WHITEPAPER — MAY 2024

CyberPlural MSSP

Whitepaper: Enhancing Cybersecurity in the FinTech Ecosystem

Testing a Mock Fintech App Designed to Replicate Common Vulnerabilities

By simulating these vulnerabilities in a controlled environment, we aim to provide valuable insights and learning opportunities for fintech organizations to strengthen their security posture.

As part of our ongoing efforts to enhance cybersecurity operations and preparedness within the fintech industry, our team tested a mock fintech application designed to replicate common vulnerabilities discovered during security assessments of real-world fintech platforms. By simulating these vulnerabilities in a controlled environment, we aim to provide valuable insights and learning opportunities for fintech organizations to strengthen their security posture.

In the preparation to putting together this mock fintech application, our team carefully considered some of the external factors that can influence the security of such platforms in real-time. The fintech industry is often characterized by aggressive timelines, with development teams under constant pressure to meet deadlines and release new features. This, in turn, can lead to security considerations being overlooked or given limited attention.

It is not uncommon for fintech organizations to rush the development process, prioritizing speed-to-market over comprehensive security assessments. This dynamic can result in the security team being afforded limited time to thoroughly evaluate the application's security posture, leading to the introduction of vulnerabilities that malicious actors can easily exploit.

Furthermore, the continuous deployment of changes and new features to fintech platforms, even when they are already in production, is another factor that can contribute to security misconfigurations and changes in the business workflow. Attackers have demonstrated their ability to capitalize on these dynamic environments, quickly identifying and exploiting vulnerabilities introduced by hastily implemented updates.

CONTRIBUTION

Hamzah Lateef

Emmanuel Akobe-Ajibolu

Abdulrahman Oyekunle

Findings from Mock Fintech Application Security Assessment

The vulnerabilities discovered in the mock fintech application highlight the importance of prioritizing API security and conducting thorough security assessments within the fintech industry. These findings mirror the real-world challenges faced by many fintech organizations, underscoring the need for a proactive, comprehensive approach to identifying and addressing security weaknesses.

Forgot Password Functionality Vulnerability - CWE-640, CWE-209, T1033

The mock fintech application's forgot password functionality exhibited a vulnerability that could enable user enumeration. When a non-existent username was submitted, the application returned an error message stating "User not found," effectively disclosing the existence of a user account. This weakness could be exploited by attackers to conduct password spraying attacks, potentially leading to account takeovers, especially if the application had a weak password policy in place.

Unrestricted User Data Dumping Endpoint - T1087

During the assessment, our team discovered an API endpoint that allowed for the retrieval of all registered users on the platform, including their UserIDs and other personally identifiable information (PII). Alarmingly, this endpoint had no access restrictions in place, granting unrestricted access to sensitive user data. This vulnerability exposes fintech organizations and their customers to significant risks, such as identity theft, phishing attacks, and other malicious activities targeting the exposed PII.

Failed Authorization and User Impersonation - CWE-285, CWE-287, T1656

The mock application's authentication mechanism was found to have a severe authorization vulnerability. Although users were assigned bearer tokens upon login, the application relied solely on UserID tracking for user sessions, rather than effectively utilizing the bearer tokens for authorization. This critical flaw enabled user impersonation, allowing both authenticated and non-authenticated users to perform actions on behalf of any other user without proper authorization checks.

Exploiting this vulnerability, our team was able to impersonate legitimate users and carry out unauthorized actions, such as initiating payments, transferring funds, and updating user details, without being subject to proper authorization verification. The absence of rate limiting on the PIN endpoint further exacerbated the potential impact, as it allowed for brute-force attacks to obtain the user's PIN, granting the attacker unrestricted access to the user's account and financial transactions.

CWE-640
Weak Password Recovery Mechanism for Forgotten Password

CWE-209
Generation of Error Message Containing Sensitive Information

CWE-285
Improper Authorization

CWE-287
Improper Authentication

CWE-778
Insufficient Logging

T1033
System Owner/User Discovery

T1111
Multi-Factor Authentication Interception

T1656
Impersonation

https://cwe.mitre.org/top25/

Race Condition Vulnerability in Transaction Processing - CWE 362

During our assessment, we identified a race condition vulnerability in the mock application's transaction processing logic. This vulnerability could be exploited to bypass the intended transaction limits and authorization checks. By carefully timing concurrent requests, an attacker could initiate multiple transactions in rapid succession, effectively overriding the application's security controls and transferring funds without proper authorization.

This race condition vulnerability highlights the importance of implementing robust concurrency control mechanisms and thoroughly testing fintech applications for race conditions, which can be difficult to detect and exploit but can have severe consequences if left unaddressed.

Excessive JWT Validity and Weak Secret Key - T1134

Further analysis of the application's session management revealed critical security flaws in the handling of JSON Web Tokens (JWT). The JWT issued to users had an excessively long lifespan, exceeding a month, and the generation of a new token did not invalidate the previous one. This excessive validity period provided attackers with prolonged access to compromised user accounts, even if the user changed their password or other credentials.

