Week-8 Authentication/login- strategies

Explain about use cases and the pros & cons of the following authentication/Login-strategies

- **Java's declarative authentication and authorization features**

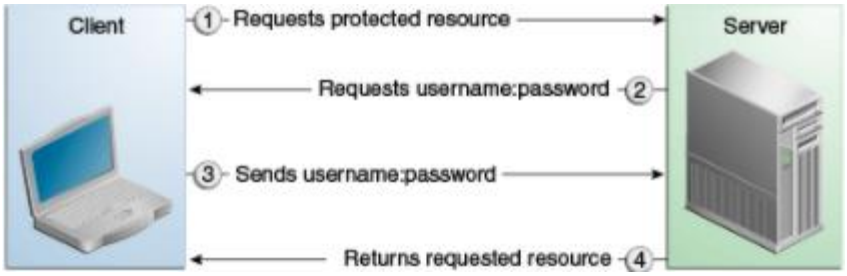
Container håndteret sikkerhed, også refereret som J2EE deklarativ sikkerhed er sammen med JAAS de sikkerheds teknologier for authentiation og authorization i Java 2 Enterprise Edition.
Pr. standard giver Oracle JAAS mulighed for at lagre user account information og sikkerhedsroller i en af to lokationer: XML-fil eller et LDAP directory.
Denne type af sikkerhed giver all access control til J2EE containeren, dermed adskiller man applikationens logik fra sikkerheds definitionerne. Ydermere bliver bruger roller mappet statisk i web application deployment descriptoren: web.xml. Det deklareres ved URL, så f.eks. Kun brugere med 'Admin' rollen kan tilgå en bestemt side.
I web.xml-filen vil man benytte sig af <security-constraint> elementet.

Om user authentication benyttes der primært to typer af authentication, FORM based og BASIC. Disse specificeres ligeledes i web.xml-filen, dog ved <login-config> elementet.

- **Basic HTTP:**

Hvis en klient gerne vil have adgang eller information fra en beskyttet ressource, vil det første klienten modtager som svar fra serveren en 401 unauthorized, som henviser til at man skal være have et login for at kunne få fat i den ressource. Herfra får klienten mulighed for at kunne indtaste login oplysninger som derefter kan sendes til serveren.
Hvis oplysningerne kan bekræftes og brugeren har adgang til de ressourcer, sender serveren derefter ressourcerne til klienten, ellers bliver der givet en fejlbesked. Hvis brugeren kan blive bekræftet men ikke er tilladt til at få ressourcerne bliver der tilsendt en 403 forbidden.
Brugernavn og password bliver base64 encoded, men base64 er en reversible encoding, som betyder man godt ville kunne se hvad der står. Derfor anses det bedst at som mindste bruge HTTPS for at have bedre sikkerheds instanser på plads.
Det som der anses som et problem med basic auth/basic HTTP er den manglende mulighed for at kunne logge ud, da browseren cacher informationen og ikke får lukket for forbindelsen til serveren.

Basic HTTP

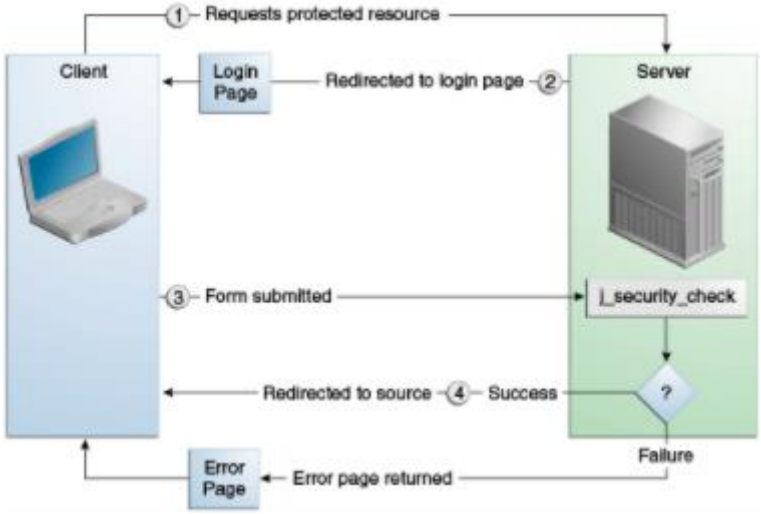


- **Form-based**:

Form based auth er mere programmatisk end basic HTTP. Her menes der at der ikke bliver brugt browserens login, men man i stedet bliver redirekted til en login side hvis klienten ikke har nogle brugeroplysninger. På login siden kan man i en form udfylde sin login oplysninger

som bliver sendt til serveren til verificering. Hvis klienten er verificeret og har tilladelse til at se ressourcerne, bliver ressourcerne sendt. Ellers kommer der en fejl besked med enten en 403 hvis klienten ikke har tilladelse til at se den, eller en 401 hvis oplysningerne ikke kunne verificeres.

Form based Authentication



- **Token based authentication:**

Det gode ved tokens er at de er stateless. Alt informationen bliver indeholdt af selve tokenen hvilket gør det ideelt at bruge det til single page applications, modsat til hvis serveren skulle holde session data.

Det medføre dog også at der er en del sikkerhedsproblemer, siden at al dataen bliver medført med payloaden; nemlig hvis en anden person kan få fat i din token. Hvis det er muligt få fat i en anden persons token, kan de i teorien tage 100% over og dermed udgive sig for at være dig så længe at tokenen er gyldig.