**Rapport security code review:**

**Opdracht:**

Controleer de code van het project op kwetsbaarheden op een aantal aspecten:

* Configuratie
* SQL injectie
* XSS
* Encryptie
* CSRF
* Autorisatie / access control

Vind eerst de hot spots, beoordeel dan of er sprake is van een kwetsbaarheid (vulnerability) en noem tegenmaatregelen (mitigations) als dat nodig is.

**Inleveren:**

Geef in de onderstaande tabellen aan

* of kwetsbaarheden aanwezig zijn op deze aspecten
* zo mogelijkheden in welke bestanden op welke regelnummers
* mogelijke beschermingsmaatregelen

Lever deze in

|  |  |
| --- | --- |
| **Configuratie** (verkeerde instellingen, extensies, leesrechten, etc.?) | |
| Welke kwetsbaarheden zijn er? |  |
| In welke bestand(en) en op welke regel(s) |  |
| Welke tegenmaatregelen  kun je treffen? |  |

|  |  |
| --- | --- |
| **SQL DB injectie** (kan de gebruiker met bepaalde invoerdata database-queries of database-acties veranderen?) | |
| Welke kwetsbaarheden zijn er? |  |
| In welke bestand(en) en op welke regel(s) |  |
| Welke tegenmaatregelen  kun je treffen? |  |

|  |  |
| --- | --- |
| **XSS** (kan de gebruiker JavaScript of i.d. te laten uitvoeren of laten opslaan?) | |
| Welke kwetsbaarheden zijn er? |  |
| In welke bestand(en) en op welke regel(s) |  |
| Welke tegenmaatregelen  kun je treffen? |  |

|  |  |
| --- | --- |
| **Encryptie**  (is de versleuteling sterk of zwak, is de versleuteling te breken of te omzeilen?) | |
| Welke kwetsbaarheden zijn er? |  |
| In welke bestand(en) en op welke regel(s) |  |
| Welke tegenmaatregelen  kun je treffen? |  |

|  |  |
| --- | --- |
| **CSRF**  (wordt een http-request vanaf een ander domein geaccepteerd?) | |
| Welke kwetsbaarheden zijn er? |  |
| In welke bestand(en) en op welke regel(s) |  |
| Welke tegenmaatregelen  kun je treffen? |  |

|  |  |
| --- | --- |
| **Autorisatie / access control**  (kan de gebruiker bepaalde acties uitvoeren zonder de juiste gebruikersrechten?) | |
| Welke kwetsbaarheden zijn er? |  |
| In welke bestand(en) en op welke regel(s) |  |
| Welke tegenmaatregelen  kun je treffen? |  |