Responsible disclosure

At Learnbeat, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present. If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

Contribute to our security

Vulnerabilities can be found in two ways: By accident when using our learning system regularly, or intentionally by looking for a security flaw. We would like to work with you to protect our customers and our systems.

Please do the following

- E-mail your findings to security@learnbeat.nl. Encrypt your findings using our PGP key to prevent this critical information from falling into the wrong hands,
- 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 not reveal the problem to others until it has been resolved,
- Do not use attacks on physical security, social engineering, distributed denial of service, spam, applications of third parties or other tools that have an impact on the availability of our systems.
- 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.

What we promise

- If you have followed the instructions above, we will not take any legal action against you with regards to the report,
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission unless required by law. Reporting under a pseudonym is possible,
- We will keep you informed of the progress towards resolving the problem,
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise), and
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The amount of the reward will be determined based on the severity of the leak and the quality of the report. We use the Common Vulnerability Scoring System Version 3.0 Calculator to determine this, but we reserve the right to deviate from this. Only reports that fall within the scope of this policy are eligible for a reward. Rewards are only awarded to EU/EER residents.
- We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

Scope

The following reports are outside the scope of this policy and are never eligible for a reward.

- In principle, we do not accept reports that are the result of an automated security scanner.
- If a reported issue has been reported previously, or is already known to us, we will not award a reward.
- This policy only applies to our web application, located at inloggen.learnbeat.nl and login.learnbeat.com except file uploads

- Attacks that are out of Learnbeat's control are generally out of scope. Among which:
    - Man-in-the-middle-attacks (MITM)
    - Attacks which require access to the device of an user (for example physical access or external access)
    - Attacks that need the credentials of an user
    - Exported CSV files that can execute commands in Excel, Numbers, Google Sheets, or other CSV programs
    - Exploits that require users to modify code running on their own device (for example, opening browser developer tools and executing commands)

If you make a report, we'll ask for an exploit or proof of concept. If you can't execute an attack, not even a hypothetical one, we're unlikely to award a bounty. For example, here are some areas that we generally consider to be outside the scope of this policy:

- Failure to follow best practices that do not lead to an exploit
- Vulnerabilities in third-party code or services that do not lead to an exploit
- General disclosure of information, such as the Server- or X-Powered-By headers
- Missing HTTP security headers, such as:
    - Content-Security-Policy
    - Feature-Policy
    - HTTP Strict Transport Security
    - HTTP Public Key Pinning
    - X-Content-Type-Options
    - X-XSS-Protection
    - Referrer Policy
    - P3P
    - Certificate Transparency (Expect-CT)
    - X-Download-Options
    - X-DNS-Prefetch-Control

In principle, the parts below are also out of scope. We will assess this on a case-by-case basis:

- Social engineering (phishing) of Learnbeat-personnel or users
- List containing usernames or email addresses
- Denials of service targeting a single user
- Changing the Host-header to create redirects
- Lack of integrity of sub-resources
- Email Security: DMARC, DKIM, SPF
- DNSSEC
- Expiration time session cookie
- Password Policy Issues
- Disclosure of non-sensitive internal identifiers (such as user IDs)
- Bypass two-factor authentication (2FA) with third-party logins, such as Google

If you're not sure whether an issue falls within the scope of this policy, we'd appreciate it if you do report it.

Based on http://responsibledisclosure.nl/ by Floor Terra