BASHROCK

Security and responsible disclosure

How to report a security vulnerability in bashrock.com, and what you can expect from us.

VERSION 1.0 · EFFECTIVE 18 OCTOBER 2026 · ENGLISH

Online version: https://bashrock.com/en/legal/security

Reporting a vulnerability

If you think you've found a security vulnerability in bashrock.com, please email info@karwanstark.se with "Security" in the subject line. Please include:

- what you found and where (addresses, parameters);
- how to reproduce it, step by step;
- what an attacker could achieve with it.

Reports in English or Swedish are welcome.

What we ask of you

- Tell us before you tell anyone else, and give us reasonable time to fix the issue.
- Test only as much as you need to show the issue. Don't access, change or delete data that isn't yours, and stop as soon as you reach any.
- Don't degrade the site for others: no denial of service, no spam and no high-volume automated scanning. The site's rate limits and security checks will block heavy automated traffic anyway.
- Don't use social engineering, phishing or physical attacks, and don't target our people, our suppliers or our hosting provider.

What you can expect from us

- We confirm that we've received your report within five working days.
- We keep you informed while we investigate and fix the issue.
- We won't take legal action against anyone who reports in good faith and follows this policy.
- With your permission, we credit you once the issue is fixed.

We don't pay rewards for reports.

Scope

In scope: bashrock.com and www.bashrock.com.

Out of scope: findings from automated scanners without a demonstrated impact; missing security headers or best practices without a concrete way to exploit them; rate limits and security checks that work as intended; vulnerabilities in services we use but don't run, which should be reported to their owners.

Machine-readable contact

Our contact details for security reports are also published in the standard format at /.well-known/security.txt.