**3. Mitä tarkoitetaan injektiohyökkäyksillä, miten ne yleensä tehdään, mitä niillä pahimmillaan voi saada aikaiseksi ja miten niitä torjutaan?**

Injektiohyökkäys on haitallisen koodin syöttäminen ohjelmistoon, joka kerää haluttuja tietoja. Yleisin injektiohyökkäys on SQL-injektio, jossa SQL-kyselyyn saadaan sopivalla syötteen valinnalla aiheutettua ongelmia. Pahimmillaan voit muokata järjestelmän dataa tai suorittamalla palvelimelle tallennettua ohjelmakoodia. Ne voi torjua simppelisti tarkistamalla aina kaikki käyttäjän antamat syötteet. Torjumiseen on myös valmiskirjastoja, jotka estävät SQL-injektio hyökkäyksen.

**4. Mitä tarkoitetaan XSS-hyökkäyksillä, miten ne yleensä tehdään, mitä niillä pahimmillaan voi saada aikaiseksi ja miten niitä torjutaan?**

XSS-hyökkäys, eli Cross-site scripting, on yleensä hyökkääjän sisällyttävää Javascriptiä käyttäjälle lähetettäviin sivuihin. Voi varastaa evästeitä, lukea lomaketietoja, ladata haittaohjelmia, kirjoittaa sivun sisältöä uusiksi... Tarkistamattomien lomakkeiden avulla koodi saadaan järjestelmän sisään. Niitä torjutaan tarkistamalla aina käyttäjän syötteet ennen niiden tallentamista palvelimelle. PHP:ssä tähän toimii hyvin strip\_tags-funktio. Tähän voi myös käyttää sopivaa kirjastoa sisällön karsimiseen.

**5. Nimeä ainakin kaksi tietoturvaominaisuuksia tarjoavaa kirjastoa valitsemallesi ohjelmointikielelle**

DOMPurify, XSS puhdistus. Puhdistaa HTML-koodin ja torjuu XSS-hyökkäykset. SQLMAP, automatisoi prosessin, joka tunnistaa ja torjuu SQL-injektion.