Vulnerability Report on Coinhako website.

by

Saloni Ghule
Kreet Rout
Shreya Singh
Nitin Kumar

Weve tried exploiting SQL injections, XXS, IDOR, DoS and DDos, but none worked, the below vulnerability is the only one that seems to be a threat.

Description:

Allowing sign-up with temporary disposable email IDs on coinhako website introduces a significant security risk. Temporary email services tool Tempail, provide users with easily accessible and discardable email addresses, making it difficult for the platform to track and verify the identity of users effectively. This can lead to various malicious activities, including but not limited to fraudulent account creation, money laundering, and unauthorized access to user accounts.

Impact on Business:

1. *Increased Risk of Fraud:* Allowing the use of disposable email addresses significantly increases the risk of fraudulent user registrations. This can lead to an increase in fraudulent transactions, loss of funds, and damage to the platform's reputation.

2. *Reduced KYC Effectiveness:* Crypto trading platforms are often required to perform Know Your Customer (KYC) checks to comply with legal and regulatory requirements. Allowing disposable email sign-ups can undermine the effectiveness of these checks, potentially exposing the platform to legal and compliance issues.

3. *Loss of Trust*: Users may lose trust in the platform if they perceive it as lacking stringent security measures. This loss of trust can lead to a decrease in user engagement and may discourage potential investors from using the platform.

4. *Data Breach Risk:* Disposable email accounts can be used to hide malicious intent, making it easier for attackers to exploit vulnerabilities and gain unauthorized access to user accounts. This increases the risk of data breaches and theft of sensitive user information.

CWE:

This vulnerability can be associated with multiple Common Weakness Enumeration (CWE) identifiers. Some relevant CWEs might include:

- CWE-799: Improper Control of Interaction Frequency: Allowing disposable email sign-ups may result in improper control of user interactions and identity verification.

- CWE-601: URL Redirection to Untrusted Site ('Open Redirect'): Attackers could use disposable email addresses to perform phishing attacks or redirect users to malicious sites.

CVE:

A specific CVE identifier may not be applicable to this issue, as it is more of a general security concern rather than a specific software vulnerability. However, a crypto trading platform's security team should address this issue as part of their security improvements.

Recommended Mitigation:

To mitigate this vulnerability, the crypto trading platform should implement the following measures:

1. Filtering based on known email companies : On the Server Side the developers may include a List of mailing service providers and validate the mail field fed by the user.

2. Enhanced KYC: Implement a robust Know Your Customer (KYC) process to ensure that users are who they claim to be, reducing the risk of fraudulent activities.

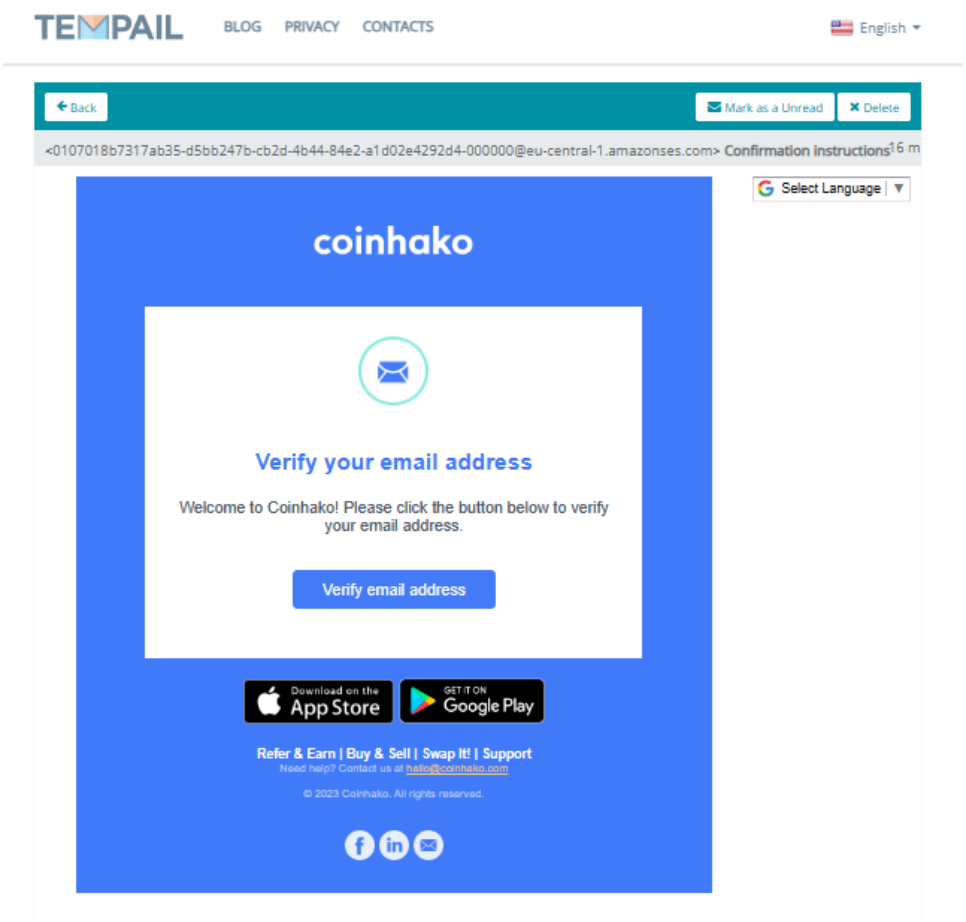
3. Monitoring and Reporting: Implement real-time monitoring for suspicious activities and implement a reporting mechanism for users to report potential fraud or suspicious behavior.

