cycode

Cycode Bug Bounty Program

We at Cycode cooperate with security experts across the globe in various ways to stay up-to-date with the latest security techniques.

As part of these efforts, Cycode looks forward to working with the security community to find vulnerabilities in order to keep our businesses and customers safe.

If you've discovered a security issue that you believe we should know about, we'd love to work with you. Further, under the Cycode Bug Bounty Program (the “Program”) you may be entitled to a monetary reward for your efforts.

The Bug Bounty Program applies to security vulnerabilities found within Cycode's public-facing online environment. This includes Cycode's websites, SaaS environment and exposed APIs listed below as Eligible Targets. For the protection of our customers, we do not disclose, discuss or confirm security matters until our Security Team completes its comprehensive investigation, and diagnoses and fixes all relevant issues.

Bounty Eligibility

- You must agree and adhere to the Program rules and terms and conditions set forth below.
- You must be the first to report the related issue in order to be eligible for a bounty.
- You must provide all additional information required for our Security Team to review your application and findings and reproduce and triage the issue, promptly upon our request.
- Cycode's partners, customers, service providers and any other related parties are not eligible for participation in this program.

Program Rules

- Please provide detailed reports with reproducible steps. If the report is not detailed enough to reproduce the issue, the issue will not be eligible for a reward.
- Submit one vulnerability per report, unless you need to chain vulnerabilities to provide impact.
- When duplicates occur, we only award the first report that was received (provided that it can be fully reproduced).
- Multiple vulnerabilities caused by one underlying issue will be awarded one bounty.
- Do not disclose the reported vulnerability to others until we’ve had reasonable time to address it.
- You are requested to make a good faith effort to avoid any privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with explicit permission of the account holder.
- Do not knowingly harm any Cycode service or product or the experience or useability of these by others.
- Do not attempt to gain access to, modify, or damage data belonging to others.
- Do not use any “robot”, “spider” or other automatic device, program, script, algorithm, or methodology, or any similar or equivalent manual process, to access, acquire or copy any Cycode services or product (or its data and/or content) or to to find vulnerabilities. They’re noisy and we may ban your IP address.

- Do not attempt non-technical attacks such as social engineering, phishing, or physical attacks against our employees, users, or infrastructure.

We will investigate legitimate reports and make every effort to quickly correct any vulnerability. A well written report will allow us to more quickly and accurately triage your submission.

- Provide details of the vulnerability, including information needed to reproduce and validate the vulnerability and a Proof of Concept (POC).
- A clear description of the issue, including the impact you believe it has to the user, Cycode or others.
- Specific reproduction steps including the environment used for testing (browsers, devices, tools, configuration) and any accounts used during testing.
- Your recommendations to resolve the issue.

Eligible Targets

At this time, the scope of the Program is focused predominantly on security vulnerabilities found in the following targets:

- app.cycode.com
- api.cycode.com
- app.eu.cycode.com
- api.eu.cycode.com
- www.cycode.com

Vulnerabilities submitted outside this scope are generally less likely to receive recognition or rewards

Exclusions (Out of scope vulnerabilities)

The following vulnerabilities are not eligible for awards under the Program:

- Network level Denial of Service attacks
- Application Denial of Service by locking user accounts
- Descriptive error messages or headers (e.g. Stack Traces, banner grabbing)
- Disclosure of known public files or directories, (e.g. robots.txt)
- Outdated software / library versions
- OPTIONS / TRACE HTTP method enabled
- CSRF on logout
- CSRF on forms that are available to anonymous users
- Cookies that lack HTTP Only or Secure settings for non-sensitive data
- Self-XSS and issues exploitable only through Self-XSS
- Reports resulting from automated scanning utilities without additional details or a POC demonstrating a specific exploit
- Attacks requiring physical access to a user's device
- Attacks dependent upon social engineering of Cycode employees or vendors.

