GILDED

Bug Bounty Program

Gilded considers privacy and security to be core functions of our platform. Earning and keeping the trust of our users is our top priority, so we hold ourselves to the highest privacy and security standards. If you have discovered a security issue that you believe we should know about, we would love to work with you.

Please let us know about it and we'll make every effort to quickly correct the issue.

Vulnerabilities

In scope

We use the CVSS calculator to determine severity. Bounties are rewarded based on severity.

The following areas are generally considered of Critical severity:

- Stored cross-site scripting (XSS) vulnerability
- Remote code execution
- File system access

The following areas are generally considered to be High severity:

- Privilege escalation (for example, seeing something that should be locked or editing something that shouldn't be editable) or authentication issues
- Cross-Site Request Forgery (CSRF) on user data
- Sensitive data sent unencrypted (for example, with HTTP and not HTTPS)

The following areas are generally considered to be Medium severity:

- Vulnerabilities when uploading CSVs
- Insecure TLS configuration when a fix would be backwards-compatible
- Lack of `secure` or HTTP-only flags on sensitive cookies

The following areas are generally considered to be Low severity:

- Self-XSS (XSS), a user performing XSS on themselves only
- Leaking the `Referer` header when leaving Gilded, disclosing sensitive information
- On a case-by-case basis, issues with publicly-available malicious browser extensions that capture user data
- On a case-by-case basis, exploits for legacy browsers (any version of Internet Explorer or any version of Chrome/Firefox/Safari/Chromium/Opera/Edge that is not the latest)

See below for more on third-party vulnerabilities.

Out of scope

We generally do not accept reports that are simply the output from an automated security scanner (even lightly annotated). Feel free to use security scanners, but please don't copy-paste their output into our program without additional insight.

If a report is a duplicate, we won't award a bounty or reputation. A report is a duplicate if our other security review processes have already identified the issue.

A specific vulnerable behavior found in one part of Gilded is not necessarily eligible for a bounty if an identical problem is uncovered in another part of the Gilded, though we'll assess this on a case-by-case basis. If the same vulnerability affects multiple parts of the product, please let us know in a single report—we'll take that into consideration when assessing severity (such a vulnerability might be eligible for a higher reward), and when marking reports as resolved. For example, if we fail to sanitize URLs in five parts of the Gilded product, that should probably be one report, not five.

The following areas are always out of scope:

- blog.gilded.finance
- invest.gilded.finance
- support.gilded.finance

Attacks that are beyond Gilded's control are generally out of scope. These include:

- Man-in-the-middle (MITM) attacks outside of Gilded's control (for example, modifying traffic by controlling a wireless router)

- Attacks requiring access to a user's device (such as physical access or remote access)
- Attacks requiring the user's credentials
- Exported CSV files that can execute commands in Excel, Numbers, Google Sheets, or other CSV programs
- Exploits requiring users to modify code running on their own device (opening up browser developer tools and running commands, for example)

We also ask for an exploit or proof of concept for reports. If you can't produce an attack, even a hypothetical one, we are unlikely to award a bounty. For example, here are some areas we generally consider to be out of scope:

- Arbitrary file upload (which is a Gilded feature)
- Mis-adherence to best practices that does not lead to an exploit
- Vulnerabilities in third-party code or services that do not lead to an exploit
- Generic information disclosure, such as the `Server` or `X-Powered-By` headers
- Missing HTTP security headers, such as:
    - Content-Security-Policy
    - Feature-Policy
    - HTTP Strict Transport Security
    - HTTP Public Key Pinning
    - X-Content-Type-Options
    - X-XSS-Protection
    - Referrer Policy
    - P3P
    - Certificate Transparency (Expect-CT)
    - X-Download-Options
    - X-DNS-Prefetch-Control

We also consider the following areas to be out of scope, though there may be some exceptions:

- Social engineering (phishing) of Gilded staff or users
- Username or email enumeration
- Denials of service scoped to a single user or workspace
- API key disclosure for third-party services
- Changing the `Host` header to cause redirects
- Missing subresource integrity

- Email security: DMARC, DKIM, SPF
- DNSSEC
- Session cookie duration
- Session expiration after logout
- Issues related to password policies
- Disclosure of non-sensitive internal IDs (such as user IDs)
- Two-factor authentication (2FA) bypass with third-party sign-ins like Google

If you're not sure whether an issue is in scope, we'd appreciate it if you file a report anyway!

Third party issues

Gilded uses several third party services. If they have vulnerabilities, we'd like to know. We can't guarantee bounty for those but we encourage you to report issues to both us and to them.

If the vulnerability might reasonably affect our users, we'll likely grant a bounty. The bounty amount will be determined on a case-by-case basis due to possible difficulties assessing the true severity of the issue. As such, vulnerabilities in third-party services are *not* eligible for the default bounty amounts listed in the "Areas in scope" section above, and the bounty amount will be determined on a case-by-case basis.

Disclosure guidelines

Do not disclose any issues to the public or to any third party without Gilded's permission. If you have questions, please ask us.

Rewards

Critical	High	Medium	Low
$500	$250	$100	$50

Bug bounty rewards are payable in BTC or ETH