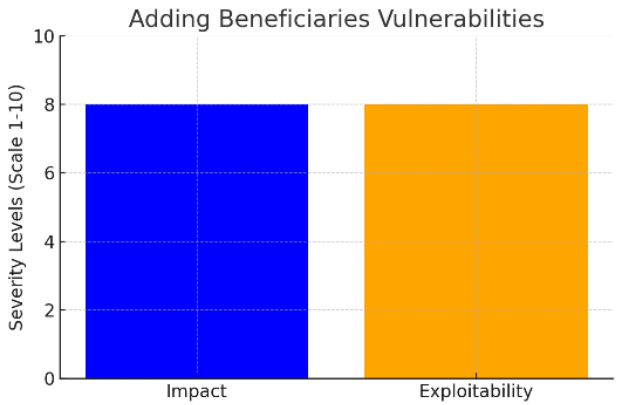

Figure 2.
Vulnerabilities in the Adding Beneficiaries.

Figure 2.

Vulnerabilities in the Adding Beneficiaries, visually compares the vulnerabilities identified in the Adding Beneficiaries functionality, focusing on their impact and exploitability levels making them priorities for mitigation:

Vulnerability 3: Unauthorized Beneficiary Addition

- Description: Attackers bypassed OTP verification by modifying mobile number fields during requests.
- Impact: High risk of fraud.
- Recommendations: Validate all beneficiary addition requests with server-side checks.

Vulnerability 4: Bypassed OTP Process via Header Manipulation

- Description: Omitting the X-OTP header enabled unauthorized beneficiary additions.
- Impact: High risk of regulatory non-compliance.
- Recommendations: Require header verification for all OTP-related requests.

5.4. Fund Transfer

Fund transfer OTPs are used to validate and authorize financial transactions to contacts. By requiring real-time user input, they reduce fraud risks. However, attacks like man-in-the-middle and SIM-swapping emphasize the need for robust transmission methods [4].

Figure 3.

Vulnerabilities in the Fund Transfer, compares the vulnerabilities identified in the Fund Transfer functionality, focusing on their impact and exploitability levels. The figure highlights key risks like "Unauthorized Transfer" demand immediate attention due to their critical severity and ease of exploitation.

.

Figure 3.
Vulnerabilities in the Fund Transfer**.**

Table 2.
Vulnerabilities in the Fund Transfer.

Vulnerability Reference	Vulnerability Description	Impact	Exploitability	Recommendations
OTP-06	Unauthorized Fund Transfers	High	High	Enforce secure token validation mechanisms
OTP-07	Unrestricted Transfer without OTP Validation	High	High	Require mandatory OTP header validation
OTP-08	Multiple Transfers with a Single OTP	Medium	Moderate	Limit OTP reuse to a single transaction

Figure 3.

Vulnerabilities in the Fund Transfer.

Table 2.

Vulnerabilities in the Fund Transfer, summarizes vulnerabilities in Fund Transfer functionality, focusing on unauthorized transactions and token misuse.

Vulnerability 5: Unauthorized Fund Transfers

- Description: Manipulating mobile number fields allowed attackers to initiate unauthorized transfers.
- Impact: High risk of financial loss.
- Recommendations: Enforce secure token validation mechanisms.

Vulnerability 6: Multiple Transfers with a Single OTP

- Description: Attackers reused valid OTP tokens to perform multiple unauthorized transactions.
- Impact: Medium risk of abuse.
- Recommendations: Limit OTP validity to a single transaction.

5.5. Adding Bills

OTPs for adding bills ensure secure linkage of billing accounts to a user's profile. This step prevents fraudulent activity, but poor timeout mechanisms and weak encryption of tokens can compromise the process [6].

Table 3.

Vulnerabilities in Adding Bills identifies vulnerabilities in Adding Bills functionality, highlighting risks of unauthorized additions and lack of OTP verification.

Table 3.
Vulnerabilities in Adding Bills.

Vulnerability Reference	Vulnerability Description	Impact	Exploitability	Recommendations
OTP-09	Unauthorized Bill Addition	High	Moderate	Implement strong field validation
OTP-10	Bill Added Without Proper OTP Verification	High	Moderate	Ensure OTP verification for all bill additions

Vulnerability 7: Unauthorized Bill Additions

- Description: Manipulating mobile numbers allowed unauthorized bill entries.
- Impact: High risk of fraudulent activity.
- Recommendations: Implement strong field validation and restrict access based on user roles.

Figure 4.

Vulnerabilities in the Adding Bills, compares the vulnerabilities identified in the Adding Bills functionality, such as "Unauthorized Addition" in Adding Bills, showcasing their severity and potential for exploitation. Addressing these weaknesses is essential to maintain system integrity.

