1. What is OWASP and what is its primary mission as described in the article?

OWASP är en förkortning för Open Web Application Security Project. OWASP är en internationell, idell organisation som strävar efter att öka säkerheten för webbapplikationer och därmed minska risken för cyberattacker. OWASP erbjuder bland annat dokumentation, verktyg, videor och forum och allt deras material är gratis och finns tillgängligt på organisationens hemsida.

2. Explain the concept of "Injection". Provide an example of how an injection attack could compromise a web application's security.

En injektionsattack kan inträffa när opålitlig data skickas till en kodtolkare via ett formulär eller liknande och syftet är att manipulera, hämta eller förstöra data. En angripare kan till exempel lägga in SQL-databaskod i ett formulär där användaren ska skriva in sitt användarnamn. Om det finns brister i formulärets säkerhet leder detta till att SQL-koden körs.

3. Explain two strategies to prevent Broken Authentication vulnerabilities.

Bristande säkerhet inom autentiseringssystem kan leda till att angripare får tillgång till användarkonton, vilket kan äventyra säkerheten för ett helt system om de får tillgång till ett admin-konto. En metod för att undvika detta är att använda tvåfaktorsautentisering, det vill säga att inloggningen sker i två steg. En annan strategi är att begränsa eller fördröja upprepade inloggningsförsök.

4. Describe the potential consequences of Insecure Deserialization in web applications. How can developers protect against such attacks?

Serialisering innebär att man konverterar objekt från en applikations kod till ett annat format. Deserialisering innebär istället att man konverterar tillbaka serialiserad data till objekt som kan användas av en applikation. Säkerhetsbrister i deserialiseringsprocessen kan öka risken för exempelvis DDoS-attacker och RCE (Remote Code Execution)-attacker. Enligt OWASP är det enda tillförlitliga sättet att skydda sig från osäker deserialisering att förbjuda deserialisering av data från osäkra källor.

5. Briefly define Cross-Site Scripting (XSS) as outlined in the article and list two methods suggested in the article to prevent XSS attacks in web applications.

Cross-site scripting innebär att en angripare lägger in skadlig kod i en säker webbsida. Den skadliga koden körs när en användare laddar webbsidan, vilket kan leda till att angiparen får tag i känsliga användaruppgifter. Koden kan till exempel läggas till i slutet av en url eller publiceras på en sida med användargenererat innehåll. Exempel på strategier för att undvika cross-site scripting är att maskera opålitliga HTTP-förfrågningar samt att validera och/eller sanera användargenererat innehåll. Vissa ramverk, såsom ReactJS och Ruby on Rails, ger även ett visst inbyggt skydd mot cross-site scripting.