Responsible Disclosure Policy

KhataBookPay understands that the protection of customer data is a significant responsibility and requires the highest priority.
We value the assistance of security researchers and members of the security community in helping us keep our systems secure.
The responsible disclosure of security vulnerabilities helps us ensure the security and privacy of all our users.

Reporting a Vulnerability

If you have discovered a potential security vulnerability in any of our products or services that meets the criteria outlined below, please report it to us at **support@khatabookpay.com**.

- You can expect an acknowledgment from our security team within **24 hours** of submission.
- **KhataBookPay** will assess and define the severity of the issue based on its impact and ease of exploitation.
- We typically take **3 to 5 business days** to validate reported issues.
- Actions will be initiated promptly to remediate confirmed vulnerabilities in line with our commitment to security and privacy.
- We will notify you once the issue is resolved.

Responsible Testing Guidelines

While conducting security research:

- Do **not** violate our privacy policies, modify or delete unauthenticated user data, disrupt production systems, or degrade the user experience.
- Perform testing **only within the defined scope** below.
- Use the official reporting channel (**support@khatabookpay.com**) to disclose vulnerabilities.
- **Do not publicly disclose or publish** details of any vulnerability before it has been resolved and you have received written permission from KhataBookPay.
- Maintain **strict confidentiality** about all vulnerability information until notified that the issue has been fixed.

Reporting Guidelines

When submitting a report, please include:

- A clear **description and potential impact** of the vulnerability.
- A **detailed step-by-step guide** to reproduce the issue.
- (Optional) A **video Proof of Concept (PoC)**, if available.
- Your **preferred name or handle** for recognition in our *Security Researcher Hall of Fame.*

Domains in Scope

- **khatabookpay.com**

Qualifying Vulnerabilities

We welcome reports on the following types of issues:

- Remote Code Execution (RCE)
- SQL/XXE Injection and Command Injection
- Cross-Site Scripting (XSS)
- Server-Side Request Forgery (SSRF)
- Misconfiguration Issues (Servers / Applications)
- Authentication and Authorization Vulnerabilities
- Cross-Site Request Forgery (CSRF)

Non-Qualifying Vulnerabilities

The following types of issues are **not eligible** under this policy:

- HTML Injection and Self-XSS
- Host Header and Banner Grabbing Issues
- Automated Tool Scan Reports (e.g., Web, SSL/TLS, or Nmap scans)
- Missing HTTP Security Headers or Cookie Flags on Non-Sensitive Cookies
- Rate Limiting or Brute Force Attacks
- Login/Logout CSRF
- Session Timeout Issues
- Unrestricted File Uploads

- Open Redirects
- Formula/CSV Injection
- Denial of Service (DoS) / Distributed DoS (DDoS)
- Vulnerabilities requiring physical access to the victim's device
- Issues affecting outdated or unpatched browsers (more than two versions behind the latest stable release)
- User Enumeration (e.g., user email or ID disclosure)
- Phishing or Spam issues (including SPF/DKIM/DMARC configurations)
- Vulnerabilities found in third-party services
- EXIF Data not stripped from images

Found a Bug?

If you believe you've found a valid vulnerability, please reach out to:
support@khatabookpay.com

We appreciate your efforts in helping us maintain a secure ecosystem for all users.
