Engels:

Not in scope:

Z-CERT will not process reports of vulnerabilities or security issues that cannot be abused or are trivial. Below are a couple of examples of known vulnerabilities and issues that are outside the scope. This does not mean they are not important or should not be resolved, however our CVD process is meant for issues that can be actively abused. For example a vulnerabilities that can be abused by a public available exploit or a misconfiguration that can be used to bypass an existing security control. This list of exclusions is derived from a list used by the CERT of Surf (https://www.surf.nl/responsible-disclosure-surf).

- HTTP 404 codes/pages or other HTTP non-200 codes/pages and content spoofing/text injections in these pages

- Fingerprinting/version disclosures op public services

- Public files or directories that do not contain confidential information

- Clickjacking problems that can only be exploited by clickjacking

- No secure/HTTP-only flags on unconfidentional cookies

- OPTIONS HTTP method enabled

- Rate-limiting without clear impact

All issues related to HTTP security headers, for example:

– Strict-Transport-Security

– X-Frame-Options

– X-XSS-Protection

– X-Content-Type-Options

– Content-Security-Policy

SSL-configuration issues

– SSL Forward secrecy disabled

- No TXT record for DMARC or a missing CAA-record

- Host header injection

- Reports of outdated versions of any software without a proof of concept of a working exploit