Vulnerability Disclosure Policy

Introduction

This Vulnerability Disclosure Policy applies to any security vulnerabilities you may consider reporting to The JEllie Foundation (the “Organisation”). We encourage you to read this policy fully before submitting a report and to act in compliance with it.

We greatly value the effort of those who report security vulnerabilities. However, please note that we do not offer any monetary rewards for vulnerability disclosures, as we are a charity.

Reporting

If you believe you have found a security vulnerability, please submit your report to us via email at vulnerability@imajica.com.

In your report, please include the following details:

- The website, IP, or page where the vulnerability can be observed.

- A brief description of the type of vulnerability (e.g., “XSS vulnerability”).

- Steps to reproduce the issue. These should be benign, non-destructive proof of concept. This helps us triage your report quickly and accurately, reducing the likelihood of duplicate reports or malicious exploitation.

Format of Email (Example)

\*\*URL of Website:\*\* [Insert URL]

\*\*Page Where Vulnerability Can Be Observed:\*\* [Insert Page]

\*\*Summary:\*\*

[Add brief description of the vulnerability]

\*\*Steps to Reproduce:\*\*

1. [Add step]

2. [Add step]

3. [Add step]

\*\*Supporting Material/References:\*\*

[List any additional material (e.g., screenshots, logs, etc.)]

\* [Attachment/Reference]

What to Expect

After submitting your report, we will respond within 5 working days and aim to triage your report within 10 working days. We will keep you informed of our progress.

Priority for remediation will be assessed based on the impact, severity, and exploit complexity of the vulnerability. Please note that vulnerability reports may take time to triage and address. You are welcome to inquire about the status, but please limit your inquiries to once every 14 days to allow our teams to focus on remediation.

We will notify you when the reported vulnerability has been remediated, and you may be invited to confirm that the solution adequately addresses the issue.

Once resolved, we welcome requests to disclose your report, but please coordinate the public release with us to ensure accurate guidance for affected users.

Guidance

You must NOT:

- Break any applicable laws or regulations.

- Access unnecessary or excessive amounts of data.

- Modify data within our systems or services.

- Use invasive or destructive scanning tools to find vulnerabilities.

- Attempt or report any form of denial of service.

- Disrupt our services or systems.

- Submit reports detailing non-exploitable vulnerabilities or minor best practice issues.

- Communicate vulnerabilities or associated details other than as described in this policy.

- Social engineer, 'phish', or attack the Organisation’s staff or infrastructure.

- Expect or request any financial compensation for your efforts.

You must:

- Comply with data protection rules and respect the privacy of the Organisation’s users, staff, and contractors. Do not share or fail to secure any data retrieved from our systems.

- Securely delete all data retrieved during your research as soon as it is no longer required or within one month of the vulnerability being resolved.

Legalities

This policy is designed to align with good practices for vulnerability disclosure. It does not grant permission to act in any manner inconsistent with the law or that might cause the Organisation or its partners to breach legal obligations.

If legal action is initiated against you by a third party and you have complied with this policy, we will take steps to clarify that your actions were conducted in compliance with it.

Thank you for helping us keep our users safe!