**Welke veiligheidsrisico’s bedreigen je applicatie en wat is de impact van tegenmaatregelen?**

**Risico’s**

Een risico is dat de gegevens van de gebruiker kan worden gestolen. Daarnaast kan er XSS-attacks plaatsvinden. Een andere risico is dat de webapplicatie een SQL injection attack krijgt. Ook is er risico op Broken Authentication and Session Management.

**Tegenmaatregelen**

Om deze risico’s tegen te gaan kan er ten eerste een overstapping plaatsvinden naar https en om dan XSS-attacks tegen te gaan zal er als oplossing gebruik worden gemaakt van Content Security Policy (CSP). Met CSP geef je via een speciale HTTP-header precies aan van welke andere sites er scripts ingeladen mogen worden, of er plaatjes van andere websites gehaald mogen worden. Om de SQL injection attack te voorkomen kan je het beste elke keer per actie controleren voor welke ID het bedoeld is, zodat de hacker niet zomaar gegevens kan downloaden, aanpassen en verwijderen. Om Broken Authentication and Session Management tegen te kunnen gaan zal er voldoen moeten worden aan alle vereisten voor verificatie en sessiebeheer die zijn gedefinieerd in OWASP's Application Security Verification Standard (ASVS) -gebieden V2 (authenticatie) en V3 (Sessiebeheer). Daarnaast moet er ook grote inspanningen worden geleverd om XSS-fouten te voorkomen die kunnen worden gebruikt om sessie-ID's te stelen.

Het is best groot om deze tegenmaatregelen te implementeren. Ten eerste heb je voor https een certificaat nodig. Daarnaast zijn de andere maatregelen niet zomaar te regelen door wat aan te passen in Java EE en tomcat. Wat wel nog mogelijk is om in mijn concrete situatie aan te passen is door gebruik te maken van een speciale HTTP-header door middel van CSP. Daarnaast kan ik extra code schrijven om de ID te controleren voor de ID’s doeleinden, zodat de kans op SQL injection flink daalt.

Mijn aanbeveling is dat de tegenmaatregelen voor CSP en SQL injection als eerst zo snel mogelijk moeten worden geregeld.

**Literatuurlijst**

Top 10 2013-A2-Verbroken authenticatie en sessiemanagement. (z.d.). Geraadpleegd op 4 juli 2018, van https://www.owasp.org/index.php/Top\_10\_2013-A2-Broken\_Authentication\_and\_Session\_Management

Top 10 risico's voor webapplicaties. (z.d.). Geraadpleegd op 4 juli 2018, van https://www.security.nl/posting/26765/Top+10+risico's+voor+webapplicaties