Sensibull Bug Bounty Program

We try our best to keep all platforms of Sensibull secure, and make every effort to keep on top of the latest threats by working with our inhouse security team and external security consultants. If you are able to spot any security issues or vulnerabilities, please send reports to security@sensibull.com

Please note that the Bug bounty program is only for reporting valid security bugs. For reporting any application related issues, please visit our Support portal and create a ticket.

We would like to continuously build relationships and work with as many security technology enthusiasts as possible, and fairly reward any such issues spotted as well.

Rewards

We will reward reports according to the severity of their impact on a case-by-case basis as determined by our security team. We may reward more for unique, hard-to-find bugs; we may also reward less for bugs with complex prerequisites that have lower risk of exploitation of our platforms or are more seen to be as good practices to be implemented.

Issues like Clickjacking, Social Engineering, DDOS, Missing CAA DNS entries , DMARC DNS settings, Jailbreak detection, Lack of obfuscation, Lack of root detection etc will not be eligible for any reward. Rate limits bounties and application constraint bypass via parallel requests are only considered if it causes a loss to business or customer data or if there is potential monetary loss.

How to report a bug

To participate in Sensibull's Bug Bounty Program, please send reports to security@sensibull.com

All accepted bug reports would be required to accept a non-disclosure agreement, and share their PAN, bank account details & their address (for tax and compliance purposes), to further receive any bug bounty rewards. All reward payments are also subject to tax deducted as source.

Responsible disclosure

The identified bug can be reported to security@sensibull.com

Program scope

Our platforms, applications & website URLs, that belong to Sensibull:

- https://sensibull.com/
- https://web.sensibull.com

Android application:

- https://play.google.com/store/apps/details?id=com.sensibull.mobile

iOS application:

- https://apps.apple.com/us/app/sensibull-for-options-trading/id1534984988

Exclusions:

- Any staging/QA environments of Sensibull are only eligible for severe issues like root access of the host , leaking sensitive information or infrastructure details etc.

Infra and network security

Open network ports, open services other than public HTTP Endpoints etc. DoS and DDoS tests ARE PROHIBITED.

All the bounty rewards will be paid based on an internal assessment by our security team. Based on the severity, we will revert within 1-7 business days, and communicate whether the bug report was accepted/declined and the steps forward including the payment of the reward.