March 2023

Responsible Disclosure Policy

If you discover a potential security vulnerability within Middle's web applications or APIs, we ask that you disclose it to us as quickly as possible and in a responsible manner as stated in this policy.

Overview

Middle takes the security of its web applications, APIs and customer data very seriously. We also value the work of security vulnerability researchers who contribute to that security.

The purpose of this policy is to provide security vulnerability researchers a way of engaging Middle to share their findings with us in good faith. The overall objective is to ensure that security vulnerabilities in our systems and applications are identified and mitigated in a timely manner.

If you have any questions, please contact us at security@middle.finance.

What this policy covers

We allow you to conduct security vulnerability research and testing only on our services and products to which you have authorised access, and only in a responsible manner. This policy does not cover any action that is unlawful or contrary to legally enforceable terms and conditions for using our services and products.

The following types of research are strictly prohibited:

- accessing or attempting to access accounts or data that does not belong to you
- attempting to modify or destroy any data
- executing or attempting to execute a denial of service (DoS) attack
- any activity that degrades our system's performance
- sending or attempting to send unsolicited or unauthorised email, spam or any other form of unsolicited messages

- conducting social engineering (including phishing) of on Middle employees, contractors or customers or any other party
- posting, transmitting, uploading, linking to, sending or storing malware, viruses or similar harmful software that could impact our services, products or customers or any other party
- testing third party websites, applications or services that integrate with our services or products
- the use of automated vulnerability scanners
- exfiltrating any data under any circumstances
- any kind of activity that portrays you as acting from or on behalf of the Middle system or its staff
- any activity that violates any law.

What happens next?

You can report a potential security vulnerability by emailing us at security@middle.finance with as much detail so we can reproduce your steps.

Once you have reported a potential security vulnerability, we will:

- Acknowledge receipt of your report within 24 hours and contact you to verify the issue and determine the appropriate course of action.
- Agree upon a date for public disclosure. We ask that you refrain from publicly disclosing any information about the issue until we have had an opportunity to investigate and fully address it.
- Address all reported security issues in a timely and responsible manner. If we confirm that a vulnerability exists, we will work to develop and resolve the issue as quickly as possible.

We do not compensate individuals or organisations for identifying potential or confirmed security vulnerabilities.

Recognition

We thank the researchers who help keep our products and services safe by reporting security vulnerabilities responsibly in accordance with this Policy.