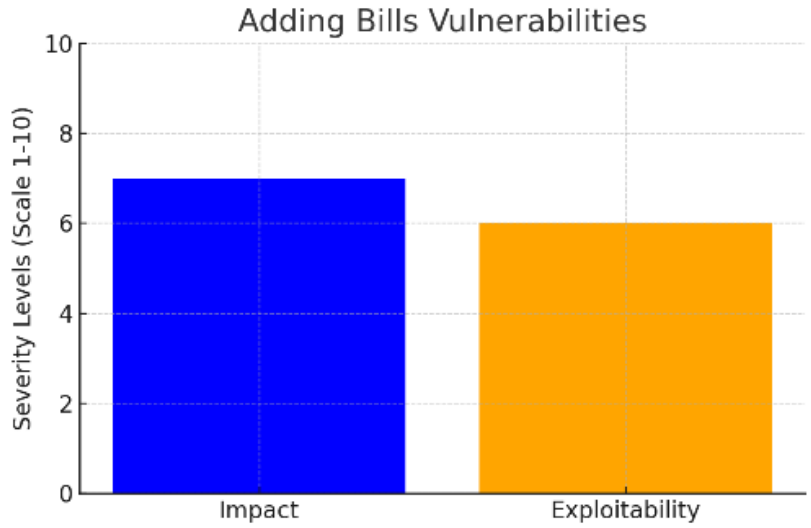

Figure 4.
Vulnerabilities in the Adding Bills.

5.6. IVR Verification

IVR (Interactive Voice Response) OTPs are used to authenticate users during voice-based interactions. Delivered via SMS or audio playback, they protect sensitive operations. However, vulnerabilities in delivery channels and replay attacks can undermine their effectiveness [7].

Table 4.
Vulnerabilities in IVR Verification.

Vulnerability Reference	Vulnerability Description	Impact	Exploitability	Recommendations
OTP-11	Beneficiary Verification Compromised via IVR	Medium	Moderate	Ensure IVR systems authenticate calls securely

Table 4.

Vulnerabilities in IVR Verification details vulnerabilities in IVR Verification, emphasizing the need for secure session validation to prevent bypass.

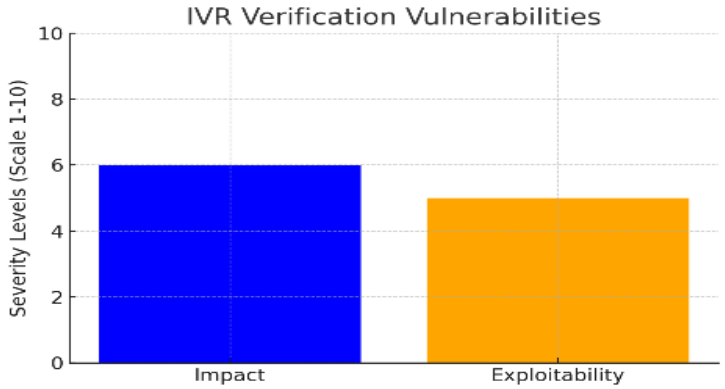

Figure 5.
Vulnerabilities in the IVR Verification.

Figure 5.

Vulnerabilities in the IVR Verification, compares the vulnerabilities identified in the IVR Verification functionality, focusing on their impact and exploitability levels, the figure provides insights into vulnerabilities in IVR Verification, such as "IVR Bypass," emphasizing their relative ease of exploitation and moderate impact.

Vulnerability 8: Bypassed IVR Call Validation

- Description: Attackers intercepted and manipulated mobile numbers to bypass IVR verification.
- Impact: Medium risk of fraud.
- Recommendations: Ensure IVR systems authenticate calls through secure session validation.

5.7. OTP Timeout

Timeout mechanisms ensure OTPs are invalidated after a short duration, reducing the risk of unauthorized use. Poor implementation, such as overly extended validity or predictable expiration policies, can be exploited by attackers [2].

Figure 6.

Vulnerabilities in the OTP Timeout, compares the vulnerabilities identified in the OTP Timeout functionality, focusing on their impact and exploitability levels. The figure compares vulnerabilities like "Expired OTPs Accepted" in OTP Timeout, highlighting their moderate impact and lower exploitability compared to other functionalities.

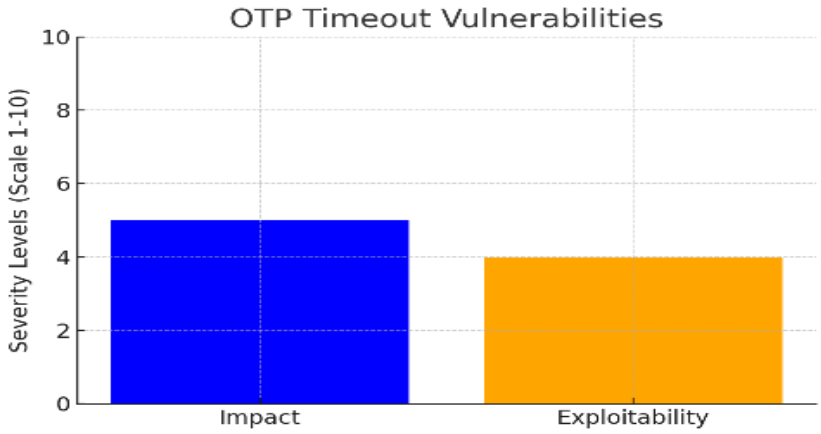

Figure 6.
Vulnerabilities in the OTP Timeout.

Table 5.
Vulnerabilities in the OTP Timeout.

Vulnerability Reference	Vulnerability Description	Impact	Exploitability	Recommendations
OTP-12	OTP Expiration Failure Leads to Extended Access	Medium	Low	Enforce strict expiration checks on all OTPs

Figure 6.

