Afterpay Responsible Disclosure of Security Vulnerabilities Guidelines

Introduction

At Afterpay we endeavour to make sure our systems are worthy of our customers' trust. As part of this effort, we want to encourage responsible disclosure of security vulnerabilities. If you believe you've discovered a potential security vulnerability within Afterpay's applications or infrastructure, we strongly encourage you to disclose it to us as quickly as possible and in a responsible manner.

We appreciate the assistance and patience of security researchers and are committed to reviewing all reports that are disclosed to us. We will do our best to address each issue in a timely fashion, and request that you await confirmation from the Afterpay security team that the issue has been resolved before public disclosure. A key element of these Responsible Disclosure Guidelines is that you do not disclose (either publicly or to any other third party) the details of any potential security vulnerabilities without express written consent from us.

To encourage responsible disclosure, we will not take legal action against security researchers in relation to the discovery and reporting of a potential security vulnerability, where both the relevant discovery, and reporting, are conducted strictly in accordance with these Responsible Disclosure Guidelines, and with applicable laws and regulations. In the event of any non-compliance, we reserve all of our legal rights.

How to report a vulnerability:

You can responsibly disclose potential security vulnerabilities to the Afterpay Security Team by emailing security@afterpay.com. Ensure that you include details of the potential security vulnerability and exploit with enough information to enable the Security Team to reproduce your steps.

When reporting a potential security vulnerability, please include as much information as possible, including:

- An explanation of the potential security vulnerability;

- A list of products and services that may be affected (where possible);
- Steps to reproduce the vulnerability;
- Proof-of-concept code (where applicable);
- The names of any test accounts you have created (where applicable); and
- Your contact information (Does not have to be identifying an email is plenty).

Guidelines

We encourage you to conduct responsible security research on our products and services, but only in accordance with the following guidelines:

1. Vulnerability research and testing is only permitted on services and products to which you have authorised access.
2. Do not engage in any activity that causes harm (or could potentially cause harm) to Afterpay, our customers, suppliers, third parties, or our employees.
3. Do not engage in any activity that can potentially or actually stop or degrade Afterpay's services or assets.
4. Do not engage in any activity which could lead to reputational or brand damage to Afterpay or any of its related companies, partners, merchants, or customers.
5. Do not engage in any activity that violates (a) federal or state laws or regulations or (b) the laws or regulations of any country where (i) data, assets or systems reside, (ii) data traffic is routed or (iii) the researcher is conducting research activity.
6. Do not store, share, compromise or destroy Afterpay or customer data. If personal data that is not publicly available is encountered, you should immediately halt your activity, purge related data from your system, and immediately contact Afterpay. This step protects any potentially vulnerable data, and you.
7. Do not initiate a fraudulent financial transaction.
8. Await confirmation from the Afterpay Security Team that the issue has been resolved and the vulnerability is able to be shared, before such information or vulnerability is shared with a third party or disclosed publicly.

Activities not covered by the Responsible Disclosure Program

The following types of research and actions are strictly prohibited, and are considered to be a breach of these Responsible Disclosure Guidelines:

- Physical Testing
- Social Engineering. For example, attempts to steal cookies, fake login pages to collect credentials
- Phishing
- Denial of service attacks (E.g. Syn Flood)
- Resource Exhaustion Attacks lasting longer than 1 second or across a large volume of requests
- Any actions which harm or may harm Afterpay's systems, applications, infrastructure, property, or people.
- Any other actions which may lead to the exposure, compromise, damage or destruction of Afterpay data including but not limited to:
    - Customer Data;
    - Merchant Data;
    - Afterpay Source Code; or
    - Afterpay IP.