Mailmeteor’s Vulnerability Disclosure Program

Mailmeteor fosters an open relationship with the security community, as we recognize the importance of application and data security. Our Vulnerability Disclosure Program demonstrates our commitment to security as a key value and to uphold our legal responsibility to good-faith security researchers who choose to help validate our applications.

Qualifying vulnerabilities

Any design or implementation issue that substantially affects the confidentiality or integrity of user data is likely to be within the scope of the program. Common examples include:

- Cross-site scripting;
- Cross-site request forgery;
- Mixed-content scripts;
- Authentication or authorization flaws;
- Server-side code execution bugs.

Reporting a Vulnerability

Any vulnerabilities you may find should be reported to our security team via an email sent to the following address: security@mailmeteor.com. To ensure confidentiality, we encourage you to encrypt any sensitive information you send us.

Bounties

The decision to pay a reward is entirely at our discretion. You must not violate any law. You are responsible for any tax implications or additional restrictions depending on your country and local law. We reserve the right to cancel this program at any time.

Disclosure

In order to protect our customers, TINT requests that you not post or share any information about a potential vulnerability in any public setting until we have researched, responded to, and addressed the reported vulnerability and informed customers if needed.

Disclaimer

The content contained herein is correct as of April 2022, and represents the status quo as of the time it was written. Mailmeteor's security policies and systems may change going forward, as we continually improve protection for our customers.

Make sure to regularly check our Privacy Policy and Security Center to stay up to date.