MICROBLINK

Public

Bug Bounty Policy

At Microblink, we take security seriously and value the contribution of security researchers in identifying vulnerabilities that help us secure our systems and protect our users. Our Bug Bounty Program is designed to reward responsible disclosure of vulnerabilities that could impact the security of our products, services, or data.

If you've discovered a security issue, we'd love to work with you to resolve it. This document outlines how to participate in our program, what is in scope, exclusions, and how rewards are determined.

Scope

The following assets are eligible for testing under this program:

- *.microblink.com (all subdomains)
- Microblink APIs
- Microblink mobile applications
- Any other explicitly stated assets communicated by Microblink as part of this program.

Out-of-scope assets

The following are excluded from the scope of this program:

1. **Non-exploitable issues:**
    - Missing security headers (e.g., CSP, X-Frame-Options) without demonstrable impact.
    - SPF / DKIM / DMARC misconfigurations without evidence of exploitability.
    - Self-XSS vulnerabilities requiring user interaction.
2. **Theoretical vulnerabilities:**
    - Issues that cannot be practically exploited.
    - Vulnerabilities requiring unlikely user behavior or unrealistic attack scenarios.

3. **Third-party services:**
    - Vulnerabilities in third-party platforms or services not owned by Microblink (even if on Microblink domains).
4. **Denial of service (DoS) attacks:**
    - Submissions related to DoS attacks or resource exhaustion.
5. **Other exclusions:**
    - Reports resulting from automated scanning tools without clear proof of concept (PoC).
    - Username enumeration on login or password reset pages.
    - Outdated software / library versions without a demonstrable exploit.
    - Clickjacking without a specific exploit.
    - Mail configuration issues (e.g., SPF / DKIM / DMARC settings).
    - CAA DNS record issues (absence or misconfiguration).
    - Publicly accessible login panels or autocomplete functionality in non-sensitive form fields.
    - Unsafe or deprecated TLS / SSL algorithms and configurations (e.g., support for SSLv2 / SSLv3, RC4, 3DES, export-grade cyphers, weak signature algorithms like MD5, TLS compression, or protocols vulnerable to attacks such as BEAST, POODLE, FREAK, Logjam, DROWN, Sweet32.
    - Sensitive information disclosure reports that only involve information already publicly available or not considered confidential will not be eligible for a reward.

How to submit a report

To submit a vulnerability report, send an email to our dedicated security team at security@microblink.com. Please include the following details in your submission:

1. A clear description of the vulnerability.
2. Steps to reproduce the issue, including any necessary credentials or accounts used during testing.
3. Proof of concept (PoC) demonstrating the exploitability of the vulnerability.
4. The potential impact of the vulnerability if exploited.
5. Recommendations for remediation (optional).

We will acknowledge receipt of your vulnerability report within 14 days. Our security team will review your submission and provide an initial assessment or follow-up within 14 days of your report.

Program rules

To participate in our Bug bounty program, you must adhere to the following rules:

1. Do not exploit any vulnerabilities beyond what is necessary to demonstrate the issue.
2. Avoid accessing, modifying, or deleting any data during testing.
3. Do not publicly disclose any vulnerabilities before they are resolved by Microblink.
4. Testing must be limited to in scope assets only.
5. Do not use automated tools excessively or perform denial of service attacks.
6. Avoid social engineering, phishing, or physical attacks against Microblink employees or infrastructure.

Failure to comply with these rules may disqualify you from receiving rewards.

Safe harbor

Microblink supports ethical hacking efforts and will not pursue legal action against researchers who:

1. Follow this program's scope and rules.
2. Report vulnerabilities responsibly without exploiting them maliciously.
3. Avoid causing harm or disruption during testing.

If you inadvertently access proprietary data during testing, report it immediately and do not store, share, or use it in any way.

Rewards

We offer monetary rewards based on the severity and impact of validated vulnerabilities

Severity Level	Reward Amount (USD)	Examples
Low	$25 — $49	Information disclosure with limited impact (e.g., non-sensitive metadata exposure); minor security issues with demonstrable, but low, impact
Medium	$50 — $99	Reflected XSS with practical exploitability; access control issues allowing unauthorized access to non-sensitive data; open redirects with demonstrated risk
High	$100 — $500	Remote code execution; privilege escalation; unauthorized access to sensitive data; authentication bypass; significant business logic flaws

Severity is determined using industry standard frameworks such as OWASP guidelines and CVE details. The final reward amount is at Microblink's discretion and may vary based on the quality and impact of the submission.

Response timeline

Stage	Timeframe
Acknowledgment of receipt	Within 14 days
Initial assessment/follow-up	Within 14 days

Payment process

Once a vulnerability report is validated and accepted:

1. We will confirm the reward amount with you via email.
2. You will be required to sign a Non-Disclosure Agreement (NDA) prior to payment.
3. Payment will be issued via Paypal after the NDA has been signed.

If you do not sign the NDA within seven business days, we will send a follow-up reminder. If there is no response after an additional three business days, the reward will be forfeited.

Legal terms

By participating in this program:

- You agree to abide by all applicable laws and regulations.
- You agree to keep all information about the vulnerability confidential and not to disclose it to any third party without our written consent.
- Eligibility for rewards is determined at Microblink's sole discretion.

Microblink reserves the right to modify this program at any time without prior notice.

Contact us

If you have any questions about this program or need clarification regarding the scope or exclusions, please contact us at security@microblink.com.

We appreciate your efforts in helping us maintain a secure environment for our users.