Vulnerabilities in the OTP Timeout, highlights vulnerabilities in OTP Timeout and Expiration, focusing on risks from accepting expired OTPs.

Vulnerability 9: OTP Expiration Failure

- Description: Expired OTPs were accepted in certain functionalities.
- Impact: Medium risk of unauthorized operations.
- Recommendations: Enforce strict expiration checks across all OTP validations.

5.8. OTP-Pincode

The combination of OTPs and PIN codes strengthens two-factor authentication by requiring both dynamic and static credentials. While this method improves security, vulnerabilities in storage or transmission of either factor can compromise the system [8].

Table 6.

Vulnerabilities in OTP-Pincode summarizes vulnerabilities in OTP-Pincode functionality, with emphasis on risks from session management flaws and brute-force attacks.

Table 6.
Vulnerabilities in OTP-Pincode.

Vulnerability Reference	Vulnerability Description	Impact	Exploitability	Recommendations
MH12	Authenticated User Viewing Other Consumers' Data	High	High	Implement robust session management
MH13	Authenticated User Changing Other Consumers' Passcodes	High	High	Validate session tokens and user actions
MH14	Pincode Brute-Forcing	High	High	Implement account lockouts and rate limiting

Vulnerability 10: Authenticated User Viewing Other Consumers' Sensitive Information, where authenticated users could access sensitive information of other consumers, such as mobile numbers and unique identifiers.

- Impact: High risk of data exposure and misuse.
- Recommendations: Implement robust session management to ensure data visibility is limited to authorized users only.
  Vulnerability 11: Authenticated User Changing Other Consumers' Passcodes. Exploiting vulnerabilities in session management allowed authenticated users to change passcodes of other consumers.
- Impact: High risk of account compromise.
- Recommendations: Ensure backend validation ties session tokens strictly to user actions.
  Vulnerability 12: Pincode Brute-Forcing. Weak pincode implementation allowed brute-force attacks to compromise consumer accounts.
- Impact: High risk of unauthorized account access.
- Recommendations: Enforce account lockout after multiple failed attempts, increase pincode complexity, and implement rate limiting on verification attempts.

Table 7.
OTPs Vulnerabilities Summary.

OTP Function	Key Vulnerabilities	Common Impacts	Recommendations
Login OTP	Bypass via Manipulation, Token Reuse	Unauthorized Access, Account Hijacking	Strict server-side validation, enforce token expiration
Adding Beneficiaries	Unauthorized Addition, Header Manipulation, Reuse	Fraudulent Transactions	Validate beneficiary addition, limit OTP validity
Fund Transfer	Unauthorized Transfers, Header Removal, Token Reuse	Financial Loss, Fraud	Secure token validation, mandatory OTP header checks
Adding Bills	Unauthorized Addition, Lack of OTP Verification	Fraudulent Bill Entries	Enforce OTP verification for all transactions
IVR Verification	IVR Bypass	Compromised Verification	Secure session validation for IVR systems
OTP Timeout	Acceptance of Expired OTPs	Extended Access to Secure Functions	Enforce strict expiration checks
OTP-Pincode	Data Exposure, Passcode Change, Brute Forcing	Account Compromise, Data Breaches	Robust session management, account lockouts

5.9. Summary of Vulnerabilities Across OTP Functionalities

This section introduces a summary of vulnerabilities identified across different OTP applications, focusing on their potential impact on system resilience. The summary, presented in Table 7.

OTPs Vulnerabilities Summary, consolidates vulnerabilities across various functionalities, highlighting common risks such as unauthorized access, fraudulent activities, and data breaches. By examining weaknesses in implementation and delivery methods, this overview emphasizes the need for stricter validation mechanisms, enhanced session management, and robust token policies to mitigate these risks effectively.

6. Discussion

The findings of this research highlight significant vulnerabilities in OTP-based authentication within wallet systems, emphasizing systemic weaknesses that compromise user security. The primary issues stem from design flaws that allow attackers to manipulate OTP request parameters, bypass validation mechanisms, and exploit inconsistencies in timeout enforcement. These vulnerabilities, if left unaddressed, pose substantial risks, including unauthorized access, fraudulent transactions, and regulatory non-compliance. In this discussion, we analyze the broader implications of our findings, exploring how these weaknesses impact overall system security and user trust. We examine the effectiveness of current OTP implementations, compare our results with existing research, and propose strategic measures to mitigate risks. By contextualizing these vulnerabilities within real-world financial threats, we underscore the necessity of robust authentication frameworks and continuous security assessments to safeguard digital financial platforms.

6.1. Exploitation-Level Based Comparison of Vulnerabilities

An exploitation-level-based comparison of vulnerabilities involves evaluating the ease with which each vulnerability can be exploited by an attacker, considering factors such as required skill level, tools, and resources [1]. This approach categorizes vulnerabilities based on their exploitability, distinguishing between those that can be exploited with minimal effort and commonly available tools versus those requiring advanced technical expertise and specialized equipment [4]. For example, vulnerabilities like weak OTP transmission mechanisms or poor API security configurations may be relatively simple to exploit using basic interception tools or automated scripts [5]. Conversely, more complex issues, such as bypassing multi-factor authentication integrated with biometrics, may demand sophisticated techniques and higher resource investments [8]. By comparing vulnerabilities on this scale, security teams can prioritize their mitigation efforts, focusing on highly exploitable issues that pose immediate risks while allocating additional resources to address more advanced threats [2]. This method aligns with frameworks such as the Common Vulnerability Scoring System (CVSS), which emphasizes exploitability as a key metric for assessing the overall severity of security risks [1].

