**Rapport security code review:**

**Voorbereiding**:

Gebruik campagneLaravel.zip en campagne.sql.

Pak de zip uit en voeg de vendor-map toe met het commando “composer update”.

Maak database campagne aan en vul deze met het sql-bestand.

Start de applicatie.

**Opdracht:**

Controleer de code van Campagne op kwetsbaarheden op een aantal aspecten:

* Configuratie
* SQL injectie
* XSS
* Encryptie
* CSRF

Extra

Controleer de code van Campagne op kwetsbaarheden op een aantal aspecten:

* Autorisatie / access control

**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 op itslearning

|  |  |
| --- | --- |
| **Configuratie** (verkeerde instellingen, extensies, leesrechten, etc.?) | |
| Welke kwetsbaarheden zijn er? | 1. Username en password zijn root en “ ” 2. Debug staat aan |
| In welke bestand(en) en op welke regel(s) | 1. .env 15-16 2. .env 9 |
| Welke tegenmaatregelen  kun je treffen? | 1. Betere username en password verzinnen of in beveiligde map 2. uitzetten |

|  |  |
| --- | --- |
| **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? |  |

**EXTRA**

|  |  |
| --- | --- |
| **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? |  |