ÜBER
COACHING

Om de veiligheid van de applicatie te waarborgen zijn een aantal maatregelen genomen tijdens het programmeren, deze maatregelen zijn;

- Hashing
- Beveiliging tegen XSS scripting
- Prepared statements
- Session management

In dit verslag zal worden uitgelegd hoe dit geïmplementeerd is en hoe dit het proces van ontwikkeling heeft beïnvloed.

Hashing

Om de veiligheid van alle wachtwoorden te kunnen waarborgen hebben we eerst aan alle wachtwoorden een salt toegepast en ze daarna gehashed opgeslagen zodat wanneer er onverhoopt dingen uit de database gelezen kan worden een aanvaller nog steeds de wachtwoorden niet weet.

XSS beveiliging

Onder het motto "vertrouw nooit de cliënt" hebben we geprobeerd om alles zoveel mogelijk serverside te doen. We hebben een paar keer er voor moeten kiezen om bepaalde berekeningen clientside te doen, maar aangezien deze berekeningen alleen over de gegevens van de desbetreffende cliënt gaan kwamen te tot de conclusie dat dit niet erg is. Deze data voegt niks toe en vraagt niks op uit de database. Het zijn dus statische paginas die geen betrekking hebben op gevoelige data, een voorbeeld hiervan is de calculator pagina wanneer men niet ingelogd is. Deze pagina maakt gebruik van javascript om het BMI en het vetpercentage van een persoon te bereken. Hierbij wordt geen gebruik gemaakt van de database. Om dit op deze manier te implementeren hebben we af en toe anders over een stuk code na moeten denken, maar over het algemeen heeft dit niet voor problemen gezorgd.

Prepared statements

Om de webapplicatie tegen SQL injecties te beveiligen maken we gebruik van prepared statements, dit zorgt er voor dat onze databases niet op deze manier voor een malafide gebruiker toegankelijk zijn. Aangezien alle input eerst gefilterd wordt door de server kan er geen malafide input gegeven worden en is de veiligheid van de applicatie gewaarborgd omtrent het databasegebruik. De applicatie is zo voldoende beschermt en niet meer vatbaar voor SQL injecties.

Session management

Om problemen met database opvragen te voorkomen maken we gebruik van een session cookie en als de user niet gevalideerd kan worden of de cookie leeg is word de user geredirect naar de login pagina. Deze cookies zijn gedefinieerd als onvoorspelbare strings om zo te voorkomen dat een kwaadwillende gebruiker een session gemakkelijk kan hijacken en zo gevoelige informatie kan achterhalen.