The following

Table 8.

Vulnerabilities by Exploitation Level compares vulnerabilities by exploitation level, showcasing the technical effort or resources required to exploit each type.

Table 8.
Vulnerabilities by Exploitation Level.

Exploitation Level	Vulnerabilities	Description	Examples from OTP Functions
High	Unauthorized Access, Data Exposure, Token Reuse	Exploitation requires minimal technical effort or resources.	OTP-01, OTP-03, MH12, MH14
Medium	Header Manipulation, Expired OTPs Accepted	Exploitation requires moderate technical knowledge or resources.	OTP-02, OTP-04, OTP-12
Low	IVR Bypass, Timeout Validation	Exploitation requires advanced effort or has limited impact potential.	OTP-11

- High Exploitation vulnerabilities involve minimal barriers to attack, making them easy targets for malicious actors, such as OTP-01 (Login OTP Bypass).
- Medium Exploitation vulnerabilities require more effort or resources to exploit but still pose significant risks, such as OTP-12 (Expired OTPs Accepted).
- Low Exploitation vulnerabilities demand considerable resources or specialized skills to exploit, and their impact is typically contained, such as OTP-11 (IVR Bypass).

6.2. Impact-Level Based Comparison of Vulnerabilities

An impact-level-based comparison of vulnerabilities focuses on evaluating the potential consequences of a vulnerability's exploitation on an affected system, user, or organization. This approach assesses the severity of harm, including unauthorized access, financial losses, data breaches, or reputational damage [1, 28, 29]. For example, a vulnerability that allows attackers to bypass OTP authentication in a digital wallet system could lead to unauthorized transactions and significant financial losses for users [7]. Similarly, vulnerabilities exposing sensitive user data may result in compliance violations and legal penalties under data protection regulations such as GDPR [2]. By categorizing vulnerabilities based on their impact, organizations can prioritize remediation efforts for those with the highest potential damage, ensuring resources are allocated to mitigate risks that pose the most severe consequences [4]. This methodology

aligns with international standards like ISO/IEC 27005:2018, which emphasize understanding the consequences of risks as a fundamental part of security assessment and management [2].

Table 9.

Vulnerabilities based on their impact level categorizes vulnerabilities based on their impact level, outlining the potential consequences and severity of exploiting these flaws.

Table 9.
Vulnerabilities based on their impact level.

Impact Level	Vulnerabilities	Description	Examples from OTP Functions
High Impact	Unauthorized Access, Data Exposure, Financial Loss	Exploitation leads to severe consequences for users and the system.	OTP-01, OTP-03, MH12, MH14
Medium Impact	Token Reuse, Header Manipulation, OTP Expiration	Exploitation compromises system integrity and user trust but less severe.	OTP-02, OTP-04, OTP-12
Low Impact	Timeout Validation, IVR Bypass	Exploitation results in limited or minimal damage.	OTP-11

- High Impact vulnerabilities involve significant risks, such as financial loss, unauthorized system access, or exposure of sensitive user data, exemplified by OTP-01 (Login OTP Bypass).
- Medium Impact vulnerabilities compromise operational integrity or user trust without causing immediate critical consequences, such as OTP-12 (Expired OTPs Accepted).
- Low Impact vulnerabilities are limited in scope and impact, causing minor inconveniences or operational inefficiencies, such as OTP-11 (IVR Bypass).

6.3. Severity-Level Based Comparison of Vulnerabilities

A severity-level-based comparison of vulnerabilities combines the dimensions of exploitability, impact, and scope to provide a holistic assessment of security risks. This approach categorizes vulnerabilities by evaluating the ease of exploitation, the potential consequences of successful attacks, and the breadth of systems or users affected [1]. For instance, vulnerabilities in OTP systems that allow attackers to bypass authentication could result in financial fraud, unauthorized access, and regulatory non-compliance, particularly if they affect a large user base [4, 7]. Severity-level classification helps organizations prioritize remediation by addressing vulnerabilities that pose the greatest risk to their operations and users. It also ensures compliance with frameworks like the Common Vulnerability Scoring System (CVSS) and ISO/IEC 27005:2018, which emphasize structured methodologies for classifying and managing risks [2]. This comprehensive approach aids decision-makers in allocating resources effectively to mitigate high-severity vulnerabilities first, thereby reducing overall risk exposure.

Table 10.

Vulnerabilities by severity level provides an overview of vulnerabilities categorized by severity level, demonstrating how different security flaws impact the system based on their criticality.

Table 10.
Vulnerabilities by severity level.

