

SODECO TRADING - BUG BOUNTY HUNTER AGREEMENT

1. DEFINITIONS

“Asset”: An ICT system, network, technology, infrastructure, application, software, or other target, communicated by a Company in its Program, for the purpose of having its security assessed by Researchers (previously known as the “Environment”).

“Bounty”: A monetary reward, that is awarded to the first Researcher who successfully makes a Submission of a Vulnerability in the Company’s Asset.

“Company”: A customer using this bug bounty initiative to reach out to Researchers via email invitations and to receive Submissions.

“Company Data”: Any information, files, personal data, or other data which becomes known to a Researcher or to which a Researcher obtains access in the context of participation in a Program. Examples include program descriptions, Asset information, Vulnerabilities, login credentials, and other confidential information.

“Ethical Hacking”: The process of attempting to penetrate a network or computer system and bypass system security to identify potential security vulnerabilities and inform the system owner of such vulnerabilities. Ethical hacking is conducted with good intentions and aims to improve system security.

“Program”: A Company’s security initiative communicated via email invitations, through which the concerned Company authorizes Researchers to test the security of an Asset and report identified Vulnerabilities. Programs primarily target the financial sector, including banking, trading, and brokerage web applications. The Program is referred to as the **“Web Site Test”**.

“Program Conditions”: The Company’s description of the assistance it is seeking from Researchers, including the scope, requirements, and remuneration terms for Bounties. Program Conditions will be provided via email before a Researcher can participate in a Program.

“Researchers”: Independent security researchers (ethical hackers), willing to participate in one or more Programs via email invitations. Researchers may act in a professional or non-professional capacity and may have different levels of experience and expertise. Anyone who initiates activities of Ethical Hacking under a Program is considered a Researcher.

“Submission”: A Researcher’s description of a Vulnerability identified in an Asset, in the context of participation in a Program. Submissions serve as notifications to the Company and are submitted via the designated email address provided in the Program invitation.

“Vulnerability”: A bug, defect, or weakness that compromises the security of the information or communication technologies, potentially exploitable by malicious parties.

2. OPERATION AND BACKGROUND

Researchers will receive an email invitation from the Company outlining the Program details, scope, and Program Conditions. Researchers operate independently and voluntarily, choosing which Programs to participate in and determining their time commitment.

If a Researcher identifies a Vulnerability, it must be disclosed promptly to the Company via the provided email address. The goal is to allow the Company to take appropriate action to resolve the Vulnerability and improve system security.

The Company assumes no responsibility for interactions between Researchers and other parties. Participation in a Program is solely between the Researcher and the Company named in the invitation email.

3. REGISTERING AS A RESEARCHER

Sign-up to participate in the Program is at the discretion of the Company. Selection is based on the Researcher's level and achievements on platforms such as **HackerOne** and **Bugcrowd**.

If a Researcher does not have a **HackerOne** or **Bugcrowd** profile and has never successfully submitted vulnerabilities through those programs, the Company reserves the right to decline the request to join the Program.

A confirmation email will be sent to Researchers who are accepted to join and participate in the Programs.

By responding to a Program invitation and participating in a Program, you accept and agree to comply with the terms of this Bug Bounty Hunter Agreement. If you do not agree with any term herein, you may not participate in any Program and are not authorized to access Assets.

By participating, you declare and warrant that you:

- Have the right, power, and authority to enter into this Agreement;
- Are at least 18 years old (or at least 16 with parental or guardian permission);
- Are not subject to any legislative measures prohibiting you from engaging in Ethical Hacking;
- Are not prohibited from performing Ethical Hacking activities by law, your organization, or employer.

Your participation is strictly personal. You must maintain confidentiality regarding all Program details and are responsible for all activity linked to your participation.

4. PARTICIPATING IN A PROGRAM

Companies will invite Researchers via email to participate in security testing of specific Assets. Each email invitation will include:

- A description of the Program scope;
- Any prohibited actions;
- The bounty amounts for qualifying vulnerabilities;
- Any additional Program Conditions.

