## Deelvraag Fraude gevoelig?

Vooral na dat we dit jaar ook security hebben gehad, leek het ons wel leuk om een degelijke vorm van beveiliging te integreren. Hierbij hebben we erg kritisch gekeken naar alle mogelijkheden om de beveiliging te verbeteren.

Het begint al bij de database. Databases zijn erg belangrijk en applicaties die ervan af hangen horen een erg goede beveiliging. In de applicatie zelf hebben we al gekeken naar alle input die door users wordt gegeven. In ons design is er al weinig input wat het een erg veilig ontwerp maakt, maar we vonden een heel ver gezochte zwakheid. Als iemand met een aangepaste nhl-pas gebruikt maakt van het systeem, zou er een probleem kunnen onstaan, deze bug(foutje in de sofware) is verholpen en zou daarbij alleen voorgekomen zijn als iemand bewust het systeem zou aanvallen.

Door de toevoeging van een webapplicatie die dezelfde database gebruikt, werd het risico al een stuk groter. Sites of webapplicaties die gekoppeld zijn aan een database kunnen erg onveilig zijn als ze niet goed zijn verbeterd. Nu gebruikt hij een test-database, maar als in de toekomst de NHL-database er aan gekoppeld wordt, dan is beveiliging natuurlijk een belangrijk aspect.

Daarom hebben we erg veel veiligheids-methoden toegepast in de code. De regel is dat alle user input nagekeken moet worden, dit wordt netjes gedaan. Ook moet alle data waar meegewerkt wordt nagekeken als de gebruiker een vorm van invloed er op heeft. We bekijken zelfs de data die vanuit de database zelf komt. Ook blijft de data op de database zelf staan en kan daardoor heel moeilijk van buiten af veranderd worden.