Grove Ventures Bug Bounty Policy

Introduction

At Grove Ventures, security is integral to maintaining trust with our partners, portfolio companies, and the broader ecosystem. As a venture capital firm committed to fostering innovation, we invite ethical security researchers to help us strengthen our systems by responsibly reporting vulnerabilities.

This Bug Bounty Program reflects our commitment to collaboration, transparency, and proactive security management.

Scope

In-Scope Systems:

- Websites: All pages and subdomains hosted under https://grovevc.com.
- Email Infrastructure: Security-related issues in Grove Ventures' email systems.

Out-of-Scope Systems:

- Third-party platforms or services not owned or managed by Grove Ventures.
- Social engineering attacks (e.g., phishing attempts targeting Grove employees).
- Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attacks.
- Physical security vulnerabilities.
- Automated reports without manual validation or actionable insights.

Eligibility

Participation is open to:

- Individuals aged 18 and above.
- Researchers not restricted by applicable laws or export regulations.

Exclusions:

- Grove Ventures employees, contractors, and their immediate family members. - Individuals using unethical or malicious testing methods.

Submission Process

To report a vulnerability:

1. Prepare Detailed Information:
   - Description of the issue and its security impact.
   - Step-by-step instructions to reproduce the vulnerability.
   - Screenshots, video evidence, or proof-of-concept code (if applicable).
2. Submit via Email:
   - Send your report to Contact@grovevc.com.
   - Use "[Bug Bounty Submission]" as the subject line.
3. Keep Findings Confidential:
   - Do not disclose or exploit vulnerabilities before Grove Ventures resolves them.

What You Can Expect:

- Acknowledgment of your submission within 3 business days.
- An initial assessment and status update within 10 business days.
- Resolution or mitigation updates within 30 days.

Severity Rating and Reward Structure

Reports will be categorized based on severity, impact, and reproducibility. Rewards correspond to the issue's significance and originality:

Severity	Description	Reward Range
Low	Minimal security risks, no significant user impact.	$50
Medium	Moderate vulnerabilities with limited data exposure or impact.	$75 - $125
High	Serious vulnerabilities affecting core functionality or data.	$125 - $250
Critical	Systemic vulnerabilities, major data exposure, or system control.	$750 - $1,500

Examples:

Critical: SQL injection enabling data theft.

High: Authentication bypass on sensitive systems.

Medium: Cross-Site Scripting (XSS) affecting user accounts. **Low**: Security headers missing in HTTP responses.

Rewards are determined at Grove Ventures' discretion and based on the quality of the report.

Response Timeline

Acknowledgment: Within 3 business days.

Initial Assessment: Completed within 10 business days.

Resolution Timeline: Mitigation or status updates shared within 30 days.

Reward Distribution: Issued within 10 business days after resolution confirmation.

Disclosure Policy

Responsible disclosure is critical to ensuring vulnerabilities are handled securely. Researchers must:

- Avoid exploiting vulnerabilities for any reason beyond proof-of-concept testing.
- Maintain confidentiality until Grove Ventures provides explicit approval for public disclosure. - Work collaboratively with Grove Ventures to validate and resolve issues.

Participants adhering to responsible disclosure will be recognized in Grove Ventures' Security Hall of Fame unless anonymity is requested.

Exclusions

Reports not eligible for rewards include:

- Findings outside the defined scope (e.g., vulnerabilities in third-party platforms).
- Denial-of-Service (DoS) or brute-force vulnerabilities.
- Vulnerabilities requiring physical access.
- Reports without sufficient detail, evidence, or reproducibility.

Legal Protections

Ethical researchers acting in good faith under this policy will not face legal repercussions. Grove Ventures commits to:

- Safe harbor for security research conducted responsibly within the program scope.
- Transparent communication regarding findings and their resolution.

Contact Information

For questions or to submit vulnerabilities:

- Email: Contact@grovevc.com
- Use “[Bug Bounty Submission]” in the subject line.

Policy Updates

This Bug Bounty Policy may be updated periodically to reflect changes in Grove Ventures' systems or practices. Updates will be posted on https://grovevc.com.

Acknowledgment

We thank the security research community for its valuable contributions to safeguarding Grove Ventures’ systems. Your efforts directly enhance our ability to operate securely and build trust with our partners.