By responding to an email invitation and participating in a Program, you:

- Must read and comply with all Program Conditions before engaging with an Asset;
- Must use only Ethical Hacking techniques and avoid any methods that may disrupt the Asset;
- Must promptly report any identified Vulnerabilities via the designated email address;
- Are responsible for ensuring compliance with applicable laws regarding privacy and data protection;
- Are liable for any damages resulting from your actions;
- Acknowledge that unauthorized access beyond the Program scope may be illegal and subject to legal action.

5. PROHIBITED ACTIONS

You may not:

- Exploit Vulnerabilities beyond what is necessary for identification and reporting;
- Use (Distributed) Denial of Service (DoS or DDoS) attacks, social engineering, or prohibited techniques;
- Install malware, viruses, or any harmful technologies;
- Access, copy, or download Company Data beyond what is necessary for reporting;
- Disclose any findings without explicit written permission from the Company.

If a third-party system is unintentionally affected, you must stop testing immediately and report the issue to the Company.

6. SUBMITTING VULNERABILITIES

If you discover a Vulnerability, you must promptly submit a report via the designated email address. The report must clearly describe the Vulnerability, its impact, and the steps to reproduce it.

7. BOUNTIES

The Company will reward qualifying Vulnerability Submissions based on the following remuneration structure:

- **Participation Reward:** If at least one valid Vulnerability is found, the Researcher will receive a fixed reward of \$500 USD in addition to any applicable Bounties.
- **Multiple Valid Vulnerability Bonus:** If a Researcher submits at least three (3) valid vulnerabilities rated as Medium, they will receive a guaranteed reward of \$3,500 USD.
- **Additional Bonus:** If more than three valid vulnerabilities are submitted, additional bonuses may be awarded at the Company's discretion.

Bounties are awarded only if:

- The Researcher is the first to report the Vulnerability;
- The Vulnerability is validated and confirmed by the Company;
- The Researcher has complied with all Program Conditions and this Agreement.

Bounties are discretionary and subject to verification. Payments will be made in **USD** via a method designated by the Company. Researchers are responsible for any applicable taxes and legal obligations regarding payments. **Payments will be sent directly to the bank account specified by the Researcher.**

8. CONFIDENTIALITY

All information related to a Program, including discovered Vulnerabilities, is strictly confidential. Researchers may not disclose or share information without written authorization from the Company. Unauthorized disclosure may result in legal consequences.

9. INTELLECTUAL PROPERTY RIGHTS

1. You may not engage in any activity that infringes or misappropriates the industrial-, intellectual- or other proprietary rights of others. In particular, you must ensure the content of your profile and Submissions do not violate the intellectual property rights of any party.
2. You will remain the owner of the intellectual property rights in your Submissions. Do note that you are required to maintain any information related or retraceable to a Company confidential, in accordance with article 9.

3. By submitting a Vulnerability through email, your Submission will be sent to both Sodeco Trading, and the Company involved. By making a Submission, you provide:
 1. to the Company to whom you direct your Submission an irrevocable, in time unlimited, non-exclusive, non-transferable, worldwide, royalty-free license to use, access, copy, reproduce, display, modify, translate, transmit and distribute copies of that Submission to the extent needed for the purpose of assessing the Vulnerability and improving the security of its systems, assets and environments.
 2. to Sodeco Trading an irrevocable, in time unlimited, non-exclusive, worldwide, royalty-free license to use, reproduce, copy, display, modify, translate and disclose (within its organisation and to the Company to whom your Submission is addressed) any content of your Submissions, within its intended purpose, which in particular implies that Sodeco Trading will use your Submissions to comply with any of its obligations vis-à-vis you and/or the Company involved and/or to demonstrate or proof such compliance where relevant. Sodeco Trading will not claim ownership of your Submissions.
4. Sodeco Trading may collect anonymous/statistical information about your Submissions and may use such information for any purpose it sees fit, including for commercial purposes. By signing up to this program, you irrevocably agree thereto.

