JENSEN yrkeshögskola
TRÄNING FÖR VERKLIGHETEN

Kursnamn: *Säker kommunikation över internet*
Klass: *FWK23G*
Termin: ***Höstterminen 2023 och Vårterminen 2024***

BLOGGPLATTFORM DEL 2

INLEDNING

Bakgrundsbeskrivning, frågeställning, avgränsning och mål	Bakgrund: Säkerhet är alltid en viktig aspekt av alla applikationer. Studerande ska få möjlighet att utveckla en enklare bloggapplikation som använder moderna metoder för att kommunicera över internet. Applikationen innehåller också nu OAuth och en ett grundläggande rollsystem för hantering av behörigheter. Studerande skyddar även sin applikation mot XSS och CSRF. Mål: Skapa en enklare applikation som använder moderna metoder för säkerhet. Exempelvis saltning och hashing av lösenord och token-baserad sessionshantering. Avgränsning: Bloggen behöver bara innehålla text och titel.
Varför ska ni utföra detta arbete?	Syftet: ● Lära sig hantera lösenord. ● Lära sig hantera olika privilegier. ● Lära sig om OAuth 2.0. ● Lära sig om Role-based Access Control ● Lära sig förebygga vanliga attacker som XSS och CSRF.
Vad ska ni leverera?	Följande ska levereras: 1. Länk till ett offentligt GithubRepo I repot måste det framgå för läraren: ● Vilka användare som finns och deras lösenord. ● Hur jag återskapar er databas. Två förslag gällande Redis: ○ Skriv en fil 'commands.redis' där alla SET finns åtskilda med ny rad mellan varje kommando ○ Använd SAVE och skicka med .rdb-filen i inlämningen på LearnPoint ● Vilka dependencies som används. Lägg därför alla dependencies i package.json

ER PROJEKTUPPGIFT

Vad ska ni göra?	Er uppgift är att skapa en blogg. I bloggen ser man olika användares blogginlägg. Alla användare ska i sitt flöde se de olika blogginläggen och vem som har skapat dem. Blogginläggen innehåller bara text och en titel. Krav [G] Varje användare kan logga in med ett unikt användarnamn och lösenord. [G] Lösenordet sparas hashat och saltat i databasen. [G] Sidan ska komma ihåg vem du är – om du öppnar sidan på nytt ska du fortfarande vara inloggad. Inom en rimlig tidsram förstås. Det ska också stå uppe i högra hörnet ”inloggad som {användarnamn}”. [G] Applikationen går att starta utan problem. [G] Blogginläggen ligger i en databas och inte hårdkodade. [G] Vid varje blogginlägg ska det framgå vem som har skrivit det. [G] Varje blogginlägg ska ha datum och tid vid sig. [G] Appen lagrar eventuell sessionsdata i en databas, inte i minnet. [G] Applikationen använder lämpliga metoder och statuskoder. [G] Det finns ett admininlogg. Admininlogget ska ha behörighet att ta bort alla inlägg från plattformen. [G] Nya användare ska kunna registrera sig. [G] En användare kan logga in/registrera sig via GitHub (OAuth 2.0). [G] Varje användare kan själv lägga upp blogginlägg via ett formulär. [VG] Varje användare kan ta bort sina egna inlägg. [VG] Användare kan kommentera på varandras inlägg. I kommentarsfältet ska användaren kunna använda HTML för att formattera sina inlägg. exempel blir **exempel**. [VG] Sidan använder sig av flera metoder för att säkra sig mot XSS och CSRF. [VG] I din inlämning ska du specificera några kodändringar och instruera hur man skulle kunna utföra en XSS-attack med skydden borttagna. Det räcker med att injicera en alert(), [Bonus] Användare kan “gilla” varandras inlägg. Det ska då framgå i alla inlägg vem/vilka som gillat inlägget. Om du är inne på sidan när någon gillar ditt inlägg får du en notis, utan att du behöver refresha sidan (använd WebSockets för detta). En väl implementerad bonus-feature kommer att ge fyra bonuspoäng på tentan.

INLÄMNING OCH REDOVISNING

Inlämning	Inlämning sker via Learn Point **15 Januari 23.59**

BEDÖMNING OCH ÅTERKOPPLING

Bedömning sker mot följande betygskriterier:	Betygskriterierna för Godkänd respektive Väl godkänd är: Godkänt (G) För att få betyget Godkänt (G) ska den studerande ha genomfört kursen och nått alla kursmål. Väl Godkänt (VG) För att få betyget Väl Godkänt (VG) ska den studerande ha genomfört kursen och nått alla kursmål. Den studerande ska vidare kunna föra välgrundade och nyanserade resonemang och kunna göra välgrundade och nyanserade bedömningar gällande tillämpningen av de metoder och verktyg som ingår i denna kurs. **Godkänd** ● Samtliga G-krav från kravspecifikationen är uppfyllda. **Väl godkänd** ● Samtliga VG-krav från kravspecifikationen är uppfyllda.
Återkoppling	Grupperna får skriftlig återkoppling via lärplattformen LearnPoint **senast den 29 Januari**