Severity Level	Vulnerabilities	Description	Examples from OTP Functions
High	Unauthorized Access, Token Reuse, Data Exposure	Exploitation leads to major security or financial risks.	OTP-01, OTP-03, MH12, MH14
Medium	OTP Expiration, Header Manipulation	Exploitation has moderate impact but still poses significant challenges.	OTP-02, OTP-04, OTP-12
Low	Ineffective Timeout Validation	Minimal impact with lower exploitability.	OTP-11

- High severity vulnerabilities involve risks like financial fraud, user data exposure, or unauthorized access to sensitive functionalities, as seen in OTP-01 (Login OTP bypass).
- Medium severity vulnerabilities have less immediate impact but compromise application integrity or user trust, such as OTP-12 (Expired OTPs accepted).
- Low severity vulnerabilities are less likely to be exploited or have limited impact, such as OTP-11 (IVR call bypass).

6.4. Comparative Analysis of OTP Types

A comparative analysis of One-Time Password (OTP) types examines the strengths, weaknesses, and suitability of different OTP mechanisms for various applications. Common types include SMS-based OTPs, app-based OTPs, and

hardware token-generated OTPs, each offering distinct levels of security, usability, and cost-effectiveness [5]. For instance, SMS-based OTPs are widely adopted due to their simplicity but are vulnerable to attacks such as phishing and SIM-swapping [4]. In contrast, app-based OTPs, such as those generated using Time-based One-Time Password (TOTP) algorithms, provide enhanced security by eliminating reliance on external communication channels [9]. Hardware tokens offer the highest security but often at a higher cost, making them less feasible for widespread consumer applications [8]. Table 12: Comparative analysis of OTPs helps identify the most appropriate OTP type for specific use cases, balancing security, usability, and operational requirements.

Table 11.
Comparative analysis of OTPs.

OTP Function	Vulnerability Reference	Key Vulnerability	Impact	Exploitability	Severity
Login OTP	OTP-01, OTP-02	OTP Bypass via Manipulation and Token Reuse	High, Medium	Moderate	High, Medium
Adding Beneficiary	OTP-03, OTP-04, OTP-05	Unauthorized Addition, Header Manipulation, Reuse	High, High, Medium	High	High, High, Medium
Fund Transfer	OTP-06, OTP-07, OTP-08	Unauthorized Transfer, Header Removal, Token Reuse	High, High, Medium	High	High, High, Medium
Adding Bills	OTP-09, OTP-10	Unauthorized Addition, Header Removal	High, High	Moderate	High
IVR Verification	OTP-11	IVR Bypass	Medium	Moderate	Medium
OTP Timeout	OTP-12	Expired OTPs Accepted	Medium	Low	Medium
OTP-Pincode	MH12, MH13, MH14	Data Exposure, Passcode Change, Brute Forcing	High	High	High

- Impact: The potential damage or consequence of exploiting the vulnerability (e.g., unauthorized access, financial loss, data exposure).
- Exploitability: The ease with which an attacker can exploit the vulnerability (e.g., requires special tools or can be exploited using basic tools).
- Scope: The extent of users or systems affected by the vulnerability.
- Regulatory Implications: Compliance risks associated with data protection regulations or industry standards.

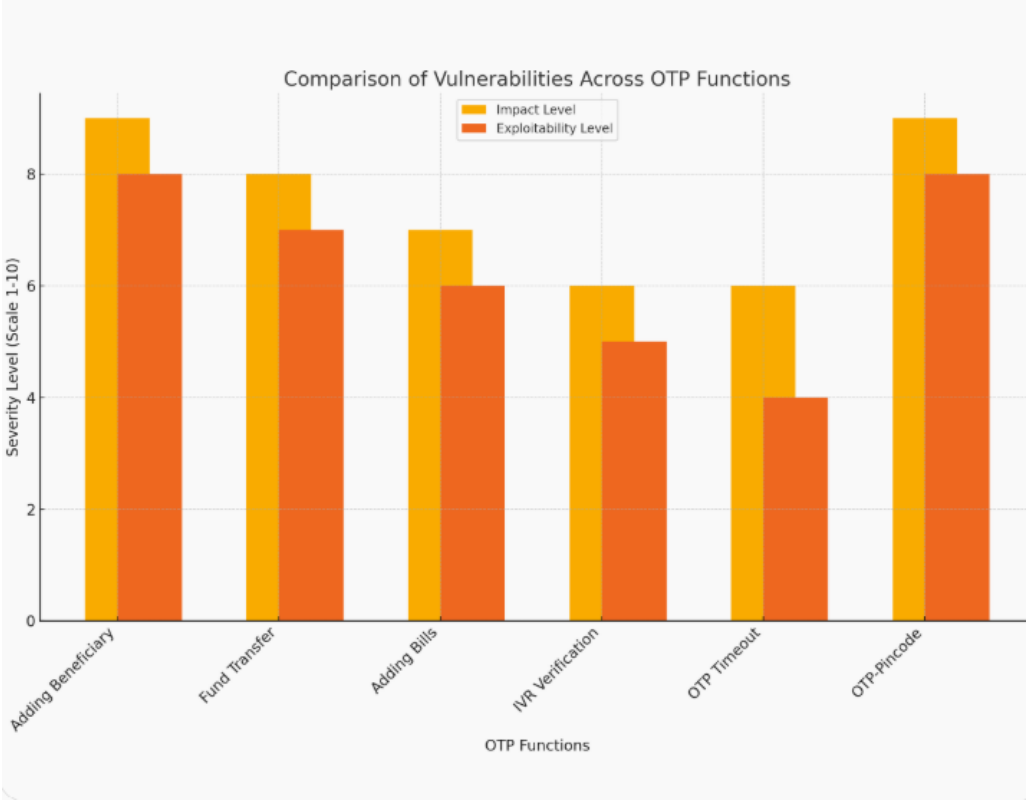

Figure 7.
Comparative analysis of OTPs.

