

BLOCKCHAIN CASE STUDY

Industry
Blockchain

Client Background

The company is one of India's leading cryptocurrency wallet providers, with over 10,000 daily transactions. They have over 200,000 registered users and process digital currency transactions worth over \$30 million.

Environment

- Over 2,00,000 Plus Registered users
- Operates around 57 countries
- 10,000 Plus transactions in a day

Business Challenges

- Perform the test in a live environment during peak cryptocurrency transaction times.
- Preventing the misuse and public disclosure of user data.
- Keeping the app from being hacked by cryptocurrency criminals.

Solution

The organization approached Kratikal's security testing department to identify any technical or logical flaws in its clients' e-wallets. To get recommendations on how to mitigate the dangers of exploiting those vulnerabilities.

Approach

- The test was carried out in a dummy environment.
- The test was conducted as a Grey Box exercise.
- Various hacks were attempted to test their web and mobile application.
- The tests were conducted in accordance with the best practices available in the industry, such as Open Web Application Security Project (OWASP), SANS 25, NIST and more.



Major Findings

- It was revealed that the settings relating to "add value" into wallet may be changed, allowing an attacker to add up to \$5000 per transaction by simply subtracting \$1.
- Brute force attacks were possible with two-factor authentication via email or SMS.
- Some configuration files containing sensitive information were exposed to the public.



Risks

- Because the wallet amount parameters may be modified with, attackers might add as much money as a cryptocurrency wallet.
- The server could be hijacked if sensitive information is leaked.
- A hacker might take over user's accounts and transfer all their cryptocurrency to his own wallet. Millions of dollars could be lost because of this.
- They might use two-factor authentication to obtain access to their accounts.



Impact

- By changing the pricing parameter, it was possible to buy currencies for free, resulting in daily losses of approximately \$ 1.2 million.
- The firm could face large financial losses, potential lawsuits, and a damage to their brand image if their application's accounts are hacked.
- If sensitive client information regarding their clients and users is leaked from their application, they may be subject to large fines under various compliances and local Cyber laws in the countries where they work.
- E Hijacking of their app's accounts could result in a full loss of funds in their consumers' wallets.

Recommendations

- To address the issue of parameter tampering, we recommended to the company that parameters be checked at the server and the server's response matched the request received by the application.
- We recommended significant changes to the architecture and authentication mechanism of the application.
- For database security and server design, we advised the company on advanced controls and cryptographic techniques (such as obfuscation techniques).
- We recommended that they change their application processes to avoid wallet leaks and account takeovers.
- Detailed documentation of the application's vulnerabilities was provided, outlining the problem, its cause, and how to fix it.

"With cryptocurrency wallets being hacked left and right, we enlisted Kratikal's help to assess our application's security. Our team had a wake-up call because of their results. We have been operating cryptocurrency e-wallets and exchanges for a long time and were unaware of any issues with our platform. We appreciate the team's efforts and will continue to collaborate with them. "

- CTO, Cryptocurrency Wallet


Kratikal Privacy Commitment

Kratikal is dedicated to safeguarding your company from modern dangers, such as data leakage. For this reason, we do not reveal the names of our case study participants.

 +91 9289192210

 sales@kratikal.com

 www.kratikal.com

 A-130, 2nd Floor, Sector 63, Noida,
Uttar Pradesh, India-201301