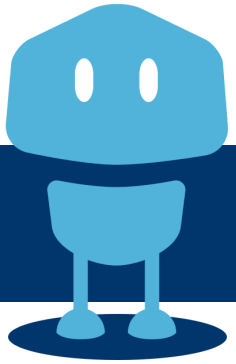
HYPERNODE®

by byte

Responsible Disclosure Policy



Responsible Disclosure Policy

At Byte we take the security of our servers, and our hosting platform, very serious. We understand that many of our customers entrust their most important data to us, and we strive to keep this data as secure as possible.
As such, we implemented this policy to offer a safe and secure way to report possible security, and further increase the security of our services. Working together we can ensure that all the services we offer, all information in our systems, and our clients' data, is as secure as possible.

Do's and Don'ts

- We accept reports for all the systems we use; All systems and services running under the byte.nl, hypernode.com and magereport.com domains. Any vulnerabilities on our clusterhosting environment, and on the Hypernode vagrant / docker setup, or generic Hypernode vulnerabilities, are also welcome.
- The testing of sites from our customers, including sites hosted under the testbyte.nl, or the hypernode.io domain, is **explicitly NOT ALLOWED**.
- Please don't use attacks on physical security, social engineering, (D)DoS, brute-forcing, or phishing. If you think you've found a vulnerability in any of the above fields, please contact us and we'll work on this together and see what our options are.
- If a reported vulnerability turns out to not be in our system, but in a third party's system, or in a system managed by one of our clients, we will forward the report to said party.
- Do not abuse found vulnerabilities. Don't download more information than is necessary to show the vulnerability.
- Changing or removing of data is not allowed. This includes scrubbing your own 'footprints', logfiles, history files, etc, etc.
- If, once a vulnerability is fixed, you wish to make a blogpost or some other sort of publication on this vulnerability, we would prefer to do so in collaboration.

What to do when you find a vulnerability

- Please report your findings via e-mail to security@byte.nl. If you feel the need, please use our PGP public key to encrypt your communications with us.
- Include all information that is needed to reproduce the problem, such as IP addresses, URLs, and arguments. Screenshots, HAR (HTTP Archive) files, and videos are also welcome. If you run across any customer data, or confidential information, during this process, please inform us of this as well.

- After reporting your findings please delete all acquired data/information.
- We ask you not to share and/or publish anything regarding your findings, until we've had the opportunity to fix the problem, and inform any possibly affected clients and/or third parties.

What you can expect of us.

- We will respond within 2 working days to your report, with an initial analysis and a plan to fix things.
- We will keep you informed of our progress in fixing the vulnerability.
- We will handle your report with strict confidentiality, and will not share any personal information without your permission, unless we are required to do so by law. If you would rather make a report under a pseudonym, that is also possible.
- We will not take any legal action against you, in regard to the report, as long as you have followed the instructions above.
- We will include a summary of your report, in a 'Hall of Fame' on our website.
- We will credit your name/pseudonym, with your permission, in all publications (Hall of Fame, blog posts, newsletter, or changelog) regarding this report.