Responsible Disclosure

At Zuyd University of Applied Sciences we consider the security of our information 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 users and our systems.

This Responsible Disclosure policy is not an invitation to scan our company network actively and extensively as a means of discovering weak points, Brute force attacks, DDoS, and social engineering fall outside the scope of this Responsible Disclosure policy.

Which vulnerabilities can be reported?

Vulnerabilities that pose a risk to system security can be reported to us. Examples include vulnerabilities that enable login forms to be bypassed or provide unauthorized access to databases containing personal information.

Not every defect in a system constitutes a vulnerability. In general, the following defects do not result in a potential security breach and we therefore kindly request that you do not report such vulnerabilities to us:

- Defects that do not affect the availability, integrity, or confidentiality of data.
- The availability of the WordPress xmlrpc.php functionality when its abuse is limited to what is known as a 'pingback denial-of-service' attack.
- The opportunity to use cross-site scripting on a static website or a website that does not process any sensitive (user) data.
- The availability of version information, for example via an info.php file. One exception in this scenario is when the version information reveals that the system uses software that contains known vulnerabilities.
- The lack of HTTP security headers as used by mechanisms such as Cross-Origin Resource Sharing (CORS), unless this lack of a security header demonstrably results in a security problem.

If you have any doubts about whether the defect you have found constitutes one of the above exceptions, then you can of course still report the defect to us. We will subsequently determine whether the defect constitutes a vulnerability and take appropriate follow-up action.

You are asked

To email your findings as soon as possible to csirt@zuyd.nl. If confidential information is involved, you are asked to encrypt the findings, using our PGP key for example, to prevent the information from falling into the wrong hands;

- Not to misuse the vulnerability by viewing more data or by downloading more than is needed to demonstrate the leak. A directory listing is sufficient proof of access to a system; there is then no need to open or copy files, etc.
- Not to alter or delete any information.
- Not to share confidential information, such as personal data, with others.
- Not to share the vulnerability with others until it has been resolved.

- Not to conduct attacks on the physical security or applications of third parties, not to conduct social engineering (including phishing), distributed denial-of-service (DDoS) attacks, or brute force attacks on authentication or other systems.
- To give us sufficient information to reproduce the vulnerability so that we can resolve it as quickly as possible. The IP address, the URL of the affected system, a description of the vulnerability and of the action taken are usually sufficient, but more may be needed if the vulnerabilities are more complex.
- Provide an e-mail address or telephone number to enable us to contact you if we have any questions. We prefer to communicate via e-mail.
- It is permitted to make the situation public only when the notifier and Zuyd University of Applied Sciences have agreed that the vulnerability may be made public, when all affected parties have been properly informed, and when Zuyd University of Applied Sciences has indicated that the vulnerability has been resolved.
- If a vulnerability cannot be resolved, or only resolved with difficulty, or if the process is very costly, the notifier is only authorized to make the vulnerability public with the express permission of Zuyd University of Applied Sciences. Zuyd University of Applied Sciences would prefer to be involved with any publication about any such vulnerability.

We ask you not to report trivial vulnerabilities, configuration settings or bugs that in themselves cannot be misused. Please note that if you do send us any such reports or findings, we are not obligated to respond. These include for example:

- Output results obtained from automated scanning tools such as Nmap, tls scanners etc. without proof of exploitability.
- Reports of obsolete versions of any software without a proof of concept of a working exploit.
- Reports on missing best practices settings for example on e-mail settings such as spf, dkim, dmarc, protocol settings such as ipv6 protocol support or dnssec.
- Fingerprinting or labeling of operating systems on servers that host public services.
- Sensitive information found in public files or directories, such as robots.txt, security.txt, rfc2350 or public articles on our website.
- Issues found with SSL/TLS configurations such as: disabled SSL Perfect Forward Secrecy, support for weak cipher suites.
- Clickjacking and problems that can only be exploited via clickjacking.
- Anything related to HTTP security headers, for example lack of Strict-Transport-Security, X-Frame-Options, X-Content-Type-Options etc.

Principles of our policy:

- If you submit your report in accordance with the procedure, then there will be no grounds for legal consequences in relation to your report. We will handle your report in confidence, and we will not share your personal details with third parties without your permission unless we are compelled to do so by law or by a court ruling.
- We will only specify your name on the Hall of Fame as the discoverer of the vulnerability in question if you give permission for us to do so.
- We will confirm receipt of the report within one working day, and we strive to send an assessment of your report within three working days. We will also give you progress updates regarding the resolution of the problem.
- Zuyd University of Applied Sciences of Applied Sciences will strive to have the security problem identified by you resolved within no more than 60 days. Upon

resolution of the problem, we will consult with you to determine whether and in what way to publish details of the problem and its resolution.

Hall of Fame

As of 2024, Zuyd University of Applied Sciences of Applied Sciences will place a Hall of Fame on its website each year to highlight and thank the researchers, who desire a mention on our Hall of Fame, with the best reports from the previous year. Your (screen)name will be on display until the next yearly update of the Hall of Fame.

The following quality requirements are considered for the creation of the list:

- The quality of the report should be sufficient (i.e., no 'naked' automated scan report, or duplicate of findings on a public posting).
- The information in your report has had a significant impact on improving the digital security posture of Zuyd.
- With multiple reports from the same reporter: the percentage of good and qualitative reports is high.
- The quality of the reporting in the notification is good.

 The policy is based on the example of Floor Terra and NCSC.