Out of scope:
- Software versions with known vulnerabilities, unless proven to be exploitable.
- Missing or sub-optimal security related headers (including cookie flags) or technologies (subresource integrity, frame sandboxing, samesite, etc.).
- Session fixation and missing session revocation
- Non-optimal TLS/SSL configuration
- Sub-optimal rate limits
- Unsafe file upload, unless proven exploitable.
- Weak password policy
- Insecure HTTP methods such as OPTIONS
- Account creation/change or newsletter subscription not validating e-mail address
- Denial of Service attacks.
- Potentially sensitive paths in robots.txt.
- Open redirects
- Dangling IPs
- Best practices concerns
- Path disclosure
- Banner grabbing issues (figuring out what web server we use, etc.)
- UUID enumeration of any kind
- Open ports without an accompanying proof-of-concept demonstrating vulnerability
- Vulnerabilities as reported by automated tools without additional analysis as to how they're an issue
- Invalid or missing SPF (Sender Policy Framework) records
- Content spoofing / text injection
- Forms missing CSRF tokens (we require evidence of actual CSRF vulnerability)
- Attacks requiring physical access to a user's device
- Social engineering of Kaartje2go staff or contractors

Out of scope domains:
- splunk.kaartje2go.nl
- quiz.kaartje2go.nl