# Sherlock Bug Bounty Platform Rules

In order to facilitate cordial and productive exchanges between protocol customers and whitehats, Sherlock has established a set of rules for whitehats and protocol customers to define proper conduct.

Breaking these rules as a whitehat could result in removal or ban from the Sherlock platform and/or withholding of payout.

Breaking these rules as a protocol team could result in removal from the Sherlock platform and/or provide cause for breakage of the mutually signed agreement.

## Whitehats

### Ethical Standards

- Adhere to ethical standards and legal guidelines. Any actions that compromise the integrity, privacy, or availability of systems beyond what is necessary for testing are strictly prohibited.
- No harm: Ensure that your testing does not negatively impact users or infrastructure.
- Always default to the assumption that the protocol team has good intentions.
- Do not threaten, blackmail, dox, or otherwise create a negative environment for the protocol customer.
- Do not communicate with the protocol customer outside of the official channel provided by Sherlock
- By submitting a vulnerability through Sherlock, you are agreeing to abide by the outcome of the Sherlock dispute resolution process

### Testing Environment

- Replicating tests on public mainnet or testnet is prohibited. All testing should be conducted on local forks of either testnet or mainnet.
- Use only authorized environments for testing to avoid any unintended disruptions or security risks.
- Avoid testing with external dependencies and third-party systems not controlled by the protocol customer to avoid any leaks of the potential vulnerability

### Service Disruptions

- Any denial of service attacks that are executed against project assets are strictly forbidden.
- Automated testing of services that generates significant amounts of traffic is not permitted.

### Vulnerability Disclosure

- Do not publicly disclose vulnerabilities before they are resolved. Reports must be submitted through the Sherlock platform, and we will notify you when it is safe to disclose.
- Do not discuss (publicly or otherwise) any aspect of a submitted vulnerability without consent from the protocol customer
- Report via Sherlock: Use the official reporting channels to submit your findings.
- Never exploit a vulnerability or threaten to do so
- Do not attempt to rescue funds without the written consent of the protocol customer
- Publicly known bugs or bugs reported in a previous audit are never eligible for payout or reimbursement of deposit

### Payouts

- Do not try to cajole a protocol customer into paying you. Always use the provided Sherlock resolution mechanisms.

## Protocol Customers

### Ethical Standards

- Do not communicate with the whitehat outside of the official channel provided by Sherlock.
- Do not pay whitehats who submit bugs on Sherlock outside of Sherlock's designated channel or without Sherlock's consent.
- Do not claim a bug report is a known or duplicate issue without clear evidence of where it was publicly available before the whitehat's submission timestamp.
- Always default to the assumption that the whitehat has good intentions.
- By listing your bug bounty program on Sherlock, you are agreeing to abide by the outcome of the Sherlock dispute resolution process.