1. **What is OWASP and what is its primary mission as described in the article?**
   Svar: OWASP är ett Open Web Application Security Project som är en internationell organisation. Denna organisation fokuserar på säkerheten för webbapplikationer. Ett av huvuduppdragen för denna organisation är att se till att allt deras innehåll är fritt tillgängligt för alla för att förbättra säkerheten för deras webbapplikation.
2. **Explain the concept of "Injection". Provide an example of how an injection attack could compromise a web application's security.**

   Svar: Injektionsattacker inträffar när någon matar in skadlig data på en webbplats, som att fylla i ett formulär eller skicka information, för att lura den att köra farlig kod. Till exempel, istället för att skriva ett användarnamn i ett formulär, kan en hackare skriva en speciell kod för att bråka med webbplatsens databas. Webbplatsen kan köra den skadliga koden om formuläret inte är ordentligt skyddat. Denna typ av attack kallas en SQL-injektion.

   För att stoppa dessa attacker kan webbplatser kontrollera och rensa de uppgifter som användarna skickar in. Validering innebär att avvisa all data som ser misstänkt ut, medan sanering innebär att fixa eller ta bort de misstänkta delarna. Databashanterare kan också lägga till extra skydd för att begränsa skadan om en attack inträffar.
3. **Explain two strategies to prevent Broken Authentication vulnerabilities.**
   Svar:
   - Tvåfaktorsautentisering (two-factor authentication eller 2FA)
   - Med hastighetsbegränsning kan vi begränsa eller fördröja upprepade inloggningsförsök.
4. **Describe the potential consequences of Insecure Deserialization in web applications. How can developers protect against such attacks?**
   Svar:
   - Serialisering är som att packa in möbler i lådor så att de kan förvaras eller flyttas. Deserialisering är som att öppna de där lådorna och sätta ihop möblerna igen så att de kan användas. Det här problemet påverkar många webbplatser som ofta packar och packar upp data för att använda det på olika sätt.

     En osäker deserialiseringsattack inträffar när någon manipulerar "lådorna" (datan) medan den packas upp. Till exempel, om flyttarna bråkade med dina lådor under flytten, kan du sluta med trasiga eller utbytta möbler. På samma sätt kan en osäker deserialiseringsattack orsaka stora problem, som att krascha webbplatsen (DDoS-attack) eller låta hackare köra skadlig kod (fjärrkörning av kod).

- För att förhindra detta kan webbplatser övervaka uppackningsprocessen och kontrollera vilken typ av data som används. Det säkraste sättet att undvika dessa attacker är dock att aldrig packa upp data från opålitliga 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.**

   Svar:

   - Cross-site scripting (XSS) händer när en webbplats låter användare lägga till skadlig kod på en webbsida eller URL som andra kan se. Detta kan låta angripare köra dålig JavaScript-kod i någon annans webbläsare.

     Till exempel kan en angripare skicka ett e-postmeddelande som ser ut att vara från en betrodd bank, med en länk till bankens webbplats. Men länken har skadlig JavaScript-kod lagt till i slutet. Om bankens webbplats inte blockerar denna typ av attack, kommer den dåliga koden att köras i offrets webbläsare när de klickar på länken.

   - För att förhindra XSS kan webbplatser fly eller rensa bort osäkra användarinmatningar och kontrollera allt användargenererat innehåll för säkerhet. Att använda moderna verktyg som ReactJS eller Ruby on Rails kan också hjälpa eftersom de inkluderar inbyggt skydd mot XSS.