Inlämningsuppgift 2  
2dt902 - Mjukvaruarkitektur

[Jw223rn@student.lnu.se](mailto:Jw223rn@student.lnu.se)

Jesper Wingren

Uppgift 1:

**Inblandade aktörer:**

Användare – Detta är personen som interagerar med systemet exempelvis försöker logga in på systemet med hjälp av identifiering.

System – Detta tar emot identifiering och påbörjar autentisering samt auktorisering vid lyckad autentisering.

**Use-cases:**

Identifiering:

Användaren anger användarnamn, email eller liknande alternativt väljer att logga in med gmail.

Systemet tar emot användarens identifiering och förbereder för autentisering.

Autentisering:

Användaren fyller i lösenord, verifiering med fingeravtryck eller liknande för gmail loggar användaren in med sitt konto.

Systemet validerar vad användaren fyllt i och jämför det med lagrad data. Vid lyckad autentisering så godkänns användare tillträde och vid felaktig visas ett felmeddelande till användaren. För gmail sköts det liknande bara att autentisering sköts via ett tredjeparts anslutning.

Auktorisering:

Systemet kontrollerar användarens privilegier och tillhandahåller den information och funktioner användaren ska ha tillgång till.

Användaren får efter detta tillgång till de funktioner som är bestämt.

Noteringar att ha med:

Användare ska ha tillgång till pet shop utan att vara inloggad men man kan då inte genomföra köp.

En bild som visar diagram, linje, rita, design

Automatiskt genererad beskrivning

Uppgift 2:

**QAS 1:**

Source: Användare (ej inloggad)

Stimulus: Försöker göra beställning

Artifact: Beställningshanterare

Enviroment: Online, webbsida

Response: Icke auktoriserad

Response measure: Tillåt inte användaren att komma vidare och meddela ej inloggad till användare samt led användare till logga in sidan.

**QAS 2:**

Source: Användare

Stimulus: Loggar in med felaktigt lösenord flertalet gånger

Artifact: Inloggningshanterare

Enviroment: Online, webbsida

Response: Lås konto samt meddela mailadress kopplad

Response measure: Meddela kontoägaren att obehörig försökt komma åt kontot och tvinga ägaren att ange nytt lösenord för kontot. Logga ip och info i systemet att felaktiga inloggningsförsök skett.

**QAS 3:**

Source: Användare

Stimulus: Försöker logga in på flera konton med felaktiga lösenord inom kortare tidsspann

Artifact: Inloggningshanterare

Enviroment: Online, webbsida

Response: Blocka IP-adress

Response measure: Efter att försökt komma åt flera konton via samma ip-adress blocka från att genomföra fler inloggningsförsök. Logga även ip-adressen så att systemet vet om vid framtida försök.

Uppgift 3:

För QAS 1 vid en ej inloggad användare försöker genomföra ett köp så ”provides” auktoriseringskomponenten att användaren ej är inloggad och loggar därmed det samt att notifieraren uppmärksammas för att påpeka det för användaren.

Vid QAS 2 där användaren felaktig lägger in fel lösenord så ”requires” autentiseringskomponenten inloggningsinfon för att bekräfta felaktiga uppgifter. Efter det ”provides” autentisering med felaktig inloggning och meddelar loggningshanteraren som loggar och lagrar ip-adressen i databasen. Den meddelar även ip-adress blockeraren att de inkommit felaktig inloggning som kollar om denna ip-adress framkommit vid flera fall av misslyckande inloggningsförsök (i detta fall nej). Notifieraren får även denna information och meddelar mailadressen för kontot att det har genomförts misslyckade inloggningsförsök.   
Vid QAS 3 så sker samma som vid QAS 2 förutom att ip-adress blockerare får till sig att samma ip-adress har loggats vid flera inloggningsförsök och därmed blockar ip-adressen för framtida inloggningar genom att lagra den i databasen som blockerad för autentiseringshanteraren att hämta vid inloggningsförsök.

En bild som visar text, diagram, skärmbild, Plan

Automatiskt genererad beskrivning

Uppgift 4:

Inloggningshanterare har bytts ut till autentisering och auktorisering istället för mer förtydligande samt databas har bytts ut till datalagring.

