Responsible Disclosure Exceptions

Application

- Self-XSS that cannot be used to exploit other users
- Verbose messages/files/directory listings without disclosing any sensitive information
- CORS misconfiguration on non sensitive endpoints
- Missing cookie flags on non sensitive cookies
- Missing security headers which do not present an immediate security vulnerability
- Missing DNS entries
- Cross-site Request Forgery with no or low impact
- Presence of autocomplete attribute on web forms.
- Reverse tabnabbing
- Bypassing rate-limits or the non-existence of rate-limits.
- Best practices violations (password complexity, expiration, re-use, etc.)
- Clickjacking on pages without sensitive actions
- CSV Injection
  Sessions not being invalidated (logout, enabling 2FA, ..)
- Hyperlink injection/takeovers
- Mixed content type issues
- Cross-domain referer leakage
- Anything related to email spoofing, SPF, DMARC or DKIM
- Username / email enumeration
- E-mail bombing
- HTTP Request smuggling without any proven impact
- Homograph attacks
- XMLRPC enabled
- Banner grabbing /Version disclosure
- Open ports without an accompanying proof-of-concept demonstrating vulnerability
- Weak SSL configurations and SSL/TLS scan reports
- Not stripping metadata of images
- public API keys without proven impact

General

- In case that a reported vulnerability was already known to the company from their own tests, it will be flagged as a duplicate.
- Theoretical security issues with no realistic exploit scenario(s) or attack surfaces, or issues that would require complex end user interactions to be exploited, may be excluded or be lowered in severity
- Spam, social engineering and physical intrusion
- DoS/DDoS attacks or brute force attacks.
- Vulnerabilities that are limited to non-current browsers (older than 3 versions) will not be accepted
- Attacks requiring the usage of shared computers, man in the middle or compromised user accounts

- Recently disclosed zero-day vulnerabilities in commercial products where no patch or a recent patch (< 2 weeks) is available. We need time to patch our systems just like everyone else - please give us 2 weeks before reporting these types of issues.
- Attacks requiring unrealistic user interaction