Settle Bug Bounty Program

The scope for Settle's Bug Bounty program includes most of our assets; if it is not explicitly out of scope and there is a security impact, we want to know about it. Issues without security impact that are submitted to our program will be closed. Please review the program's Out of Scope section and all other policies before submitting a report.

Your participation in our Bug Bounty Program is voluntary. Before finding and reporting any vulnerabilities you are required to read and agree to the Bug Bounty Program Terms (the "Program Terms"). In these terms, references to "you" or "researcher" refer to a researcher that submits a high-quality report in accordance with the Settle Bug Bounty Program Terms and "we" or "us" refers to Settle.

I. Program Terms

1. Safe Harbor

Any activities conducted in a manner consistent with this policy will be considered authorised conduct, and we will not initiate legal action against you. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will make it known that your actions were conducted in compliance with this policy. Settle reserves all legal rights in the event of non-compliance with this policy.

2. Program Eligibility

To be eligible to participate in our Bug Bounty Program, you must:

- Be at least 18 years of age if you test using a Settle account.
- Not be employed by Settle or any of its affiliates or an immediate family member of a person employed by Settle or any of its affiliates.
- Not be in violation of any European Union or national law or regulation with respect to any activities directly or indirectly related to the Bug Bounty Program.

If (i) you do not meet the eligibility requirements above; (ii) you breach any of these Program Terms or any other agreements you have with Settle; or (iii) we determine that your participation in the Bug Bounty Program could adversely impact us, our affiliates or any of our users, employees or agents, we, in our sole discretion, may remove you from the Bug Bounty Program and disqualify you from receiving any benefit of the Bug Bounty Program.

3. Program Rules

Do:

- Do abide by these Settle Bug Bounty Program Terms.
- Do respect privacy and make a good faith effort not to access, process, or destroy personal data.
- Do be patient & make a good faith effort to provide clarifications to any questions we may have about your report.

- Do be respectful when interacting with our team, and our team will do the same.
- Do perform testing only using accounts that are your own personal/test accounts. By default, we expect your report to clearly reference your registered email address or mobile number.
- Do exercise caution when testing to avoid negative impact to customers and the services they depend on.
- Do stop whenever unsure. If you think you may cause, or have caused, damage with testing a vulnerability, report your initial finding(s) and request authorization to continue testing.

Do NOT:

- Do not leave any system in a more vulnerable state than you found it.
- Do not brute force credentials or guess credentials to gain access to systems.
- Do not participate in denial of service attacks.
- Do not upload shells or create a backdoor of any kind.
- Do not publicly disclose a Vulnerability without our explicit review and consent.
- Do not engage in any form of social engineering of Settle employees, customers, or partners.
- Do not engage or target any Settle employee, customer, or partner during your testing.
- Do not attempt to extract, download, or otherwise exfiltrate data that may have personal data or other sensitive data other than your own.
- Do not change passwords of any account that is not yours or that you do not have explicit permission to change. If ever prompted to change a password of an account you did not register yourself or an account that was not provided to you, stop and report the finding immediately.
- Do not do anything that would be considered a privacy violation, cause destruction of data, or interrupt or degrade our service.
- Do not interact with accounts you do not own.

4. Disclosure Policy and Confidentiality

Any data you receive, obtain access to or collect about Settle, Settle affiliates or any Settle users, customers, employees or agents in connection with the Bug Bounty Program is considered Settle’s confidential information ("Confidential Information").

Confidential Information must be kept confidential and only used: (i) to make the disclosure to Settle under the Settle Bug Bounty Program; or (ii) to provide any additional information that may be required by Settle in relation to the submitted report. No further use or exploitation of Confidential Information is allowed. Upon Settle's request, you will permanently erase all Confidential Information for any systems and devices.

You may not use, disclose or distribute any such Confidential Information, including without limitation any information regarding your Bug Bounty submitted report, without our prior explicit consent. You must get explicit consent by submitting a disclosure request to our program. Please note, not all requests for public disclosure will be approved.

Any unauthorized public disclosure will result in a program ban.

5. Legal

Settle reserves the right to modify the terms and conditions of this program, and your participation in the Program constitutes acceptance of all terms.

By making a Submission, you represent and warrant that the Submission is original to you and you have the right to submit the Submission.

By making a Submission, you give us the right to use your Submission for any purpose. Please check this site regularly as we routinely update our program terms and eligibility, which are effective upon posting.

II. Submitting Reports

1. Report Quality

High-quality submissions allow our team to understand the issue better and engage the appropriate teams to fix it. The best reports provide enough actionable information to verify and validate the issue without requiring any follow-up questions for more information or clarification.