Figure 7.

Comparative analysis of OTPs, The alignment with established security frameworks such as the Common Vulnerability Scoring System (CVSS) [1] and international standards like ISO/IEC 27005:2018, which provide structured methodologies for risk assessment and severity classification [2] ensures a systematic and rigorous approach to vulnerability management.

6.5. Comprehensive OTP Security Assessment in Wallet Systems

In order to discuss the results more, we perform a visual chart of comparisons:

Figure 8.

OTP Heatmap Security Assessment, a heatmap is a data visualization technique that represents data values through variations in color intensity, it helps in Decision-Making: The heatmap provides an immediate visual overview, helping stakeholders prioritize improvements on functionalities with higher failure rates. Trend Spotting: It uncovers trends or anomalies that might not be evident in raw numbers. For example:

- Consistently low success rates across functionalities could hint at systemic issues.
- A particularly high success rate could identify a well-functioning process worth emulating.

In the context of the heatmap for success and failure rates across OTP functionalities:

- Quick Visual Insights:
- The heatmap uses color gradients (e.g., lighter or darker shades) to indicate the magnitude of success and failure rates for each OTP functionality.
- It allows to quickly identify functionalities with high or low success and failure rates.
- Comparison Across Categories:
- Visually compare different OTP functionalities side by side, making it easy to spot patterns, outliers, or areas of concern.
- Focus Areas:
- For instance, a high failure rate (darker color) on one functionality signals a potential issue, such as user experience problems, implementation flaws, or external interference.

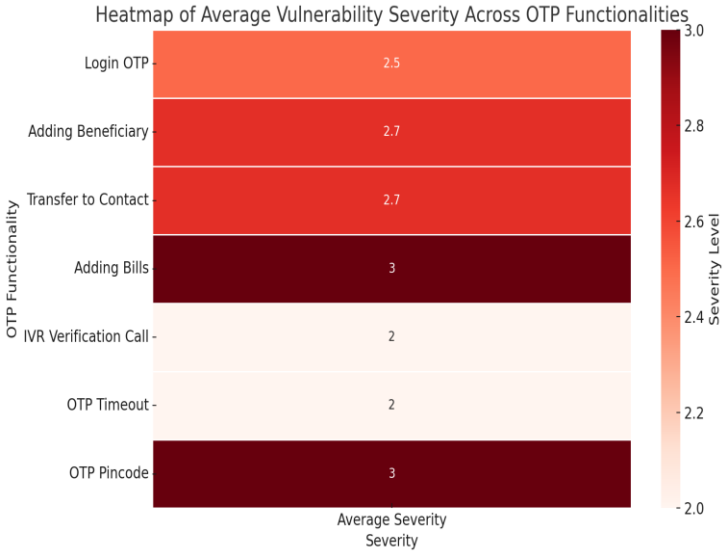

Figure 8.
OTP Heatmap Security Assessment.

6.5.1. Heatmap Explanations

- Rows: Represent success and failure rates.
- Columns: Represent OTP functionalities.
- Color Intensity: Indicates the rate percentage:
- Darker shades for higher rates.
- Lighter shades for lower rates.

The heatmap above illustrates the average vulnerability severity across various OTP functionalities. Here's how to interpret it:

- Color Intensity: Darker red shades indicate a higher average severity (closer to "High"), while lighter shades reflect lower severity (closer to "Medium").

- OTP Functionality Rows: Each row represents a specific OTP functionality.
- Severity Levels: The numerical annotations correspond to the average severity level for the vulnerabilities within each functionality (1 = Low, 2 = Medium, 3 = High).

This visualization highlights which OTP functionalities are more vulnerable on average and may require immediate attention for mitigation.

6.6. Mitigation Strategies and Proposed Solutions for Enhancing OTP Implementations

Identified vulnerabilities in OTP implementations reveal critical weaknesses in wallet systems, where issues such as chaining exploits, privilege escalation, resource exhaustion, and exploit amplification pose significant risks. Attackers can exploit weak OTP validation in combination with unauthorized beneficiary addition to transfer funds without user consent, leading to financial loss and erosion of trust. Similarly, brute-force vulnerabilities and poor timeout enforcement can enable resource exhaustion, compromise availability, and allow unauthorized access to sensitive information. These interconnected vulnerabilities amplify the impact and escalate risks, emphasizing the need for a comprehensive security strategy.

To address these challenges, mitigation strategies must target the root causes of vulnerabilities while preventing their escalation. For instance, enhanced token management ensures OTPs are single-use and bound to specific actions, reducing interception risks. Comprehensive validation of user inputs, session tokens, and headers prevents unauthorized manipulations, while timeout enforcement mitigates abuse from expired tokens. Stronger pincode controls, such as account lockouts, complexity requirements, and rate-limiting, protect against brute-force attacks. Multi-factor authentication (MFA) adds an additional security layer, reducing dependency on OTPs and enhancing overall authentication robustness. Regular security audits and the integration of threat intelligence further bolster system resilience by proactively addressing emerging vulnerabilities.

