Report Vulnerability

Have you discovered a vulnerability in our systems? We'd like to hear from you. Your assistance helps us enhance our services and their security.

You can report issues related to our online services, including (but not limited to):

Cross-site scripting
SQL injection
Cross-site Request Forgery (CSRF)
Weaknesses in authentication

Our Guidelines

When reporting a vulnerability to us, please adhere to the following rules:

- Act with integrity and avoid causing any damage during your investigation.
- Do not disrupt our services while investigating a vulnerability.
- Never disclose customer or our personal information.
- Do not share the vulnerability with others until it is resolved; instead, consult our experts and allow us time to address the issue.
- We only accept reports in English or Dutch.
- Do not employ attacks on (or with) physical security, social engineering, or hacking tools like vulnerability scanners.
- Do not insert a backdoor into any information system to demonstrate the vulnerability.
- Minimize the use of any weakness; only perform actions necessary to identify the vulnerability.
- Do not alter or delete any data from the system(s).
- Exercise caution when copying data.
- Do not make changes to system configurations.
- Avoid repeated attempts at password guessing or brute force attacks to gain system access.

Exclusions

We may choose not to reward reports for vulnerabilities with low or accepted risks. Examples of such vulnerabilities include:

- HTTP 404 codes or other non-HTTP 200 codes
- Placing plain text in 404 pages
- Release banners on public services
- Publicly accessible files and folders containing non-sensitive information
- Clickjacking on pages without a login function
- Cross-site request forgery (CSRF) on forms accessible anonymously
- Lack of 'secure'/'HTTP Only' flags on non-sensitive cookies

- Use of the HTTP OPTIONS Method
- Host Header Injection
- Absence of SPF, DKIM, and DMARC records
- Lack of DNSSEC
- Missing one or more of the following HTTP Security Headers:

  - Strict-Transport-Security (HSTS)
  - HTTP Public Key Pinning (HPKP)
  - Content-Security-Policy (CSP)
  - X-Content-Type-Options
  - X-Frame-Options
  - X-WebKit-CSP
  - X-XSS-Protection
  - After Reporting

Our security experts will investigate your report, and you'll receive an initial response within two business days. If your investigation inadvertently involves activities that may be prohibited by law, we will consider your intentions and adherence to the ruleset. We do not intend to press charges if your actions were in good faith. However, each situation will be assessed individually. We reserve the right to press charges if we suspect misuse of the vulnerability or data sharing with unauthorized parties.

Reward

For your efforts, we offer a small present or swag if your finding is not on the exclusion list. If we address vulnerabilities or make changes to our services based on your report, you may be eligible for compensation. The eligibility and compensation amount will be determined by us. If multiple reports concern the same vulnerability, the first reporter will receive compensation.

Privacy

When you submit a report, we may request your contact details (name, email, PGP public key, and telephone number). Rest assured that we do not share your information with third parties or use it for purposes other than resolving the reported vulnerability. The only exception is when we are legally obligated to do so, such as in the case of a judicial authority's request.

Third Parties

Please be aware of third-party (cloud) services, such as AWS, Microsoft, Google, etc., and their penetration testing policies before initiating your investigations.