- Username enumeration based on login or forgot password pages.
- Enforcement policies for brute force, rate limiting, or account lockout.
- SSL/TLS best practices.
- SSL attacks such as BEAST, BREACH, Renegotiation attack.
- Clickjacking, without additional details demonstrating a specific exploit.
- Mail configuration issues including SPF, DKIM, DMARC settings.
- Use of a known-vulnerable library without a description of an exploit specific to our implementation.
- Password and account recovery policies.
- Presence of autocomplete functionality in form fields.
- Publicly accessible login panels.
- Lack of email address verification during account registration or account invitation.
- Lack of email address verification password restore.
- Session control during email/password changes.

Reward

You may be eligible to receive a monetary reward if:

- You are the first person to submit an eligible vulnerability
- That vulnerability is determined to be a valid security issue by Cycode's security team
- You are, and remains, in full compliance with all Program terms

All bounty amounts will be determined at t Cycode’s absolute and sole discretion, based on our Security Team evaluation of the severity, impact, and quality of the reported issue.. There could be submissions that we determine have an acceptable level of risk such that we do not make changes.

The minimum bounty amount for a validated bug submission is $50 USD and the maximum bounty for a validated bug submission is $1,000 USD. Cycode's Security Team retains the right to determine if the bug submitted to the Bug Bounty Program is eligible. All determinations as to the amount of a bounty made by Cycode are final.

Response Targets

Cycode will make its best effort to meet the following response targets for community members participating in our Program:

* Time to first response (from report submit) - 2 business days

* Time to triage (from report submit) - 4 business days

* Time to bounty (from triage) - 8 business days

We’ll try to keep you informed about our progress throughout the process.

cycode

Payment

You'll need to submit an invoice to receive payment. The invoice must meet all legal requirements. Once we have that information, awarded bounty payments will be paid. Cycode accepts the following payment methods.

Method	Required Info
PayPal	PayPal email address
Wire	First and last name, address, bank name, SWIFT, IBAN number, sort code

Submit Your Report

Vulnerability information is extremely sensitive. When using email to report a potential security issue to Cycode Security Team, use security@Cycode.com.

It's important to include at least the following information in the email:

- Organisation and contact name
- Products or solutions and versions affected
- Description of the potential vulnerability
- Supporting technical details (such as system configuration, traces, description of exploit/attack code, sample packet capture, proof of concept, steps to reproduce the issue)
- Information about known exploits

Terms and Conditions

By submitting reports and participating in the Cycode Bounty Program (the "**Program**"), you agree to the following terms:

1. Any and all information that you acquire or gain access to as part of your action in connection with this Program, about us, our affiliates, customers and vendors is confidential ("**Confidential Information**"). You will keep such Confidential Information in strict confidence to be used only as required in the ordinary course of performing your actions under this Program. You will not copy, reproduce, sell, assign, licence, market, transfer, disclose or use, for yourself or others, directly or indirectly, any Confidential Information or anything relating to it without the prior written consent of Cycode.

2. You affirm that you have not disclosed and agree that you will not disclose the bug or your submission to anyone other than Cycode via the submission procedure detailed herein.

3. You will not use or publish in any advertising, publicity, marketing or otherwise the name, trademark or logo of Cycode or represent that you are associated therewith.

4. You may only use your own account for testing or research purposes (where applicable). If you encounter any 3rd party user information, then you should: (a) immediately cease doing so; (b) report this immediately to our Security Team; and (c) treat such information as Confidential Information.

5. You acknowledge and agree that any and all information you access is owned by Cycode or its customers and vendors. You have no rights, title or ownership to any information that you may encounter.

6. By making a submission or providing any feedback to us, you represent and warrant that such submission is original to you and that you have the right to submit it. Any and all feedback, reports, and submissions provided by you will be exclusively owned by Cycode and may be used by us for any purpose whatsoever.

7. You must comply with all applicable laws in connection with your actions under the Program.

8. Your testing activities must not violate any laws or negatively impact Cycode, Cycode’s customers or Cycode's online environment availability or performance

9. Eligibility for rewards and determination of the recipients and amount of rewards shall be at Cycode’s sole and absolute discretion.

10. The parties to this agreement are you and Cycode without any third party beneficiaries

11. Cycode may modify the terms of this Program or terminate it at its sole and absolute discretion and at any time, with or without notice.