# Reporting security issues

We do all we can to keep our systems secure. But it's always possible that you'll spot a weakness we've missed. If you do, please let us know, so that we can do something about it quickly. Reporting problems you come across is known as vulnerability disclosure (also known as coordinated vulnerability disclosure and responsible disclosure).

## How to report a problem

- Please mail details to cvd@snappet.org.
- Include as much information as possible, because that will help us reproduce the problem and put it right. We'd ideally like to have a description of what you discovered, complete with IP addresses, logs, screenshots and so on.
- Please include your contact details (phone number or e-mail address), so that we can get in touch if we need to know more.

## Other important points

- Don't tell anyone what you found.
- Destroy any data you've stumbled on.
- Don't go deeper into our systems than you need to show that there's a problem.
- Don't abuse a vulnerability you've discovered. If you do, we'll inform the police.

## What you do not need to report:

- Security bugs in third-party websites that integrate with us
- HTTP 404 codes/pages or other HTTP non-200 codes/pages.
- Banner disclosure on common/public services.
- Disclosure of known public files or directories, (e.g. robots.txt).
- Clickjacking and issues only exploitable through clickjacking.
- CSRF on forms that are available to anonymous users (e.g. the contact form).
- Logout Cross-Site Request Forgery (logout CSRF).
- Presence of application or web browser ‘autocomplete’ or ‘save password’

## Known issues

There are also problems that are already aware of and that we are working on or that we recognise as accepted risks. These problems are not mentioned on the website. Our support team is aware of them and will report them. As a result, the issue will not be dealt with.

## What we'll do

- We'll e-mail you within one working day, confirming receipt of your report.
- Within five working days, we'll respond to the substance of your report and tell you when the issue will be resolved. Weaknesses are fixed as soon as possible and certainly within three months.
- We'll keep you updated about progress with fixing the issue.
- With your help, we'll decide whether information about the issue should be published. We'll name you as the person who discovered the problem only if you want us to.

## Security.txt

RFC 9116 sets out a straightforward mechanism for organisations to publish their vulnerability disclosure policies and contacts details. The system involves publication of a file called security.txt on the organisation's website, written in a special legible and machine-readable text format. We follow this internet standard ourselves. Our security.txt file is available here: https://www.snappet.nl/.well-known/security.txt.