JSF & Security

Možnosti zabezpečení web. aplikace

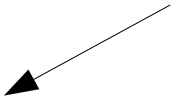
- Máme několik možností, jak zabezpečit web. aplikaci:
  - Java EE security (viz. přednáška Security ze školení Java EE)
  - Spring security (viz. přednáška o Springu)
  - Zabezpečení na úrovni servisní vrstvy pomocí anotací
    - http://docs.oracle.com/javaee/7/tutorial/doc/security-javaee003.htm
  - Programově
    - http://docs.oracle.com/javaee/7/tutorial/doc/security-javaee002.htm#GJGCS
  - Zobrazení kódu na úrovni faceletu podle toho, jakou má uživatel roli

Zobrazení HTML kódu pro uživatele s určitou rolí (Java EE security)

- Jak ve faceletu zobrazit tlačítko pouze pro uživatele s vybranou rolí:

```
<h:commandButton value="Delete" action="#{bean.delete}"
                 rendered="#{request.isUserInRole('administrator')}" />
```

- Nebo:



Tento atribut je také možné nastavit v šabloně, poté bude k dispozici na všech stránkách, které ji používají.

```
<c:set var="isAdmin"
       value="#{request.isUserInRole('administrator')}"
       scope="request" />
<h:commandButton rendered="#{isAdmin}" />
<h:commandButton rendered="#{isAdmin}" />
```

- Tento způsob je imunní vůči CSRF hacku (protože JSF kontroluje platnost podmínky i na serveru):
  - http://cs.wikipedia.org/wiki/Cross-site_request_forgery

Principal name

- Jak získat jméno uživatele ve faceletu?

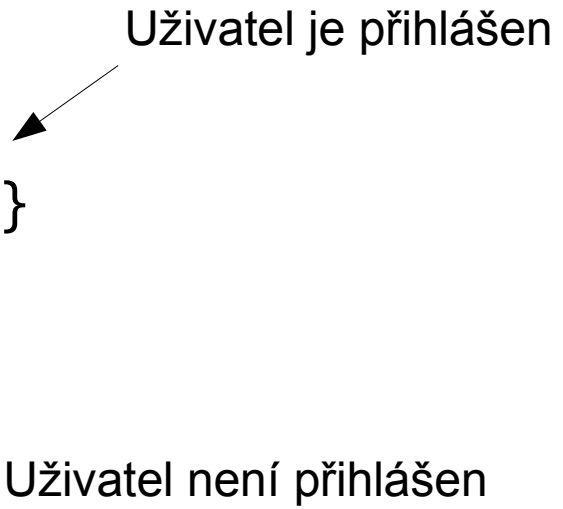
```
#{request.userPrincipal}
```

nebo:

```
#{request.remoteUser}
```

- