Updated 1st November 2024

CDN77 Bug Bounty Program – Program Terms of DataCamp Limited

At CDN77, security is a top priority. We are committed to ensuring the security and privacy of our systems, data, and users. Our Bug Bounty Program encourages you, as security researchers, to responsibly report vulnerabilities you discover.

These Program Terms outline the rules for responsible research as well as the legal boundaries of this program. By participating in the Bug Bounty Program, you agree to abide by these Program Terms and CDN77's Terms and Conditions, both of which are entered into by you and DataCamp Limited.

Terms not defined herein shall have the same definition as provided in the Terms and Conditions.

If you have any concerns or are unsure whether your security research aligns with these Program Terms at any point, we encourage you to submit any inquiries to bugbounty@cdn77.com before proceeding further.

1. Eligibility and Responsible Disclosure

1.1. Personal eligibility

To be eligible to participate in the Bug Bounty Program you must be at least 18 years of age. If you are under 18, participation is only allowed with verifiable permission from a parent or legal guardian. You must not be a resident of a country under embargo or sanctions according to the laws of the United States, the European Union, or United Kingdom. By participating, you also confirm that you are not violating any local laws or agreements, including employment contracts, that could restrict your involvement.

You are not eligible to participate if you are currently an employee or contractor of DataCamp Limited or DataCamp s.r.o. (collectively referred to as "DataCamp"), or an immediate family or household member of a DataCamp employee or contractor. Additionally, you are ineligible if you were an employee or contractor of DataCamp within one (1) year prior to participating in the Bug Bounty Program.

1.2. Material eligibility

To be eligible for a reward, you must be the first to report the vulnerability, which must be valid and within the scope of the program. Submissions that rely solely on automated scanning tools or those based on out-of-scope attacks will not be rewarded. We expect responsible disclosure, meaning you should not publicly share or disclose the issue to any third parties unless you have our written permission. We also ask that you do not exploit the vulnerability beyond what is necessary to demonstrate its existence, and you should not access, modify, or delete any customer or provider data.

2. Rules of Engagement Clause for Bug Bounty Program

Participants in the Bug Bounty Program are required to adhere to the following rules of engagement when conducting testing:

- Prohibited Mass Scanning: Mass active port or service scanning of our infrastructure is strictly prohibited without prior coordination with the CDN77 team. Such activities can overwhelm our monitoring systems. If scanning is necessary, participants must provide the IP addresses to be used in advance for approval.
- Reporting Information Disclosure: In cases of information disclosure vulnerabilities, researchers must report the issue immediately after collecting sufficient proof of impact. Any further probing or exploration without prior confirmation or coordination with the CDN77 team is not permitted.

- Brute-Force Attacks: Brute-force attacks or credential stuffing attempts on authenticated endpoints are strictly forbidden unless prior consent has been obtained from the CDN77 team.
- No Use of Client Accounts: Researchers are prohibited from using real customer accounts in their testing. Any testing involving privilege escalation (e.g., horizontal privilege escalation) must be conducted using dedicated testing accounts, which can be created specifically for Proof of Concept (PoC) purposes.
- Sensitive Information Sharing: Do not share sensitive or confidential information through unencrypted or unsecured channels. Upon request, the CDN77 team can establish a secure communication channel for safe information exchange.

By participating in the program, you agree to follow these guidelines. Non-compliance may result in disqualification from the program or forfeiture of legal protections provided under safe harbor.

3. Scope

3.1. In scope

The program covers several areas crucial to our content delivery network operations. These include our CDN infrastructure, such as load balancing, edge servers, and reverse proxies. It also encompasses the security of our APIs and management interfaces, including authentication mechanisms and data access permissions. Customer data security, particularly data in transit and encryption mechanisms, is also a major focus, as is the integrity of our content delivery mechanisms, including bandwidth management and caching systems. Additionally, our corporate website or web applications, such as customer portals and analytics dashboards, are included in the scope of the program.

The CDN77 team is primarily focused on identifying and mitigating critical security vulnerabilities, including but not limited to issues such as:

- Server-Side Request Forgery (SSRF).
- Remote Code Execution (RCE).
- Ability to modify other customer accounts.
- Ability to obtain sensitive information.
- Stored Cross-Site Scripting (XSS) resulting in the ability to obtain or modify customer data.
- Reflected XSS resulting in the ability to obtain or modify customer data.

Nevertheless, all reported vulnerabilities will be evaluated individually, with the assessment and response determined based on the overall impact of each specific case.

3.2. Out of scope

Certain areas are out of scope, such as social engineering attacks, denial of service (DoS) or distributed denial of service (DDoS) attacks, brute-force attacks on non-sensitive endpoints, and vulnerabilities found in third-party platforms not controlled by us. The testing of any vulnerabilities outside the defined scope is strictly prohibited and will result in disqualification from eligibility for legal safe harbor protections.

The following issues are out of scope and will not be considered as security vulnerabilities:

- Clickjacking on pages with no sensitive actions.
- Cross-Site Request Forgery (CSRF) on unauthenticated forms or forms without sensitive actions.
- Attacks requiring man-in-the-middle (MITM) or physical access to a user's device.
- Previously known vulnerable libraries without a working Proof of Concept (PoC).
- CSV injection without demonstrating an actual vulnerability.
- Missing best practices in SSL/TLS configuration.
- Any activity that could result in service disruption, including DoS.
- Content spoofing and text injection issues without an exploitable attack vector.

- Rate limiting or brute force issues on non-authentication endpoints.
- Missing best practices in Content Security Policy (CSP).
- Missing email best practices (e.g., SPF/DKIM/DMARC records).
- Vulnerabilities that only affect users of outdated or unpatched browsers (fewer than 2 stable versions behind).
- Software version disclosure, banner identification issues, or descriptive error messages (e.g., stack traces).

4. Reports of vulnerabilities

When submitting a vulnerability report, ensure it includes a clear title, a detailed description of the vulnerability, steps to reproduce it, an explanation of its potential impact, and, if possible, suggestions for mitigation. We do not accept video-only proof of concepts, nor will we accept reports that only contain automated scan outputs, such as BurpSuite or nmap scan results. Each report should focus on a single vulnerability unless multiple vulnerabilities must be chained to demonstrate the impact.

If duplicate reports of the same vulnerability are submitted by multiple researchers, only the first fully reproducible submission will be considered. However, if subsequent reports provide additional information or context that significantly enhances the understanding or impact of the vulnerability, such contributions may also be acknowledged at the discretion of the program administrators.

Multiple vulnerabilities caused by the same underlying issue will be treated as one. Reports must detail verifiable and reproducible vulnerabilities to be considered in-scope.

A valid vulnerability report should include:

- A clear description of the attack scenario.
- A detailed description of the vulnerability.
- Step-by-step instructions to reproduce the issue, with screenshots if they enhance clarity.
- An explanation of the security impact.
- A minimized test case.
- A demonstration that the exploit is likely.

Reports should be concise, well-written, and limited to essential details. Reporters are expected to be responsive to engineers working to resolve the bug. Including a suggested patch, if available, can help clarify the issue.

Vulnerability reports should avoid:

- Crash dumps or stack traces without symbols.
- Reports lacking a Proof of Concept (PoC) or containing a poor-quality PoC, such as a large fuzz file dump with no reduction effort.
- SSL/TLS scan reports or outputs from services like SSL Labs.

Reports can be submitted via our dedicated vulnerability submission email at bugbounty@cdn77.com.

5. Response Targets

CDN77 will make a best effort to meet the following Service Level Agreements (SLAs) for security researchers participating in its program:

- First Response: Within 3 business days.
- Time to Triage: Within 7 business days.
- Time to Resolution: Dependent on the severity and complexity of the reported issue.
- Time to Bounty: Within 15 business days.

These targets are provided as best-effort guidelines and may be subject to adjustment based on the nature and scope of the reported vulnerabilities.

6. Rewards

The reward structure for this program is based on the severity of the reported vulnerability, the potential impact, and the ease of exploitation. We utilize Bugcrowd's Vulnerability Rating Taxonomy as a general guideline for rating and categorizing vulnerabilities. However, this taxonomy is intended as a reference only, and we reserve the right to decline certain reports if the identified issue is not significant within our specific context. If any vulnerabilities are stated in these Program Terms as out of scope while being categorized as a vulnerability in Bugcrowd's Vulnerability Rating Taxonomy, the Program Terms take precedence. We reserve the right to adjust bounty awards based on the proven impact of the vulnerability. This ensures that reports demonstrating a significant, real-world effect will be compensated accordingly, while reports identifying issues without measurable impact or without relevance to our specific context may receive lower compensation or no reward.

The total rewards issued to an individual researcher or group of researchers within a month shall not exceed $5000.

We encourage researchers to focus on the proven impact of their findings to maximize potential rewards and minimize unnecessary back-and-forth discussions.

To provide clarity, the typical bounty for each severity level is outlined below. Please note that these amounts serve as approximate ranges, and final rewards will be determined at our discretion based on the demonstrated impact of the vulnerability.

The approximate rewards for various vulnerability categories are listed below:

Technical Severity	Reward
P1	$2000 - $3,000
P2	$1000 - $2,000
P3	$500 - $1,000
P4	$250 - $500
P5	$100 - $250

7. Safe Harbor

We offer legal safe harbor for participants acting in good faith. This means we will not pursue legal action against individuals who follow these Program Terms, including rules on responsible disclosure and scope, provided that they report the vulnerabilities through our Bug Bounty Program.

There are certain ineligibilities, such as vulnerabilities identified through automated tools without an exploitation path, DoS attacks, and issues found in third-party services not operated by our CDN provider. Any attacks on out-of-scope areas are ineligible for legal safe harbor.

8. Intellectual Property

By participating in the Bug Bounty Program or by submitting any report, disclosure, or information to CDN77, you acknowledge and agree that all intellectual property rights arising from or related to CDN77's technology, including without limitation all vulnerabilities, shall be solely and exclusively owned by DataCamp Limited. You grant DataCamp Limited an irrevocable, perpetual, worldwide, transferable, sublicensable, royalty-free license to use, copy, modify, create derivative works of, and otherwise exploit any and all intellectual property arising from or related to your participation in the Bug Bounty Program and/or submission, for any purpose. You represent and warrant that your participation in the Bug Bounty Program and/or submission is original to you, that you have not used or incorporated any third-party intellectual property without proper authorization, and that you have the legal right to participate in the Bug Bounty Program and make the

submission.

9. **Confidentiality**

Any information you receive or collect regarding our company, services, customers, affiliates, users, employees, or agents in connection with the Bug Bounty Program ("Confidential Information") must be treated as strictly confidential. Such Confidential Information shall only be used for purposes directly related to the Bug Bounty Program. You are expressly prohibited from using, disclosing, or distributing any Confidential Information, including, but not limited to, information related to your submission, without obtaining our prior written consent. Written consent must be obtained by submitting a formal disclosure request to bugbounty@cdn77.com. Please be advised that not all requests for public disclosure will be granted.

10. **Privacy**

Any collection, processing, and use of your information is described in the CDN77 Privacy Statement.

11. **Modifications**

We reserve the right to modify these Program Terms or terminate the Bug Bounty Program at any time, at our sole discretion. Any changes to the Program Terms will be posted on our official site, and your continued participation following such modifications constitutes acceptance of the revised terms.