Paisabazaar Marketing and Consulting Private Limited
Bug Bounty Guidelines
Version 2.0

Document Control

Type of Information	Document Data
Document Title	Paisabazaar Bug Bounty Guidelines
Document Code	Paisabazaar - BBG-V2.0
Date of Release	11 November 2025
Document Version No.	2.0
Document Owner	Information Security Team
Document Author(s)	Information Security Team
Document Approver	CISO
Security Classification	Public
Document Status	Final

Document Revision History

Ver. No.	Date	Change Description	Author	Approved By
1.0	15.05.2025	Initial release	Information Security Team	CTO
2.0	25.11.2025	Annual Document Review *pensionbazaar.com has been added to the scope Modifications made in “out of scope” section	Information Security Team	CISO

Contents

1. Introduction

Keeping customer information safe and secure is of utmost priority and a core company value for us at Paisabazaar Marketing and Consulting Private Limited ("Paisabazaar"). Paisabazaar welcomes the contribution of external security researchers and looks forward to suitably awarding them for their valuable contribution in improving the security posture of Paisabazaar.

2. Eligibility and Responsible Disclosure

To promote the discovery and reporting of vulnerabilities and increase customer safety, any applicant(s) to Bug Bounty program ("Program") must adhere to the following guidelines:

- "Applicant" is a person ("external security researcher") who applies to Paisabazaar for registering under the Program and is provided such authorization, in writing, by Paisabazaar. The Applicant shall be required to submit the security vulnerability report to Paisabazaar.
- Disqualification conditions: Applicant cannot be

i. an employee of a contractor/vendor of Paisabazaar or its subsidiaries or affiliates;

ii. a contractor/vendor of Paisabazaar or its subsidiaries or affiliates;

iii. an immediate family member of a person employed by Paisabazaar or its subsidiaries or affiliates or group company (defined for these purposes as including spouse, domestic partner, parent, legal guardian, legal ward, child, and sibling, and each of their respective spouses, and individuals living in the same household as such individuals).

- Any person(s) who is NOT an Applicant is NOT eligible to participate in the Program. If such person(s) attempts to interfere, access, modify or control the IT infrastructure including servers, website, applications etc., the same shall be considered as unauthorized access and the Company may take appropriate action against such person(s) including Civil and Criminal legal action.
- The Applicant shall not interact with an individual account (which includes modifying or accessing data from the account) without the account owner's explicit consent in writing, which the applicant must produce upon request.
- The Applicant shall not cause privacy violations and disruptions to Paisabazaar or its Customers, including and not limited to unauthorized access or destruction of data, downloading sensitive and personal information of customers, and interruption or degradation of Paisabazaar services. The Applicant must not violate any applicable laws or regulations, including and not limited to any laws and regulations relating to personal information or sensitive personal information.
- If the Applicant inadvertently accesses any customer's data or any other Paisabazaar's data without authorization while investigating an issue, applicant must promptly cease the activity that might result in further access of the customer data or Paisabazaar data and immediately notify Paisabazaar about such information which was accessed

3. Bug Bounty program processes

Paisabazaar recognizes and rewards the Applicants who help Paisabazaar keep its customers safe by responsibly reporting security vulnerabilities in our domain (please refer In-Scope section). Monetary bounties for any Program reports are entirely at Paisabazaar's discretion, based on risk, impact, number of vulnerable users, and other factors. To be considered for a bounty, you must meet the following requirements:

- Adhere to the Eligibility and Responsible Disclosure guidelines specified above.
- Report a security issue/vulnerability: Identify a vulnerability in our applications which creates a security or privacy risk. Report the vulnerability upon discovery or as soon as is feasible.
- Report a security issue/vulnerability involving one of the products or services that are within the scope of the program. We specifically exclude certain types of potential security issues, listed under "Out of scope".
- Give Paisabazaar a reasonable time to respond to the issue.
- Before engaging in any action that may be inconsistent with or unaddressed by these guidelines, contact us for clarification by submitting a new query.
- Do not use automated scanners to scan our web applications as this would result in IP blacklisting and disqualification from bug bounty program.
- Comply with all applicable laws. In turn, we will follow these guidelines when evaluating reports under our bug bounty program.
- We investigate and respond to all valid reports. Due to the volume of reports that we receive, however, we prioritize evaluations based on risk and other factors, and it may take some time before you receive a reply.
- Closure confirmation shall be sought from applicant and validated by Paisabazaar's information security team before processing bounty amount (if any).
- We determine bounty amounts based on a variety of factors, including (but not limited to) impact, ease of exploitation and quality of the report.
- We reserve the right to publish reports (and accompanying updates).
- We verify that all bounty awards are permitted by applicable laws and paid only in compliance with applicable sanction compliance laws.

