Bug Bounty Program

Welcome to the Bug Bounty Program at Blockscout! Ensuring the safety of our platform is a top priority, and we greatly appreciate thecrucial role security researchers play in contributing to open source . Should you identify a possible security vulnerability within our platform, we invite you to join our bug bounty program and share your findings.

How to report a security vulnerability

Send us an email with the information below. We ask that you please keep your findings confidential during the reporting process. We will get back to you with our diagnosis or additional comments/questions within 10 days.

1. Description of the bug/vulnerability
2. Clearly describe the vulnerability you've discovered.
3. Steps to reproduce
4. Outline the steps needed to replicate the vulnerability.
5. Impact analysis
6. Assess the potential impact of the vulnerability on users, developers, and the organization.
7. Code fix (optional)
8. If possible and appropriate, you may include a suggested code fix for the vulnerability.
9. Type of vulnerability
10. Choose a label that best fits the category of the bug for classification purposes. This aids in rewards distribution and participation.
11. Additional Context
12. Provide any additional information that could help in understanding and resolving the issue.
13. Email your report
14. Email your report tosecurity@blockscout.com

Information is also available on theSECURITY page of our Github Repo .

Rewards

If you are the first person to report the issue and we make a code or configuration change based on your findings, we will reward you with a bounty and mention in our Security Hall of Fame ! Issue risk level is determined by our team.

1. Critical Risk
2. : Up to 6000 in crypto equivalent.
3. High Risk
4. : Up to 1000 in crypto equivalent.
5. Moderate Risk
6. : Up to 500 in crypto equivalent.
7. Low Risk
8. : Up to 100 in crypto equivalent.
9.

All bounty researchers will be acknowledged (at your discretion) for your efforts in our documentation.

Bounty Considerations

Vulnerabilities in the following areas are eligible for bounty consideration.

- Business logic bugs or problems
- Remote code execution (RCE)
- Database vulnerability, SQLi
- File inclusions (Local & Remote)
- Access Control Issues (IDOR, Privilege Escalation, etc)
- Sensitive information leaks
- Server-Side Request Forgery (SSRF)
- Other vulnerability with a clear potential loss
-

Out of Scope Items

Unless presenting a serious business risk (at our discretion), the following are typically not eligible for rewards:

- Minor visual bugs, spelling errors, etc.
- Social engineering tactics (e.g., phishing)
- Issues in applications or systems not listed in the scope
- UI/UX bugs, data entry errors, and typos

- Network level Denial of Service (DoS/DDoS) vulnerabilities
- Certificate/TLS/SSL issues
- DNS configuration problems
- Server configuration issues (open ports, TLS configurations, etc.)
- Spam or social engineering techniques
- Security flaws in third-party apps or services
- Non-impactful XSS exploits
- CSRF-XSS issues related to login/logout
- Issues related to https/ssl or server-info disclosure
- Mixed Content Scripts
- Brute Force attacks
- General best practices concerns
- Recently disclosed 0day vulnerabilities
- Username/email enumeration via error messages
- Missing HTTP security headers
- Weak password policies
- HTML injection
-

Security Hall of Fame

Thank you for your help keeping vital public infrastructure like block explorers safe and secure! * blackgrease:https://github.com/blackgrease *

Last updated6 months ago