Vunerability Disclosure Policy

Summary

Security is core to our values, and we value the input of external security researchers acting in good faith to help us maintain a high standard for the security privacy of our users and systems. This policy sets out our definition of good faith in the context of finding and reporting security vulnerabilities, as well as what you can expect from us in return for your effort, skill, and dedication.

Reporting

Email your findings to security@shiftbase.com. Encrypt your findings using our PGP Key to prevent this critical information from falling into the wrong hands.

In Scope Domains

The following domains are considered within scope:

- https://app.shiftbase.com
- https://api.shiftbase.com

Rules & Guidelines

- Do not attempt to gain access to another user's account or data.
- Do not perform any attack that could harm the reliability/integrity of our services or data.
- Do not publicly disclose a vulnerability before it has been fixed.
- Only test for vulnerabilities on domains in scope.
- Do not impact other users with your testing, this includes testing for vulnerabilities in accounts you do not own.
- Automated scanners or automated tools to find vulnerabilities are forbidden and will be blocked.
- Never attempt non-technical attacks such as social engineering, phishing, or physical attacks against our employees, users, or infrastructure.
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

Issues not to report

The following are considered out of scope for our security program and will not be rewarded:

- CSRF on forms that are available to anonymous users
- Disclosure of known public files or directories (e.g. robots.txt)
- Domain Name System Security Extensions (DNSSEC) configuration suggestions
- Banner disclosure on common/public services
- HTTP/HTTPS/SSL/TLS security header configuration suggestions
- Lack of Secure/HTTPOnly flags on non-sensitive cookies
- Logout Cross-Site Request Forgery (logout CSRF)
- Phishing or Social Engineering Techniques
- Presence of application or web browser 'autocomplete' or 'save password' functionality
- Denial of Service (DDoS)
- Email related DNS configuration (e.g. DMARC / SPF / DKIM) Records on shiftbase.com
- Attacks involving stolen credentials or physical access to endpoint devices
- Issues present in older versions of browsers, plugins, or any other software
- Low Severity Clickjacking Vulnerabilities

Reward range and classification

Shiftbase may, at its sole discretion, provide rewards to eligible reporters of qualifying vulnerabilities. *High* and *Medium* vulnerabilities are the only ones entitled to a monetary reward (of up to €500). *Duplicate* and *Declined* submissions as well as any P5 (according to Bugcrowd's Taxonomy) submissions do not receive any rewards for this program. The following table outlines the categories that will result from our evaluation:

Evaluation	Description
Declined	False positives and/or very minor criticality that won't necessarily result in a change of code.
Duplicate	Same report has been made before or we are aware of the issue from any other source.
Low	Vulnerabilities like insecure cookies, clickjacking or insufficient password complexity are generally of low criticality as they are dependant of other issues and cannot be exploited by themselves.
Medium	Cross-site request forgery (XSRF or CSRF) vulnerabilities or those that might result in the changing of users data.
High	Vulnerabilities of high criticality are those that would result in bypassing authentication. An example of a high critical vulnerability is a successful SQL-injection that could be used to read data, delete users, or other kinds of database modifications.

⚠ Reports from individuals who we are prohibited by law from paying are ineligible for bug bounties. You are responsible for paying any taxes associated with bug bounties. Any bug bounties that are unclaimed after 12 months will be donated to a charity of our choosing.

Our promise to you

- We will respond as quickly as possible to your submission.
- We will keep you updated as we work to fix the vulnerability you submitted.
- We will not take legal action against you if you play by the rules.
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise)

Fine print

This is not a competition, but rather an experimental and discretionary rewards program. We may modify the terms of this program, terminate this program at any time, or not pay a reward entirely at our discretion.