Opdracht Veilig Programmeren

1. Bouw een applicatie voor een blog website. Ingelogde gebruikers kunnen een nieuwe blog aanmaken, waarop andere gebruikers middels commentaar kunnen reageren.
   Gebruikers moeten zich kunnen registreren met hun e-mailadres en een wachtwoord. In de eerste versie wordt het wachtwoord niet versleuteld en als clear tekst in de database opgeslagen. Ook vindt geen check plaats op enige vorm van complexiteit van het wachtwoord.
   In zowel de blog post als in de commentaren dient de gebruiker HTML elementen te kunnen gebruiken om de tekst op te maken. Dus met …. moet bijvoorbeeld een deel van de tekst vet gemaakt te kunnen worden. De eerste versie van de website moet onbeveiligd zijn en je moet aan kunnen tonen met screenshots/video's dat de applicatie gevoelig is voor SQL Injection en voor XSS (Cross Site Scripting). Ook tegen een blind intruder attack is de site niet opgewassen. De applicatie moet gebruik maken van cookies.
   Gebruik BurpSuite om aan te tonen dat de applicatie niet bestand is tegen de genoemde aanvallen.
   Deze eerste versie dien je als een afzonderlijke branche op te slaan in een GitHub repository.

2. Pas de applicatie stap-voor-stap aan, zodat deze wel beveiligd is tegen de genoemde kwetsbaarheden. Iedere beveiliging die wordt toegevoegd dien je op te slaan in een aparte repository en je dient ook nu met screenshots weer aan te tonen dat en hoe de applicatie beschermd is. Ook in de beveiligde site moet de gebruiker nog steeds HTML elementen kunnen gebruiken om de tekst op te maken.
   In ieder geval dien je aan te tonen dat je de volgende technieken hebt gebruikt:
   a. Stored Procedures
   b. Input sanitisation
   c. Two Factor Authentication
   d. Logging van pogingen om de site aan te vallen via XSS