Definition of done

# Generic Web Service

1. - API Urls exposen geen gevoelig informatie zoals API key, session tokets etc.
2. - Alle encoders en parsers zijn hetzelfde

# File Download

1. - Requests naar geuploadet bestanden worden niet als html/javascript gerunt

# File Execution

1. - Onbetrouwbaar bestand metadata wordt niet gebruikt met systeem APIs en libraries
2. - Gebruiker submitted bestandsnaam metadata wordt gevalideerd of genegeerd
3. - Gebruiker submitted bestandsnaam metadata wordt niet gebruikt door het systeem en URL API is beschermd tegen path traversal

# Business logic

1. - Business Logic heeft validation en afbakening
2. - Er is een limiet op specifieke acties beschreven in het TO op basis van gebruiker

# HTTP

## Security header

1. - Elk HTTP response heeft een Content-Type header
2. - Elk HTTP response heeft een safe character set
3. - Elk HTTP response content matcht de hierboven aangegeven
4. - Alle API responses bevatten een Content-Disposition header
5. - Elk HTTP response heeft een CSP ingesteld
6. - Elk HTTP response heeft een no-sniff header
7. - Elk HTTP response op elke subdomain heeft een Strict-Security-Transport header
8. - Content kan niet op een third-party site worden getoond en wordt alleen toegestaan met een geschikt Content-Security-Policy

## Validation

1. - De Origin Header wordt niet gebruikt voor authenticatie of access control
2. - De Cross-Origin Resource Sharing (CORS) Access-Control-Allow-Origin header heeft een strikt lijst met toegestane domains en subdomains. Null is niet mogelijk

# REST

1. - De inkomend Content-Type header moet de verwachtte type zijn
2. - Cross-Site Request Forgery wordt vermeden door een check op double submit cookie pattern of CSRF nonces of Origin request header checks
3. - JSON schema wordt gevalideert en geverifieerd voordat input wordt geaccepteerd
4. - HTTP Methodes moeten valid zijn voor gebruiker of actie. PUT of DELETE mag bijvoorbeeld niet gebeuren op beveiligde API en Resources