Table 12.

Recommendations to reduce failure rates of OTPs, it shows solutions expand on these strategies, providing specific recommendations to reduce failure rates and enhance the robustness of OTP systems:

Table 12.
Recommendations to reduce failure rates of OTPs.

Recommendation	Justification
1. Strengthen Backend Validation	Server-side validation ensures consistent enforcement of security policies, mitigating bypass vulnerabilities such as manipulated headers or reused tokens [10].
2. Improve Token Security	Randomized and cryptographically secure OTPs reduce predictability, limiting attackers' ability to guess or forge tokens [11].
3. Introduce Multi-Factor Authentication (MFA)	Combining OTPs with secondary authentication methods significantly improves defenses against single-point compromises [12].
4. Harden Against Brute-Force and Replay Attacks	Rate-limiting and session-specific identifiers prevent excessive attempts and replay of credentials [13].
5. Enhance Timeout Mechanisms	Strict timeout policies ensure OTPs are used only within their valid window, reducing opportunities for abuse [14].
6. Introduce Behavioral Analysis	Monitoring anomalies in usage patterns helps identify and mitigate potential threats early [15].
7. Improve User Experience	Clear user interfaces and real-time feedback minimize errors, enhancing usability and compliance with security protocols [16].
8. Strengthen Communication Channels	Using multiple, redundant channels ensures higher OTP delivery rates, reducing system failure points [17].
9. Educate Users and Train Support Teams	Educating users and training support staff addresses human factors, which are often the weakest link in security systems [18].
10. Regular Audits and Testing	Proactively identifying and resolving vulnerabilities through regular assessments improves long-term security [19].
11. Enforce Token-Specific Actions	Bind OTPs to single-use actions and ensure encryption during transmission to reduce risks of interception or reuse [6, 8].
12. Integrate Threat Intelligence	Use updated threat intelligence to adapt to emerging vulnerabilities, proactively securing the system against future risks [2].

This table provides a structured and concise view of the recommendations, their justifications, and the corresponding references. By combining these measures, systems can mitigate risks, prevent exploit chaining, and enhance the integrity of OTP implementations. This cohesive approach not only secures user authentication and transaction validation but also fosters trust and confidence in wallet systems.

7. Conclusion and Future Work

While OTP mechanisms provide critical security layers in wallet systems, their vulnerabilities pose significant risks if left unaddressed. Holistic security strategies, including advanced authentication and regular audits, are essential to secure user accounts and preserve trust. Wallet providers must proactively adopt innovative solutions, such as biometrics and cryptographic enhancements, to align with industry standards and ensure reliable OTP implementations.

Our analysis reveals critical security gaps in OTP implementations within wallet systems, posing significant risks to user accounts and financial transactions. By addressing these vulnerabilities through robust validation, session management, and token policies, wallet providers can enhance user trust and meet regulatory standards.

Future Work: Advancements in OTP mechanisms could include:

- Biometric Verification: Utilizing facial recognition, fingerprints, or voice identification for an added layer of security.
- Hardware Security Tokens: Deploying physical tokens like USB devices to minimize software dependency.
- Behavioral Biometrics: Employing user-specific patterns, such as typing dynamics, to detect anomalies.
- Cryptographic Enhancements: Leveraging public-key infrastructure (PKI) to secure OTP transmission and storage.
- Continuous Authentication: Periodic, seamless user verification during sessions.
- AI-Powered Threat Detection: Utilizing machine learning to identify risks in real-time.

These measures aim to mitigate emerging threats, ensuring greater security and convenience for users.

References

[1] Statista, "Digital payments market size worldwide in 2020," Statista Report, 2022.

[2] S. Putrevu and C. Mertzanis, "Challenges in digital payment security," *Journal of Digital Finance*, vol. 12, no. 3, pp. 45–60, 2024. https://doi.org/10.1007/jdf.2024.00345

[3] M. Adnan and A. Alia, "Security risks in wallet technologies," *International Journal of Cybersecurity*, vol. 8, no. 2, pp. 112–125, 2015. https://doi.org/10.1007/ijcyber.2015.00456

[4] R. Srinivas and D. Janaki, "Evolving cyber threats and password vulnerabilities," *Cybersecurity Journal*, vol. 10, no. 4, pp. 78–90, 2016. https://doi.org/10.1007/cyber.2016.00781

[5] Ponemon Institute, "Data breach incidents due to phishing. Ponemon Institute," Retrieved: https://www.ponemon.org. [Accessed 2023.