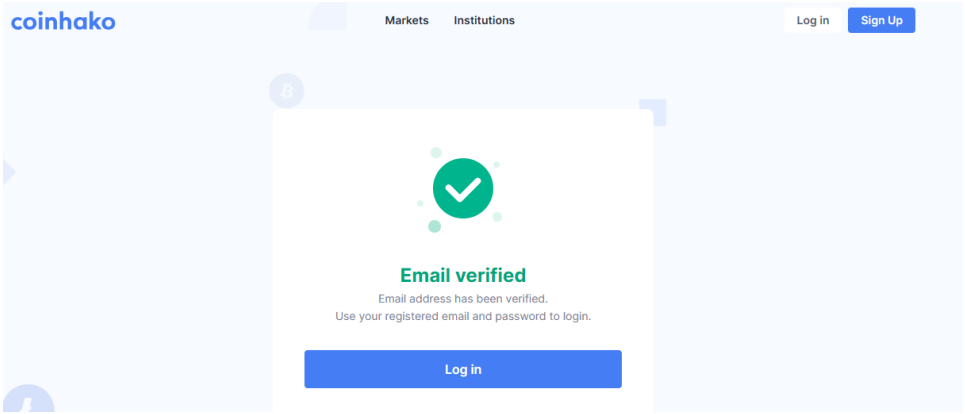
4. Account Lockout: Implement temporary account lockout for users whose activities appear suspicious. This can help prevent unauthorized access and fraud.

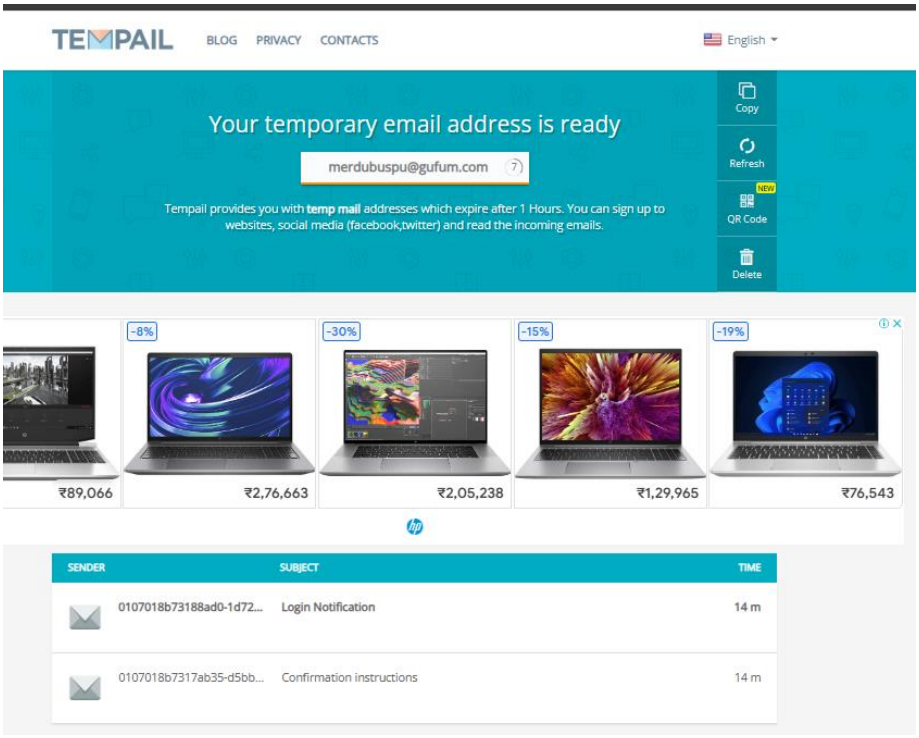
Conclusion:

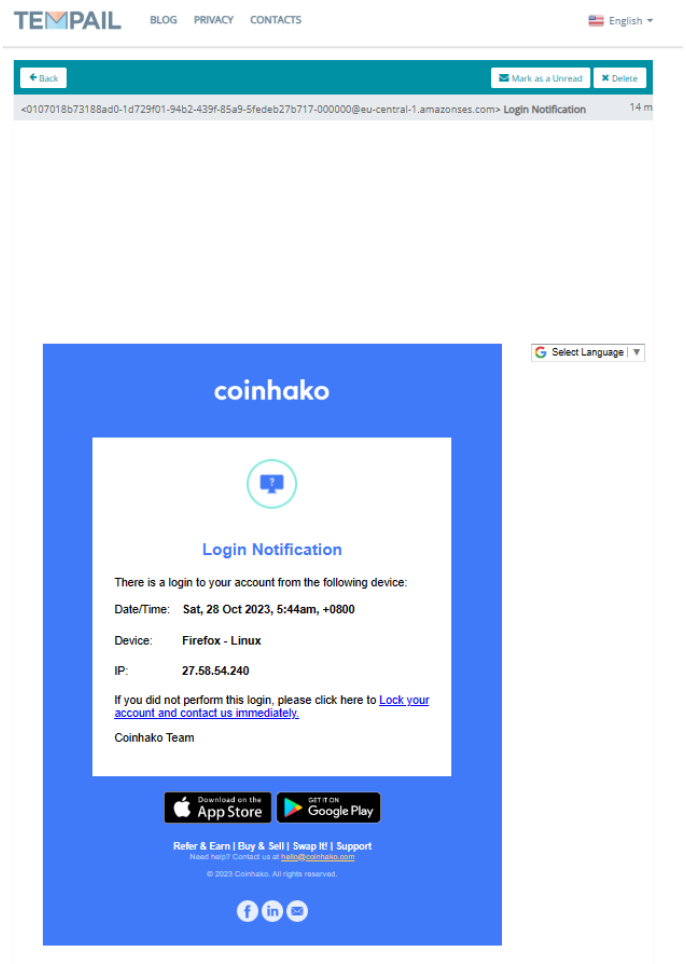
Allowing sign-up with temporary disposable email addresses on a crypto trading website poses a significant security risk to the platform. Implementing the recommended mitigation measures will help enhance security, protect user accounts, and maintain compliance with regulatory requirements.

Proof of Concept:




coinhako
Markets
Institutions
Log in
Sign Up
Email verified
Email address has been verified.
Use your registered email and password to login.
Log in


TEMPAIL
BLOG
PRIVACY
CONTACTS
English
Your temporary email address is ready
merdubuspu@gufum.com
Tempail provides you with temp mail addresses which expire after 1 Hours. You can sign up to websites, social media (facebook,twitter) and read the incoming emails.
Copy
Refresh
NEW
QR Code
Delete
-8%
-30%
-15%
-19%
₹89,066
₹2,76,663
₹2,05,238
₹1,29,965
₹76,543
SENDER
SUBJECT
TIME
0107018b73188ad0-1d72...
Login Notification
14 m
0107018b7317ab35-d5bb...
Confirmation instructions
14 m


TEMPAIL
BLOG
PRIVACY
CONTACTS
English
Back
Mark as a Unread
Delete
<0107018b73188ad0-1d729f01-94b2-439f-85a9-5fedeb27b717-000000@eu-central-1.amazonses.com> Login Notification
14 m
Select Language
coinhako
Login Notification
There is a login to your account from the following device:
Date/Time: Sat, 28 Oct 2023, 5:44am, +0800
Device: Firefox - Linux
IP: 27.58.54.240
If you did not perform this login, please click here to Lock your account and contact us immediately.
Coinhako Team
Download on the App Store
GET IT ON Google Play
Refer & Earn | Buy & Sell | Swap It! | Support
Need help? Contact us at hello@coinhako.com
© 2023 Coinhako. All rights reserved.