Report vulnerability

Have you discovered a vulnerability in our systems? Then we would like to hear from you. With your help, we can improve our services and their security.

You can report problems related to our online services. For example (but not limited to):

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

Our ruleset

Are you reporting a vulnerability to us? And is this report relevant? In that case, we always reward you with a small present or Swag. After all, you have invested time and effort in your research. Is your report significant? Then you may be eligible for compensation. We do have a ruleset:

- Act with integrity and do not cause damage during your investigation.
- Do not disrupt our services if you are investigating a vulnerability.
- Never disclose customer or our personal information.
- Anyone can report a vulnerability. Even if you are not a customer of Trad3s.
- Do not share the vulnerability with others until it is resolved. Talk to our experts and give us time to resolve the issue.
- We only handle reports in English or Dutch.
- Do not use attacks on physical security, social engineering or hacking tools such as vulnerability scanners.
- Do not place a backdoor in any (information) system (to demonstrate the vulnerability.)
- Make minimal use of a weakness. Only do what is necessary to determine the vulnerability.
- Do not change or delete any data from the system(s).
- Be cautious about copying data.
- Do not make system changes.
- Do not repeatedly attempt password guessing to gain access to systems through brute force attacks, dictionary attacks and the like.

Exclusions

If it concerns a vulnerability with a low or accepted risk, Trad3s can decide not to reward a report. Below are some examples of such vulnerabilities:

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

What happens after you file a report

Our security experts will investigate your report. You will receive an initial response within two business days. You can report to security@trad3s.com. Perhaps you are doing something in your investigation that is prohibited by law. If you do this in good faith, carefully and according to the ruleset mentioned above, we intend not to press charges. However, we do want to be able to ballance each situation separately. We consider ourselves morally obliged to press charges if we suspect that the vulnerability or data is being misused, or that you have shared knowledge about the vulnerability with others.

Reward

We always give you a litle present or Swag for the effort you have taken if what you have found is not on the exclusion list. If we fix vulnerabilities or adjust our services thanks to your report, we will give you an appropriate compensation for this. Trad3s decides whether you qualify for this and what the amount of the reimbursement is. Are others reporting the same vulnerability? Then the reimbursement is for the first reporter.

In scope

www.trad3s.com
my.trad3s.com
beta.trad3s.com

Not in scope

Dashboard.trad3s.com
Mailing.trad3s.com
Hoskinson.trad3s.com
Wiki.trad3s.com

Privacy

If you have made a report, we will ask for your contact details (name, email, PGP public key and telephone number). We do not give your information to others and do not use it for other purposes. Unless we are legally obliged to do so, for example in the case of a claim by the judicial authorities.

AWS

Our services run on Amazon Web Services. Amazon has its own rules regarding the pentesting of services on their platform. We kindly ask you to take note of these rules and to comply to them while conducting your research.

URL: https://aws.amazon.com/security/penetration-testing/