Out of scope statement

Melding kwetsbaarheden – responsible disclosure

Amsta geeft geen beloning voor triviale kwetsbaarheden of bugs die niet misbruikt kunnen worden. Hieronder staan voorbeelden van bekende of triviale kwetsbaarheden en geaccepteerde risico's, die buiten bovenstaande regeling vallen:

- HTTP 404 codes/pagina's of andere HTTP non-200 codes/pagina's en content spoofing/text injecting op deze pagina's
- Fingerprinting/versievermelding op publieke services
- Publieke bestanden of directories met ongevoelige informatie (bijvoorbeeld robots.txt)
- Clickjacking en problemen die alleen te exploiten zijn via clickjacking
- Geen secure/HTTP-only flags op ongevoelige cookies
- OPTIONS HTTP method ingeschakeld
- Rate limiting kwetsbaarheden zonder duidelijke impact
- Alles gerelateerd tot HTTP security headers, bijvoorbeeld:
    - Strict-Transport-Securit
    - X-Frame-Options
    - X-XSS-Protection
    - X-Content-Type-Options
    - Content-Security-Policy
- Issues met SSL-configuratie issues
- SSL Forward secrecy uitgeschakeld
- zwakke/onveilige cipher suites
- Issues met SPF, DKIM of DMARC
- Host header injection
- Rapporteren van verouderde versies van enige software zonder een proof of concept van een werkende exploit
- Informatieblootstelling in metadata

Meer informatie www.amsta.nl/melding-kwetsbaarheden