- Check the scope page before you begin writing your report to ensure the issue you are reporting is in scope for the program.
- Think through the attack scenario and exploitability of the vulnerability and provide as many clear details as possible for our team to reproduce the issue (include screenshots if possible).
- Please include your understanding of the security impact of the issue. Our bounty payouts are directly tied to security impact, so the more detail you can provide, the better. We cannot payout after the fact if we don't have evidence and a mutual understanding of security impact.
- In some cases, it may not be possible to have all of the context on the impact of a bug. If you're unsure of the direct impact, but feel you may have found something interesting, feel free to submit a detailed report and ask.
- Video-only proofs-of-concept (PoCs) will not be considered.
- A vulnerability must be verifiable and reproducible for us to be considered in-scope.
- All reports must demonstrate security impact to be considered for bounty reward.

2. Out-of-Scope

In addition to the explicit Out of Scope list on our program page, reports of the following issues are also out of scope:

- Physical or social engineering attempts (this includes phishing attacks against Settle employees)
- Ability to send push notifications/SMS messages/emails without the ability to change content
- Ability to take over social media pages (Twitter, Facebook, Linkedin, etc)
- Negligible security impact
- Unchained open redirects

- Reports that state that software is out of date/vulnerable without a proof-of-concept
- Highly speculative reports about theoretical damage
- Vulnerabilities as reported by automated tools without additional analysis as to how they're an issue
- Reports from automated web vulnerability scanners (Acunetix, Vega, etc.) that have not been validated
- SSL/TLS scan reports (this means output from sites such as SSL Labs)
- Open ports without an accompanying proof-of-concept demonstrating vulnerability
- Subdomain takeovers - please demonstrate that you are able to take over the page by leaving a non-offensive message, such as your username
- Best practices concerns
- Protocol mismatch
- Rate limiting
- Exposed login panels
- Dangling IPs
- Vulnerabilities that cannot be used to exploit other users or Settle -- e.g. self-xss or having a user paste JavaScript into the browser console
- Missing cookie flags on non-authentication cookies
- Cross-site Request Forgery (CSRF) with minimal security implications (Logout CSRF, etc.)
- Reports that affect only outdated user agents or app versions -- we only consider exploits in the latest browser versions for Safari, FireFox, Chrome, Edge, IE and the versions of our application that are currently in the app stores
- Issues that require physical access to a victim's computer/device
- Stack traces
- Path disclosure
- Directory listings
- Banner grabbing issues (figuring out what web server we use, etc.)
- Enumeration/account oracles
- UUID enumeration of any kind
- Invite/Promo code enumeration
- Gift card enumeration
- Account oracles -- the ability to submit a phone number, email, UUID and receive back a message indicating a Settle account exists
- Distributed denial of service attacks (DDOS)

III. Bounty Awards

Previous bounty amounts are not considered a precedent for future bounty amounts. Bounty awards are not additive and are subject to change as our internal environment evolves. We determine the upper bound for security impact and award based on that impact.

When determining bounty amounts, we consider the security impact of any given issue -- things that influence security impact are the scale of exposure and the various mitigating and multiplying factors.

For example, an issue that impacts individual users and must be done within a small window of time could be considered less severe than an issue that impacts a large number of users that can be done at any time.

Bounty payouts and amounts, if any, will be determined by us in our sole discretion. In no event are we obligated to provide a payout for any Submission. The format, currency, and timing of all bounty payouts shall be determined by us at our sole discretion. You are solely responsible for any tax implications related to any bounty payouts you may receive.

We follow the following table as a guideline to determine reward amount. The exact amount may vary depending on the details of the report.

Minor (No commercial / operational impact)	NOK 200.00
Moderate (Limited commercial / operational impact)	NOK 400.00
Major (Definite commercial / operational impact)	NOK 1,000.00
Extreme (Immediate, large-scale commercial / operational impact)	NOK 2,500.00

If we receive several reports for the same issue, only the earliest valid report that meets requirements and provides enough actionable information to identify the issue may be considered for a bounty.

IV. Additional Info

1. FAQ

Can Settle provide me with a pre-configured test account?

If credentials are necessary to access any of our assets, this will be included in our policy page under test plan or test instructions. If you do not see any instructions about test accounts in our policy, none are available or provided.

What is required when submitting a report?

- Description of the issue
- Reproduction steps written out in text (with accompanying screenshots or demonstration video, if applicable)
- Concrete security impact
- Any other relevant information you think may be helpful in reproducing or solving the issue

What is an example of an accepted vulnerability?

Valid and accepted vulnerabilities would be the type of report that identifies a unique security impact on this program's specific scope. The report must also meet any submission criteria outlined in the policy, such as test plan instructions and a working proof of concept.