

# Responsible disclosure

If you want to report a 'regular' bug, not related to security, please do so using our [issue tracker](#).

We are committed to keeping the IT environment of S.A. Proto secure. This is why we ask you, if you find any bug and/or vulnerability related to the security of the IT environment of S.A. Proto, to:

- disclose the bug to us, via [security@proto.utwente.nl](mailto:security@proto.utwente.nl), as soon as you confirm its existence;
- not make any use of the bug and/or vulnerability beyond what is necessary to confirm it;
- only access your own data to confirm the bug and/or vulnerability, where possible;
- not publicly disclose the bug and/or vulnerability until we have had a chance to correct it.

If these conditions are adhered to, we promise in return:

- to reply to your e-mail within 14 days;
- to fix the vulnerability within 60 days after we acknowledge the vulnerability;
- to give you credit for disclosing the bug and/or vulnerability;
- to allow you to publicly disclose the bug and/or vulnerability after we have fixed it, if you so wish;
- to not press any criminal charges.

Please keep in mind that this IT environment is run by volunteering students. While we take security incidents very serious, we don't have a dedicated, full-time team watching our security mailbox.

## Known configuration issues

Due to the number of duplicate reports, please be sure to check the list below for known issues.

- Our e-mail domains don't have any DKIM records present due to a technical incompatibility. We make do with SPF records.
- There is no option to invalidate your own account sessions. We haven't found a way to make this work with our session driver and due to the low impact, we're leaving this as is.

## PGP keys

Should you wish to encrypt your e-mail towards us you can use any of the PGP keys below:

- [0xD7548420DF02F8F2A15F968ED085B0850F62BCD1](#)

## Hall of Fame

The following people have already responsibly disclosed a security vulnerability or configuration issue in our website. A huge thanks to them!

## Security Vulnerabilities

- **Sagar Banwa** disclosed a persistent XSS vulnerability on the User Dashboard on *August 7, 2020*.
- **Emile Nijssen** disclosed a user input sanitation omission in our UTwente addressbook search on *May 12, 2020*.
- **Wouter Kobes** disclosed that it was possible for any user to change the profile photo of any other user on *March 15, 2018*.

## Configuration Issues

- **Mohammed Abdul Kareem** alerted us to a missing X-Content-Type-Options header on *September 2, 2020*.
- **Dhanumaalaian R** alerted us to some missing CAA records on *September 2, 2020*.
- **Hemant Patidar** suggested that changing the e-mail associated with your account could be done a little safer on *August 30, 2020*.
- **BABABOUNTY** alerted us to some missing HSTS headers on *August 28, 2020*.
- **Aditya Rana** alerted us to some missing CSP headers on *August 28, 2020*.
- **Shubham Panchal** alerted us to some missing HSTS headers on *August 27, 2020*.
- **Eshan Singh** alerted us to some missing rate limiting precautions on authentication endpoints on *August 20, 2020*.
- **Badal Sardhara** alerted us to some missing SPF records on *August 20, 2020*.
- **Niraj Mahajan** suggested that deleting user accounts should require a password, making the site a little safer, on *August 19, 2020*.
- **Vishal Jain** alerted us to missing XSS protection in one of our API endpoints on *May 25, 2018*.

From:

<https://wiki.proto.utwente.nl/> - **S.A. Proto Wiki**

Permanent link:

<https://wiki.proto.utwente.nl/ict/responsible-disclosure>

Last update: **2020/09/09 08:39**

