Responsible Disclosure Policy

KhataPayments understands that the protection of customer data is a significant responsibility and requires the highest priority.

We value the assistance of security researchers and any others in the security community to assist in keeping our systems secure.

The responsible disclosure of security vulnerabilities helps us ensure the security and privacy of all our users.

- Reach out to support@khatapayments.com, if you have found any potential vulnerability in our products that meet the criteria mentioned in the policy below.
- You can expect an acknowledgment from our security team within about 24 hours of submission.
- Khatapayments will define the severity of the issue based on the impact and ease of exploitation.
- We may take 3 to 5 days to validate the reported issue.
- Actions will be initiated to fix the vulnerability in accordance with our commitment to security and privacy. We will notify you when the issue is fixed.
- Security testing carried out should not violate our privacy policies, modify or delete unauthenticated user data, disrupt production servers, or degrade the user experience.
- Perform research only within the scope set out below.
- Use the identified communication channel, viz., support@khatapayments.com, to report the vulnerability information to us. Documenting or publishing the vulnerability details in the public domain is against our responsible disclosure policy and
- Keep information about any vulnerability confidential until the issue is resolved.

Reporting Guidelines

Please provide the following details on the report

- Description and potential impact of the vulnerability;
- A detailed description of the steps required to reproduce the vulnerability; and,
- Where available, a video POC.
- Your preferred name/handle for recognition in our Security Researcher Hall of Fame

Domains in Scope

- KhataPayments.com

Qualifying Bugs

- Remote code execution (RCE)
- SQL/XXE Injection and command injection
- Cross-Site Scripting (XSS)
- Server-side request forgery (SSRF)
- Misconfiguration issues on servers and application
- Authentication and Authorization related issues
- Cross-site request forgeries (CSRF)

Non-Qualified Bugs

- Html injection and Self-XSS
- Host header and banner-grabbing issues
- Automated tool scan reports. Example: Web, SSL/TLS scan, Nmap scan results, etc.
- Missing HTTP security headers and cookie flags on insensitive cookies
- Rate limiting, brute force attack.
- Login/logout CSRF
- Session timeout
- Unrestricted file upload
- Open redirections
- Formula/CSV Injection
- Denial of Service (DoS)/Distributed/ Denial of Service (DDoS)
- Vulnerabilities that require physical access to the victim machine.
- Vulnerabilities only affecting users of outdated or unpatched browsers *[Less than two stable versions behind the latest released stable version]*
- User enumeration such as User email, User ID, etc.
- Phishing / Spam (including issues related to SPF/DKIM/DMARC)
- Vulnerabilities found in third-party services.
- EXIF data not stripped on images.

Found a Bug

Reach out to support@khatapayments.com, if you have found any potential vulnerability