Perlego Vulnerability Reward Program (VRP)

Overview

The Perlego Vulnerability Reward Program (VRP) aims to enhance the security of our services by encouraging and rewarding responsible security research. We value the contributions of researchers who help us identify and mitigate vulnerabilities in our systems, thereby protecting our users and maintaining the integrity of our platform.

Response time

We will respond to all submissions within the below timelines, but that does not mean that submissions will be verified by our security team yet. Rewards will be issued once our security team has properly assessed and mitigated the submission.

Vulnerability Severity	**Time to respond**
Critical	2 Working days
High	5 Working days
Moderate	10 Working days
Low	15 Working days

Scope of the Program

Services in Scope

The program covers all Perlego-owned web services that handle sensitive user data. This includes:

Domains Covered: All services within the `*.perlego.com` and `*.perlego.ai` domains.

Applications: Perlego-owned APIs, web applications, mobile apps, browser extensions, and other services.

Vulnerabilities in third-party services or software are **not** included in the scope, unless the vulnerability is in the way we integrate with them. If you can repeat the vulnerability on other third-party integrations of the same vendor, please report it with them instead

If you find Perlego Employee login credentials, API keys etc, please report it, but do not attempt to successfully validate if/that it works.

Out of Scope

The following are considered out of scope and will not qualify for rewards:

- Vulnerabilities in services not owned by Perlego
- Issues in third-party libraries or software
- Physical security attacks (e.g., accessing offices, or attacking wifi networks)
- Phishing attempts against employees
- Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks
- Social engineering tactics
- Brute force attacks
- Disclosure of known public files or directories

- Privacy related issues, involving publicly available information or information that is not considered sensitive (e.g. email addresses in some contexts, Public API key disclosure without proven business impact).
- Self-XSS, where the attacker and victim are the same person, that cannot be used to exploit other users.
- Issues purely related to Search Engine Optimization (SEO), Homoglyph attacks, broken links or content-related issues.
- Missing cookie flags or security headers.
- Missing or incorrect SPF records of any kind.
- Missing or incorrect DMARC records of any kind.
- Lack of rate limiting
- HTTP/DNS cache poisoning
- SSL/TLS Issues, such as:
    - SSL Attacks such as BEAST, BREACH, Renegotiation attack.
    - SSL Forward secrecy not enabled.
    - SSL weak/insecure cipher suites.
- Logout Cross-Site Request Forgery (logout CSRF).
- Best practices violations (e.g. password complexity, expiration, extra verification step at delete account)
- Outcomes of automated tooling without clear exploitable vulnerability. Please follow our Submission Guidelines when reporting, and submissions without sufficient exploit evidence will not be eligible for a reward.
- Coupon code exposure

Qualifying Vulnerabilities

Vulnerabilities that significantly impact the confidentiality, integrity, or availability of user data. If a vulnerability has already been reported by another researcher, any

duplicate reports will not qualify for a reward. We recommend that you carefully document your findings before submitting a report.

Category	Examples
Server-side vulnerabilities	Server-side code execution, unrestricted file access, server-side request forgery
Authentication and authorization flaws	Bypassing authentication, privilege escalation, insecure direct object reference issues
Client-side vulnerabilities	Stored/reflected cross-site scripting (XSS), CSRF, clickjacking
Data leakage and privacy issues	Information disclosure, improper access controls
Large Language Model vulnerabilities	Prompt injection, insecure output handling, sensitive information disclosure,
Other critical security issues	SQL injection, command injection, sandbox escape, SaaS misconfiguration

Non-Qualifying Vulnerabilities:

Certain issues may not qualify for a monetary reward, especially if they pose minimal risk. Below are examples of non-qualifying vulnerabilities:

Category	Examples
Low-impact issues	URL redirection, bugs requiring unlikely user actions
Minimal security implications	Logout CSRF, CSRF with low impact
Issues with outdated software	Flaws affecting outdated browsers
Cosmetic issues	Presence of banner or version information
Common security techniques	Brute force attacks, DDoS attacks
Non-technical attacks	Social engineering, physical security breaches

Submission Guidelines

We kindly request the below items to be included in any submission. Adherence to these guidelines will be accounted for in the amount awarded.

1. **Title**
    - Provide a concise title summarizing the vulnerability.
    - Include details of the page or product version in question.

2. **Vulnerability Details**

Description: Explain the vulnerability, how it was discovered, and why it poses a security risk.
Impact: Describe the potential consequences if exploited.
Severity: Suggest a severity rating (Low, Medium, High, Critical). The security team will use the suggestion, but might decide to rank the severity differently.

3. **Reproduction Steps**
   - Include step-by-step instructions to reproduce the issue.
   - Provide URLs, parameters, tools, or configurations needed to replicate the vulnerability.

4. **Proof of Concept (PoC)**
   Provide evidence demonstrating the vulnerability, such as videos, screenshots, or code snippets.

5. **Environment Details**
   Specify the operating system, browser, device, and any relevant versions used during testing.

6. **Confidentiality Agreement**
   By submitting this report, you agree to maintain the confidentiality of the vulnerability and refrain from disclosing it publicly.

Duplicate Submissions:

If a vulnerability has already been reported by another researcher, any duplicate reports will not qualify for a reward.

Reward Structure

Perlego is a startup with limited funds, and while we may not offer the highest rewards in the industry, we are committed to recognizing significant contributions. The table below outlines the typical reward ranges based on the severity and impact of the reported vulnerability:

Vulnerability Type	Examples	Reward Range
Critical server-side vulnerabilities	Server-side code execution, unrestricted file access	$1,000+
High-severity logic flaws	Authentication bypass, command injection, SQL injection	$100 - $1,000
Moderate client-side vulnerabilities	XSS, CSRF, clickjacking	$50 - $100
Low-severity vulnerabilities	Information disclosure with minimal impact	$10 - $50

Note: For vulnerabilities that could cause significant harm to Perlego's reputation or business continuity, higher rewards may be offered at our discretion.

Guidelines for Investigation and Reporting

To ensure that your research aligns with our guidelines and that your findings are valid:

- **Target Your Own Accounts:** Only investigate vulnerabilities on accounts you own. Do not attempt to access data belonging to other users.
- **Avoid Disruption:** Do not engage in any activities that could disrupt Perlego's services or negatively impact other users.
- **Reporting Format:** Ensure that the reporting requirements are met by following our Submission Guidelines.
- **Reporting Vulnerabilities:** If you discover a vulnerability, please report it to us at security@perlego.com

Legal Considerations

Eligibility: We cannot issue rewards to individuals on sanctions lists or residents of countries under sanctions (e.g., Cuba, Iran, North Korea, Sudan, Syria).

Tax Implications: Researchers are responsible for any tax liabilities related to the rewards based on their country of residence and citizenship.

Program Discretion: The VRP is discretionary and can be modified or terminated at any time. The decision to issue rewards is solely at Perlego's discretion.

Legal Compliance: All testing must be conducted legally and must not disrupt or compromise any data that is not your own.

Vulnerabilities shared publicly will not be eligible for the reward.

The Perlego Vulnerability Reward Program is a collaborative effort to improve the security of our platform. We highly value the contributions of researchers who help

us protect our users and ensure the integrity of our services. We encourage you to continue your efforts in identifying vulnerabilities and reporting them responsibly.

For any questions or further clarification, please do not hesitate to contact us at security@perlego.com.

Best regards,

The Perlego Security Team

Frequently Asked Questions

How should I report a vulnerability?

If you discover a vulnerability, please report it to us at security@perlego.com following our Submission Guidelines.

Will I get a reward for reporting a vulnerability?

Depending on the type of vulnerability and severity, we may offer you a reward. Please see the Scope of the Program for what vulnerabilities qualify and our Reward Structure for example reward ranges.

What if I find a vulnerability, but I don't know how to exploit it?

Vulnerability reports sent to us must have a valid attack scenario and reproduction steps to qualify for a reward, and we consider this to be a critical element of

vulnerability research. Please follow our Submission Guidelines when reporting, as submissions without sufficient exploit evidence will not be eligible for a reward.

How long will I have to wait to know if my report qualifies for an award?

We value the contributions of researchers who help us identify and mitigate vulnerabilities in our systems and we will try to do our best to get back to you as soon as possible based on our availability and the severity of the vulnerability reported. Please see our Response Time for how long you should expect to wait for a response.

How can I check on the progress of my submission?

Please see our Response Time for how long you should expect to wait for a response. Please do not contact us for an update unless you have been waiting for longer than our stated time to respond.

What happens if I disclose the vulnerability publicly before you have a chance to fix it?

By submitting a report, you agree to maintain the confidentiality of the vulnerability and refrain from disclosing it publicly unless we have given permission for disclosure. Any vulnerabilities shared publicly will not be eligible for a reward, and we reserve the right to pursue legal action against any persons who violate our stated policies.

How will I receive my reward?

Once we have validated your submission, and confirmed it qualifies for a reward, we will reply to your email submission notifying you of acceptance and requesting further information to allow our Finance Team to send you the reward. Please note that we cannot issue rewards to individuals on sanctions lists or residents of countries under sanctions (such as: Cuba, Iran, North Korea, Sudan, Syria).

What if multiple people report the same bug? What if someone else has already reported the same vulnerability before me?

If a vulnerability has already been reported to us, new reports will not qualify for a reward. You will qualify for a reward only if you were the first person to alert us to a previously unknown vulnerability.

Can I submit a report through another channel or via a vulnerability broker?

Please note that we do not reward any submissions that aren't sent directly to security@perlego.com

My account was disabled after doing some tests. How can I get my account restored?

We recommend that you create an account dedicated only to testing before beginning any tests on our platform, since we cannot guarantee that you will get access back to your account if it is disabled due to your testing activities. If you have a question regarding your account and access to Perlego, please contact help@perlego.com

What if I have a general question about Perlego?

If you have a question regarding your Perlego account or a general enquiry about the Perlego platform, please contact help@perlego.com