Vulnerability Disclosure Policy

Moxie Partners, Inc.
Reviewed: April 18, 2025

Introduction

Moxie Partners, Inc. is committed to safeguarding the privacy and security of the medspas and entrepreneurs we serve. This Vulnerability Disclosure Policy (VDP) is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and for submitting discovered vulnerabilities to our security team.

This policy explains what systems and types of research are covered, how to report vulnerabilities, and our commitment to working with the security community to remediate issues in a timely manner.

We welcome and encourage responsible vulnerability research and appreciate contributions that help us keep our users and data secure.

Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized. We will work with you to understand and resolve the issue quickly, and Moxie will not pursue legal action related to your research.

If a third party initiates legal action against you for activities conducted in accordance with this policy, Moxie will make this authorization known to said third party upon your request.

Guidelines

Under this policy, “research” means activities in which you:

- Notify us as soon as possible after discovering a real or potential security issue.
- Avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Use exploits only to confirm the existence of a vulnerability, without accessing, exfiltrating, or persisting in the system.
- Provide us with a reasonable amount of time to resolve the issue before disclosing it publicly.
- Avoid submitting high volumes of low-quality or automated reports.
- Immediately stop testing, notify us, and do not disclose data if you discover sensitive information such as PII, PHI, or trade secrets.

Test Methods

The following test methods are not authorized:

- Denial of service (DoS or DDoS) attacks
- Social engineering (e.g., phishing, vishing), or physical intrusion
- Use of automated vulnerability scanners against production systems

Scope

This policy applies to:

- app.joinmoxie.com and all first-party subdomains under joinmoxie.com
- api.joinmoxie.com and admin.joinmoxie.com
- www.joinmoxie.com

Out of scope:

- Any systems or services not explicitly listed above (e.g., third-party vendors or tools)
- Staging, test, or sandbox environments not publicly accessible
- Third-party services Moxie uses but does not control

If you're unsure whether a system is in scope, contact us at security@joinmoxie.com before proceeding.

Moxie may expand the scope of this policy over time.

Reporting a Vulnerability

To report a vulnerability:

- - Email security@joinmoxie.com
- Anonymous submissions are permitted
- We recommend including:
    - A clear description of the vulnerability
    - The location (URL or system) affected
    - Potential impact
    - Steps to reproduce (screenshots or proof-of-concept code are welcome)

We will use your submission solely for defensive purposes, such as investigating and remediating the issue. We will not share your identity without permission.

Please note: Moxie does not currently offer a bug bounty program and decides monetary compensation on a case-by-case basis.

What to Expect from Us

If you provide contact information, we will:

- Acknowledge receipt of your report within 5 business days
- Keep you informed of progress toward remediation and decisions towards monetary compensation (note this includes the decision not to provide monetary compensation)
- Maintain an open dialogue for further questions or clarification

Questions

For any questions about this policy or to suggest improvements, contact us at: security@joinmoxie.com

Version 1.0 — April 18, 2025