Fauna Bug Bounty Program Policy

We believe our user community and unaffiliated security researchers play an important role in helping to keep Fauna and our customers secure. If you think you have found a security issue in any component of the services listed please inform us by sending an email to **security@fauna.com**. Full program details follow.

In Scope Assets

Domain	Identifier In-Scope Bounty	In Scope	Bounty
Service	https://dashboard.fauna.com/accounts/login	Yes	Yes
Service Registration	https://dashboard.fauna.com/accounts/register	Yes	Yes
API	Fauna supports both Fauna Query & GraphQL. Interaction with Fauna through FQL is via the Fauna Command Line shell, Web shell or Drivers. https://docs.fauna.com/fauna/current/api/fql/ GraphQL Endpoints: https://docs.fauna.com/fauna/current/api/graphql/endpoints	Yes	Yes

Testing Phase

- Provide your IP address in the bug report. We will keep this data private and only use it to review logs related to your testing activity.
- Include a custom HTTP header in all your traffic. Burp and other proxies allow the easy automatic addition of headers to all outbound requests. Report to us what header you set so we can identify it easily
- Social engineering (e.g. phishing, vishing, smishing) is prohibited
- Make a good faith effort to avoid 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
- Under no circumstances should any of our users be made aware that you are running a test. You may create test accounts, test user accounts, or create other test data in order to carry out your tests
- Automated security testing against the site or services is not allowed
- If private customer data is accessed during your security testing, please notify us immediately. Additionally, while testing, take measures to avoid accessing customer data or affecting customer experiences
- Don’t perform any attack that could harm the reliability/integrity of our services or data. DDoS/spam attacks are not allowed

Reporting Phase

Please submit reports to security@fauna.com and direct all subsequent correspondence to the security team. Contacting our support team about the status of a report will result in an immediate disqualification for a bounty for that report.

Please include the following information in a vulnerability report:

- Description of the vulnerability
- Steps to reproduce the reported vulnerability
- Proof of exploitability (e.g. screenshot, video)
- Perceived impact to another user or the organization
- Proposed CVSSv3 Vector & Score
- List of URLs and affected parameters
- Other vulnerable URLs, additional payloads, Proof-of-Concept code
- Browser, OS and/or app version used during testing
- Proposed remediation

Bounty Phase

- When a report has been received from another researcher and is in the process of being remediated, we only award the first report that was received
- Recently disclosed 0-day vulnerabilities are not eligible until one week after public disclosure
- Multiple vulnerabilities caused by one underlying issue will be awarded a single bounty

Bounty Severity Matrix

Our rewards are based on severity. Please note these are general guidelines and final bounty amounts are at the discretion of Fauna. Note that Fauna's Security team may choose to accept the risk posed by some vulnerabilities, and these will not be eligible for a paid bounty.

P1 - Critical, Maximum Bounty $1000
Examples - Server Security Misconfiguration, Authentication Bypass, File Inclusion, Remote Code Execution, XXE, Disclosure of secrets,, Command injection
P2 - High, Maximum Bounty $500
Examples: Oauth misconfiguration, Cross site scripting, User Enumeration with Sensitive Personal Information, Credentials on GitHub, Confidential Information Exposure
P3 - Medium Severity Bugs $250
Examples: DNS misconfiguration, Exposed Administrative Interface, Cleartext Submission of Passwords, 2FA Bypass
P4 - Low Severity Bugs $100
Examples: Debug information, CAPTCHA Bypass, Issues Affecting Single Users, Bugs Requiring Man-in-the-Middle (MithM), DBMS misconfiguration, no password policy
P5 - Acceptable Risk Bugs $0
Examples: Non-exploitable weaknesses and "won't fix" vulnerabilities.

Out of Scope Vulnerabilities

The following issues are considered **out of scope and are not eligible for a bounty**:

- Missing autocomplete attributes
- SSL/TLS scan reports
- XSS in files not developed by Fauna (e.g. third-party ads)
- Missing security-related HTTP headers which do not lead directly to a vulnerability
- Non-critical issues that affect only outdated browsers
- Denial of Service vulnerabilities (DoS)
- Cross-site Request Forgery (CSRF) with minimal security implications
- "Advisory" or "Informational" reports that do not include any Fauna-specific testing or context
- Vulnerabilities requiring physical access to the victim's unlocked device
- Bugs that don't affect the latest major version of modern browsers (Chrome, Firefox, Edge, Safari)
- Bugs that require exceedingly unlikely user interaction
- Disclosure of public information and information that does not present a significant risk
- Vulnerabilities that allow usernames to be enumerated
- Brute-Force attack
- Email Spoofing
- Javascript errors
- Rate Limit related issues. example- missing rate limit for password
- Password complexity & weak password security
- IDN homograph attack

Payment Method

Fauna issues bounty payments electronically through either PayPal or Bank transfer. If submissions are eligible for bounty payments our Security team will coordinate payments.

Thank you for conducting research to help improve the security of Fauna's service.

Safe Harbor

Any activities conducted in a manner consistent with this policy will be considered authorized conduct, and Fauna will not initiate legal action against you.