Institutt for datateknikk og informatikk, NTNU

Workshop Sikkerhet

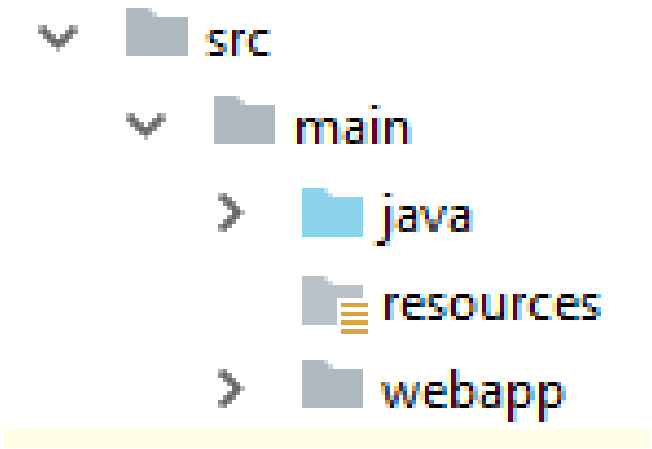
Nils Tesdal
Oppdatert, Tomas Holt

Intro - NotSoSecureBank

- Jeg (Nils) har programmert en enkel nettbank med en del sikkerhetshull
- Den er programmert med
  - JavaScript / jQuery / Bootstrap
  - Rest-tjenester med JAX-RS
  - Database (H2, hvis dere ødelegger databasen underveis kan dere slette fila ***notsosecurebank.mv.db*** i hjemmekatalogen til brukeren på serveren og starte serveren på nytt)
- Dere skal prøve å finne disse sikkerhetshullene
- Dere kan jobbe alene (unntaksvis) eller i små grupper
- Nettbanken kjøres primært på en VM som gruppen får utgitt men kan også kjøres lokalt (localhost).

Maven

- Rammeverk for bygging for Java-prosjekter.
- Dependency-management slik som npm/package.json
- *pom.xml* definerer avhengigheter og eventuelle plugins
- *pom.xml* kan brukes som prosjektfil i mange IDE'er og gjør at man kan samarbeide i team uten å bli enig om EN IDE.
- **sourcen** må ligge på riktig sted:



Oppsett av VM

- Kjøring når banken skal brukes i gruppe bør gjøre på VM som gruppen har fått.
- En på gruppen bruker ssh til å logge på deres VM
  - *ssh brukernavn@ip-adresse* (eksempel student@129.241.97.101)
  - skriv så inn passord
- Nå må Java - **JDK 8!** - installeres og konfigureres
  - *sudo apt-get install openjdk-8-jdk*
  - *sudo update-alternatives --config java*
  - velg openjdk-8 om det blir spørsmål
- Så Maven
  - *sudo apt install maven*

ssh brukernavn@maskinnavn.idi.ntnu.no

Kjøring av NotSoSecureBank

- Last så ned koden/prosjektet for banken (maven-prosjekt)
  - *git clone https://github.com/nilstes/NotSoSecureBank.git*
  - det kan nå være lurt å se igjennom prosjektet og se litt på koden
- Kjør prosjektet via
  - cd NotSoSecureBank/
  - *mvn tomcat:run*
- Da skal Tomcat være opp å kjøre på port 8080 (utskrift og feilmeldinger vil nå vises i konsollet).
- Bruk så nettleser på deres **egne** maskin(er) til å nå tjeneren på VM'en
  - http://<IP-VM>:8080/NotSoSecureBank***/***
  - **merk at den siste / i URL'en er nødvendig!**

<IP-VM> = maskinnavn.idi.ntnu.no

- Bli kjent med banken :)
  - Første gang du logger deg på med en epostadresse blir du registrert som bruker med gitt passord.
  - Registrer en bruker hver og utfør noen transaksjoner...

Oppgave 1 (A3)

- Klarer du å injisere javascript inn i nettsidene?
- Hvilke steder er dette mulig?
- Klarer du å være så ekkel at du legger inn en betaling til sidemannen som gjør at han/hun blir omdirigert til en ondsinnet side med innholdet av cookiene som parameter når han/hun går inn på "konto" i sin nettbank? NB. Bruk samme instans!
- Dette kan fikses med validering, men man bør heller (også) fikse det der verdiene skrives ut.
- Tips: http://stackoverflow.com/questions/24816/escaping-html-strings-with-jquery

Oppgave 2 (A1)

- Klarer du å endre passordet til en annen i gruppa ved å bruke SQL-injection?
- Klarer du å overføre masse penger til deg selv fra en annen i gruppa ved å bruke SQL-injection?
- Tips: Start med å legge inn en enkelt ' i et inputfelt og observer feilmeldingene du får i Glassfish/Tomcat-loggen.
- Tips: For å kjøre flere SQL-setninger kan du skille dem med ;
- Tips: For å kommentere ut resten av linja brukes --
- Tips: Gjør deg kjent med database-tabellene!

Oppgave 3 (A7 og A2)

- Klarer du å finne passordet til en på gruppa di, kun ved å bruke nettleseren?
- Identifiser 2 grove mangler i applikasjonen.