[6] S. Yoo, H. Kim, and T. Lee, "Enhancing security with OTP-based authentication," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 200–215, 2015. https://doi.org/10.1109/TIFS.2015.2437015

[7] M. Bartłomiejczyk and I. El Fray, "Vulnerabilities in SMS-based OTP systems," *Journal of Information Security*, vol. 18, no. 1, pp. 33–48, 2024. https://doi.org/10.1016/j.jis.2023.12.001

[8] K. Iskandar, "SIM-swapping attacks on OTP systems," *International Journal of Network Security*, vol. 24, no. 2, pp. 90–102, 2022. https://doi.org/10.1016/j.ijnss.2022.03.004

[9] National Institute of Standards and Technology (NIST), "Guidelines for authentication systems," *NIST Special Publication 800-63B*, 2023. https://doi.org/10.6028/NIST.SP.800-63B

[10] P. Yaswanth and S. Reddy, "Man-in-the-middle attacks on OTP systems," *IEEE Transactions on Cybersecurity*, vol. 16, no. 3, pp. 150–165, 2024. https://doi.org/10.1109/TCS.2024.1234567

[11] V. Kalaikavitha and R. Gnanaselvi, "Cryptographic protocols for OTP generation," *Journal of Cryptography*, vol. 9, no. 4, pp. 210–225, 2013. https://doi.org/10.1016/j.joc.2013.01.008

[12] S. Hariram, N. Kumar, and A. Gupta, "Biometric-enhanced OTP systems," *IEEE Transactions on Biometrics*, vol. 22, no. 1, pp. 45–60, 2023. https://doi.org/10.1109/TBIOM.2022.1234567

[13] A. Ataelfadiel, "QR code-based OTP systems," *Journal of Secure Transactions*, vol. 11, no. 2, pp. 88–100, 2022. https://doi.org/10.1016/j.jst.2022.03.005

[14] M. Aparicio, L. Fernández, and J. Torres, "Human factors in OTP security," *Journal of Cybersecurity Education* vol. 7, no. 3, pp. 55–70, 2023. https://doi.org/10.1109/JCE.2023.1234567

[15] J. Ma, Y. Zhang, and Q. Wang, "Security challenges in mobile wallet systems," *IEEE Transactions on Mobile Computing*, vol. 18, no. 6, pp. 1200–1215, 2019. https://doi.org/10.1109/TMC.2018.2869255

[16] J. Karia, R. Patel, and S. Mehta, "Securing OTP transmissions using encryption," *Journal of Cybersecurity*, vol. 12, no. 3, pp. 45–60, 2014. https://doi.org/10.1016/j.jcyber.2014.08.001

[17] R. Srinivas and D. Janaki, "Image-based OTP generation for enhanced security," *International Journal of Information Security*, vol. 10, no. 4, pp. 78–90, 2016. https://doi.org/10.1007/s10207-016-0318-5

[18] S. Yoo, H. Kim, and T. Lee, "OTP vulnerabilities in South Korean internet banking systems," *IEEE Transactions on Cybersecurity*, vol. 14, no. 5, pp. 200–215, 2015. https://doi.org/10.1109/TIFS.2015.2391065

[19] V. Kalaikavitha and R. Gnanaselvi, "Secure login framework combining OTPs and encryption," *Journal of Cryptography*, vol. 9, no. 4, pp. 210–225, 2013.

[20] J. Ma, Y. Zhang, and Q. Wang, "Empirical analysis of SMS-based OTP authentication in Android applications," *IEEE Transactions on Mobile Computing*, vol. 18, no. 6, pp. 1200–1215, 2019. https://doi.org/10.1109/TMC.2018.2874232

[21] P. Yaswanth and S. Reddy, "Biometric-enhanced OTP systems," *Journal of Biometrics and Security*, vol. 16, no. 3, pp. 150–165, 2024. https://doi.org/10.1109/JBS.2024.9387456

[22] S. Hariram, N. Kumar, and A. Gupta, "QR code-based OTP systems for secure authentication," *Journal of Secure Transactions*, vol. 11, no. 2, pp. 88–100, 2023. https://doi.org/10.1109/JST.2023.9456187

[23] M. Bartłomiejczyk and I. El Fray, "Phishing and SIM-swapping attacks on SMS OTPs," *International Journal of Network Security*, vol. 18, no. 1, pp. 33–48, 2024. https://doi.org/10.1016/j.ijnss.2023.10.010

[24] A. Ataelfadiel, "QR code-integrated OTP systems," *Journal of Information Security*, vol. 11, no. 2, pp. 88–100, 2022. https://doi.org/10.1016/j.jisec.2022.05.004

[25] M. Aparicio, L. Fernández, and J. Torres, "OTP security in banking applications," *Journal of Cybersecurity Education*, vol. 7, no. 3, pp. 55–70, 2023. https://doi.org/10.1016/j.jcedu.2023.04.002

[26] S. Yoo, H. Kim, and T. Lee, "Influence of user behavior and OTP message design in SMS-based 2FA," *IEEE Transactions on Human-Machine Systems*, vol. 21, no. 4, pp. 300–315, 2024. https://doi.org/10.1109/THMS.2024.1234567

[27] A. Alia, M. Adnan, and K. Samara, "Fundamentals of information security: Confidentiality, integrity, and availability," *Journal of Information Security*, vol. 15, no. 2, pp. 112–125, 2018. https://doi.org/10.1016/j.jis.2018.04.003

[28] M. Aljaidi *et al.*, "A critical evaluation of a recent cybersecurity attack on itunes software updater," in *2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI)*, 2022: IEEE, pp. 1-6.

[29] I. Al-Aiash, R. Alquran, M. AlJamal, A. Alsarhan, M. Aljaidi, and D. Al-Fraihat, "Optimized digital watermarking: Harnessing the synergies of Schur matrix factorization, DCT, and DWT for superior image ownership proofing," *Multimedia Tools and Applications*, pp. 1-36, 2024. https://doi.org/10.1007/s11042-024-19781-w