Moreover, the secret key used to secure the JWT was discovered to be weak, allowing our team to break the key using readily available tools. By decoding the JWT payload, we gained access to sensitive user information, including UserIDs, and were able to leverage this compromise to gain system-wide access and impersonate any user within the platform.

The mock fintech application tested was designed to replicate these real-world challenges, ensuring that the vulnerabilities uncovered reflect the practical challenges faced by fintech organizations in the face of tight deadlines, limited security resources, and the constant pressure to innovate and deploy new features.

The forgot password functionality vulnerability, the unrestricted user data dumping endpoint, and the authorization bypass issues discovered in the mock application are all too common in the fintech sector. These weaknesses are often the result of rushed development cycles, where security assessments are deprioritized, and the focus remains on meeting aggressive timelines and feature release schedules.

Similarly, the race condition vulnerability identified in the transaction processing logic highlights the inherent complexity of fintech applications and the need for meticulous security testing, even in the face of constant updates and changes. Attackers have demonstrated their ability to exploit such vulnerabilities, often by carefully timing their attacks to bypass intended security controls.

The excessive JWT validity and the use of a weak secret key in the mock application's session management further underscores the importance of proactive security measures, even in areas that may be considered "secondary" to the core functionality of the fintech platform. These vulnerabilities can have far-reaching consequences, enabling system-wide compromise and the impersonation of legitimate users.

T1134
Access Token Manipulation

CWE-362, 366, 367 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

CWE-691 Insufficient Control Flow Management

meeting aggressive timelines and feature release schedules.

limited security resources and deprioritized security assessment

rushed development cycles introducing misconfigurations

continuous deployment of changes and new features to fintech platforms.

The Imperative of API Security in the Fintech Sector: Lessons from a Mock Fintech Application

The security assessment of the mock fintech application tested by our team has shed light on the critical importance of API security in the ever-evolving fintech landscape. The vulnerabilities uncovered in this controlled environment mirror the real-world challenges faced by many fintech organizations, underscoring the urgent need for a proactive approach to addressing API-related security risks.

Throughout the assessment, the majority of the identified vulnerabilities were directly linked to misconfigurations, design flaws, and insufficient testing of the application's API infrastructure. From the **forgotten password functionality vulnerability** that enabled user enumeration to the unrestricted user data dumping endpoint that exposed sensitive PII, these findings highlight the pervasive nature of API security weaknesses in the fintech sector.

The mock application's authentication mechanism also exhibited a **severe authorization vulnerability**, allowing user impersonation and the execution of unauthorized actions, such as fund transfers and account updates, without proper verification. This type of vulnerability can have devastating consequences, compromising the trust and financial security of fintech customers.

Moreover, the discovery of a **race condition vulnerability** in the transaction processing logic exemplifies the complex security challenges inherent in fintech applications. Such vulnerabilities, if left unaddressed, can enable attackers to bypass intended security controls and execute fraudulent transactions, posing a grave threat to the financial integrity of the platform and its users.

The assessment also uncovered **flaws in the application's session management,** including the excessive validity of JWT tokens and the use of a weak secret key. These weaknesses granted our team prolonged access to compromised user accounts and the ability to impersonate any user within the platform, further underscoring the criticality of robust API security measures.

As the fintech sector continues to evolve, APIs have become the backbone of many fintech applications, serving as the primary interface for both legitimate users and malicious actors. Neglecting the security of these APIs can have **severe consequences**, exposing fintech organizations and their customers to a wide range of threats, including data breaches, financial fraud, and identity theft.

severe authorization vulnerability

race condition vulnerability

flaws in the application's session management

Inherited vulnerability in 3rd party APIs being consumed.

Insecure Design

The findings from the mock fintech application assessment serve as a stark reminder that API security can no longer be an afterthought. Fintech companies must prioritize the security of their API infrastructure, implementing robust authentication and authorization mechanisms, ensuring proper input validation and error handling, and adhering to industry-standard security best practices.

Regular **penetration testing and security assessments**, such as the one conducted on the mock application, are crucial to identifying and remediating vulnerabilities before they can be exploited by cybercriminals. By addressing the API security gaps highlighted in this assessment, fintech organizations can enhance the overall security posture of their systems and better protect their customers' sensitive information and financial assets.

Investing in API security is **not just a matter of compliance**; it is a strategic imperative to maintain trust, reputation, and long-term sustainability in the rapidly evolving fintech landscape. As the industry continues to face incessant attacks, the lessons learned from the mock application assessment can serve as a valuable guide for fintech companies to strengthen their defenses and stay ahead of emerging threats.

Thank you!

Thank you for taking the time to read this Whitepaper. If you have any questions or would like to discuss how CyberPlural MSSP can be of service to you, please don't hesitate to reach out to us.

8, P.O. W Mafemi Crescent, Abuja

+234 70 1470 2005

hello@cyberplural.com

cyberplural.com.com