B2BX Security Bug Bounty Program

June 2018

contact@b2bx.exchange
support@b2bx.exchange

Introduction

The B2BX Security Bug Bounty Program (hereinafter – "SBBP") is designed to reward those who help the company to improve the safety of its products and solutions.

Terms

"Business customer" is a B2BX client who bought B2BX products and/or solution.

"Client" or "User" is the end user of solutions who is a client of B2BX Business customer.

General provisions

Conditions to be eligible for a reward:

- The security bug must be new and previously unreported.
- The security bug must be a part of Company's code or a part of the code of Company's third-party developer involved.
- You must not be Company's employee or employee of Company's Business customer or have any kind of connection with the Company's business or Company's business customers.
- You should use your best effort not to access, delete, modify or store other software user's data; use your own data or test accounts for security research purposes.
- If you inadvertently access, delete, modify or store other user's data, we ask that you notify the Company immediately at security@b2bx.exchange and delete any stored data after notifying us.
- You must not exploit the security vulnerability for your own gain.
- You must give us a reasonable amount of time to address the security issue you raise before making any part of it public.

If a bug is reported by a team or by multiple researchers at the same time, the bounty will be split evenly amongst them.
Do not threaten or attempt to extort the Company. We will not award a bounty if you threaten to withhold the security issue from us or if you threaten to release the vulnerability or any exposed data to the public.

Types of errors

- Code injection (Code Injection/SQL Injection);
- Broken Authentication and Session Management;
- Access to personal data;
- Cross-Site Scripting (XSS);
- Cross-Site Request Forgery (CSRF);
- Confirming transactions without verification, duplicating transaction results.

Error categories

- Critical (S1): affects critical functionality or critical data (Example: access to personal data, confirming transactions without verification).
- Major (S2): affects major functionality or major data; requires data known in advance to repeat (Example: personal data access recovery, by known account attributes; DDoS back-end servers).
- Minor (S3): affects minor functionality or non-critical data; requires data known in advance to repeat (Example: rounding error).

Our guarantees

B2Broker company sincerely wishes to see its products free from any security bugs and supports those who want to help the company with that.

We will not threaten or bring any legal action against anyone who makes a good-faith effort to comply with our bug bounty program. As long as you comply with these terms, we consider your security research to be “authorized”.

We understand that many Company’ products and services are interconnected with third-party systems and services. We approve your research on Company’s products, but we cannot guarantee relevant permission for alike third party and/or related services to do so.

If you are not sure whether your behavior meets the above conditions, please, contact us by e - mail security@b2bx.exchange, and we will do our best to help you.