10. RELATIONSHIP BETWEEN COMPANY, RESEARCHER AND SODECO TRADING

1. A Program and Program Conditions are always published by or in the name of the Company whose name is indicated with the Program. Companies interact with you and allow you to participate in their Programs, through email, and act independently from Sodeco Trading. Sodeco Trading is not responsible for their actions, omissions, communication, and content (including but not limited to Program content and/or Program Conditions).
2. You provide your assistance and information in the context of a Program directly to and for the benefit of the Company involved and on your own risk and account. You are responsible for your (Ethical Hacking) activities in this context directly vis-à-vis the Company and thereby act as an independent party. Companies are independent parties inviting you to participate in their Programs and connect with you through email.
3. By participating in a Program, you are considered to accept and enter into the applicable Program Conditions vis-à-vis the Company involved. Companies can also derive rights from these Researcher T&C against you, in accordance with article 3.2. In

case of contradiction between the Program Conditions and these Researcher T&C, the Program Conditions will prevail within your (contractual) relationship with the Company.

4. You perform and provide your activities, assistance, and information on a voluntary, ad hoc and independent basis to Companies and not as an agent, representative, partner or employee of the Company or Sodeco Trading. Nothing herein shall be intended, considered, or interpreted to determine otherwise, or to give you any rights that usually come with such capacity. You are responsible for the payment of any applicable taxes, levies and/or social contributions in the context of your receipt of any Bounties and are responsible to comply with any other statutory obligations associated with your activities hereunder.

11. COMMUNICATION BETWEEN COMPANY AND RESEARCHER

1. Your Submissions and any communication made in the context of your Submission, may be accessed by both Sodeco Trading and the Company involved.
2. In the context of a specific Program or Submission, Sodeco Trading may communicate with you on the Company's request and on Company's behalf and vice versa. Sodeco Trading will act in good faith and transfer received communications between both parties without exceptions and without undue delay. All communications will fall under the confidentiality regime as stipulated above.

12. LIABILITY

Researchers must ensure that their actions do not violate third-party rights, laws, or regulations. Any harm caused to the Company or third parties due to non-compliance with this Agreement is the Researcher's responsibility.

13. DISPUTE RESOLUTION

In the event of a dispute between a Researcher and the Company, both parties agree to resolve the matter through good-faith negotiations. If no resolution is reached, the matter shall be governed by the laws of the jurisdiction specified by the Company.

14. OUR LIABILITY

1. We use reasonable efforts to keep our services safe, secure, and functioning properly, but do not guarantee the continuous operation of, and disclaim any liability in that context. Updated information and notifications may not occur in real time and may sometimes be subject to delays, which risk you accept by subscribing to the program.

2. Accordingly, to the extent permitted by applicable law, Sodeco Trading excludes all express or implied warranties, terms and conditions including, but not limited to, use or operation, merchantability and/or fitness for a particular purpose.
3. Sodeco Trading acts as coordinator and is not responsible for any content, communications, acts or omissions of Companies, Researchers or other users and disclaims any liability in this context. In particular, in no event Sodeco Trading will be liable for a Researcher's participation or other activities in the context of a Program. Confirmation of Submissions and payment of Bounties is done only upon instruction of the Company involved.
4. Sodeco Trading can only be held liable for direct damages, caused by its violation of the obligations Sodeco Trading expressly undertakes in these Researcher T&C, and this only within the limitations set out below.
5. Without prejudice to the above, Sodeco Trading's aggregate liability to you or to any third party is limited to a maximum amount of 1500,00 USD per claim and per year in total.
6. The limitation of liability in article 16.5 is not intended or construed to limit Sodeco Trading's responsibility to pay Bounties in accordance with article 8. Any claims or actions related to the payment of Bounties will irrevocably lapse and become invalid six (6) months from the date of the Submission.
7. Nothing in this agreement is intended to exclude or limit any liability that cannot be excluded or limited as a matter of law and relevant clauses will be interpreted accordingly.

16. GENERAL TERMS

The Company reserves the right to update this Agreement. Any changes will be communicated via email. Researchers must review and agree to any updates before continuing participation.

By participating in a Program, you confirm that you have read and agreed to this Agreement.