Varni Labs

Responsible Disclosure Policy

July, 2023

At Zamp Finance (Varni Labs group of companies), we take the security of our systems seriously, and it is our constant endeavour to make our website a safe place for our customers.

However, in the rare case when a security researcher or member of the public identifies a vulnerability in our systems, and responsibly shares the details with us, we appreciate their contribution, work closely with them to address such vulnerabilities with urgency, and if they want, publicly acknowledge their contribution.

Recognition eligibility

To be eligible for recognition, you must

- Be the first person to responsibly disclose the bug by emailing the vulnerability to security@zamp.finance
- Report a bug that could compromise our users' private data, circumvent the system's protections, or enable access to a system within our infrastructure

Rules of Engagement

In disclosing any bug/ issue, you must follow the rules of engagement as laid out below

- You give us sufficient time to investigate and mitigate the reported vulnerability
- You refrain from accessing sensitive information (by using a test account and/or system), performing actions that may negatively affect other Zamp Finance users (denial of service) or sending reports from automated tools
- You do not exploit a security vulnerability that you discover for any reason (This includes demonstrating additional risk, such as attempted compromise of sensitive company data or probing for additional issues)
- You don’t violate any laws or breach any agreements to discover vulnerabilities
- You do not publicly disclose details of a security vulnerability that you've reported without Zamp Finance's permission.

Program terms

We recognise security researchers who help us to keep the Zamp Finance system safe by reporting vulnerabilities in our services. Recognition for such reports are entirely at Zamp Finance’s discretion, based on risk, impact and other factors.

For recognition in Zamp Finance’s Hall of Fame, you need to meet the following requirements

- Adhere to our Responsible Disclosure Policy
- Report a security bug: Identify a vulnerability in our services or infrastructure which creates a security or privacy risk (Note that Zamp Finance ultimately determines the risk of a vulnerability, and that many software bugs are not security vulnerabilities)
    - We specifically exclude certain types of potential security vulnerabilities; these are listed under "Out of Scope”.
- If you inadvertently cause a privacy violation or disruption (such as accessing account data, service configurations or other confidential information) while investigating a vulnerability, make sure that you disclose this in your report.

We follow these guidelines when evaluating reports under our responsible disclosure program

- We investigate and respond to all valid reports. Due to the volume of reports that we receive, however, we prioritise evaluations based on risk and other factors, and it may take some time before you receive a reply
- We determine recognition in the hall of fame based on a variety of factors, including (but not limited to) impact, ease of exploitation and quality of the report. Note that extremely low-risk vulnerabilities may not qualify for hall of fame at all
- In the event of duplicate reports, we give recognition to the first person to submit a vulnerability (Zamp Finance determines duplicates and may not share details on the other reports)

Note that your use of Zamp Finance services including for the purposes of this programme, is subject to Zamp Finance's Terms and Policies. We may retain any communications about security vulnerabilities that you report for as long as we deem necessary for programme purposes, and we may cancel or modify this programme at any time.

Reporting a vulnerability

If you identify a vulnerability on our web or mobile applications and infrastructure, we request you to follow the steps outlined below

- Submit the vulnerability report form with the necessary details to recreate the vulnerability scenario. This may include screenshots, videos or simple text instructions
- Share your contact details (email address), so that our security team can reach out to you if further inputs are needed to identify or close the problem
- If the identified vulnerability can be used to potentially extract information of our customers or systems, or impair our system's ability to function normally, please refrain from actually exploiting such a vulnerability. This is necessary for us to consider your disclosure a responsible one
- While we appreciate the inputs of White Hat hackers, we may take legal recourse if the identified vulnerabilities are exploited for unlawful gains or getting access to restricted customer or system information or impairing our systems
- Report bugs to us using the Submit Report button (displayed at the top of the page)

Qualifying Vulnerabilities

Any design or implementation issue that is reproducible and substantially affects the security of Zamp Finance users is likely to be in scope for the program. Common examples include

- Injections
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Remote Code Execution (RCE)
- Authentication/Authorisation flaws
- Domain take-over vulnerabilities
- Able to take-over other Zamp Finance user accounts (while testing, use your own another test account to validate)
- Any vulnerability that can affect the Zamp Finance Brand, user data and financial transaction.

Out of Scope

The following bugs are unlikely to be eligible

- Vulnerabilities found through automated testing
- "Scanner output" or scanner-generated reports
- Publicly released CVE's or 0-days in internet software within 90 days of their disclosure
- "Advisory" or "Informational" reports that do not include any Zamp Finance testing or context
- Vulnerabilities requiring MITM or physical access to the victim's unlocked device
- Denial of Service attacks
    - SPF and DKIM issues
    - Content injection
    - Hyperlink injection in emails
    - IDN homograph attacks
    - RTL Ambiguity
- Content Spoofing
- Vulnerabilities relating to Password Policy
- Full-Path Disclosure on any property
- Version number information disclosure
- Third-party applications on the Zamp Finance Application directory (identified by the existence of a "Report this app" link on the app's page). Please report vulnerabilities with these services to the creator of that specific application
- Clickjacking on pre-authenticated pages, or the non-existence of X-Frame-Options, or other non-exploitable clickjacking vulnerabilities
- CSRF-able actions that do not require authentication (or a session) to exploit Reports related to the following security-related headers
    - Strict Transport Security (HSTS)
    - XSS mitigation headers (X-Content-Type and X-XSS-Protection)
    - X-Content-Type-Options
    - Content Security Policy (CSP) settings (excluding nosniff in an exploitable scenario)
- Bugs that do not represent any security risk
- Security bugs in third-party applications or services built on the Zamp Finance API - please report them to the third party that built the application or service
- Security bugs in software related to an acquisition for a period of 90 days following any public announcement
- HTTP TRACE or OPTIONS methods enabled
- Non-sensitive (i.e. non-session) cookies missing the Secure or Http only flags
- Tap jacking
- Mobile client issues require a rooted device and/or outdated OS version or SSL pinning issues
- Subdomain takeovers without supporting evidence
- Missing best practices in SSL/TLS configuration
- The vulnerabilities that cannot be used to exploit other users or Zamp Finance e.g., self-XSS or having a user paste JavaScript into the browser console
- Open ports without an accompanying proof-of-concept demonstrating vulnerabilities