4. Submitting a security issue/vulnerability

An Applicant, before submitting a Program report on security issue/vulnerability to Paisabazaar, must read these guidelines and then send an email to infosec@paisabazaar.com, preferably with "Security Issue – External Security Researcher" in the subject line. Once the report has been received, our security team will investigate the issue(s). We will respond to you at the earliest with triage status of the issue and/or any additional requests for clarification. Due to the volume of reports that we receive, however, we prioritize evaluations based on risk and other factors, and it may take some time before you receive a reply. We'll try to keep you informed about our progress throughout the process.

5. In-Scope Vulnerabilities

Domain *.Paisabazaar.com.

Android: Play Store – Paisabazaar owned android applications

iOS: App Store – Paisabazaar owned iOS applications

- **Customer PII exposure/compromise through any vulnerability**
  - **Definition of PII:**
    - Customer Policy Document
    - Customer Full Name in combination with other PII (Date of birth, residential address, etc.)
    - Customer Phone Number
    - Customer Email ID
    - Any other customer document (KYC documents)

- **Employee's sensitive information exposure/compromise through any vulnerability**
  - **Details:**
    - Employee's Remuneration Details
    - Employee specific documents (salary slips, KYC documents, offer letter, health records, etc.)
- **Other valid issues**
  - Account takeover
  - Payment bypass issues
  - Subdomain takeover
  - Remote Code Execution
  - Local File Inclusion
  - Remote File Inclusion
  - Server-Side Request Forgery
  - IDOR (Insecure direct object reference)
  - SQL Injection

6. Out-of-Scope Vulnerabilities

- Any vulnerability not exposing/compromising customer PII
- Attack scenarios requiring control over victim's browser/cookies/tokens/machine
- DDoS/DoS and/or other availability attacks
- Social engineering attack scenarios
- HTTP security headers issues
- Lack of Secure and HTTP-Only cookie flag
- Clickjacking
- CORS (not exploited)
- Username enumeration
- Banner disclosure on common/public services
- Self XSS Open redirects with low security impact (exceptions are those cases where the impact is higher such as stealing oauth tokens)
- Login/logout CSRF
- Email issues related to SPF/DKIM/DMARC
- Formula Injection or CSV Injection
- Open ports without an accompanying proof-of-concept demonstrating vulnerability

7. Rewards

Rewards Eligibility

The reported vulnerability should showcase PII exposure or compromise, and the reporters will be rewarded based on the risk severity classified below. Triaging will be at the sole discretion of Paisabazaar and the decision of Paisabazaar in this context shall be final and binding:

Risk Severity	Critical	High
Reward Range	$500 - $1,000	$100 - $500

Report the vulnerability at **infosec@paisabazaar.com**

8. The Fine Print

Applicants are responsible for paying any statutory taxes associated with rewards. We may modify the terms of this program or terminate this program at any time. We will not apply any changes we make to these program terms retrospectively. Reports from individuals who we are not applicants or are prohibited by law are ineligible for rewards.

9. Summary

- The Applicant should responsibly disclose the identified security issue/vulnerability through our bug bounty program.
- Both identifying and non-identifying information can put an Applicant at risk. We limit what we share with third parties. We may provide non-identifying substantive information from your report to an affected third party, but only after notifying you. We will only share identifying information (name, email address, phone number, etc.) with a third party if you give your written permission.
- We may share your report or personally identifiable information without obtaining your prior consent in the following scenarios:
    - Only where it is requested or required by law or by any court or governmental agency or authority to disclose, or for the prevention, detection, investigation including cyber incidents, or for prosecution and punishment of offences; and

Note: Paisabazaar shall, in its sole and absolute discretion, determine whether to modify or change the terms of this document, including, without limitation, the form, structure and terms of the document or the timing of and conditions to the consummation of the document.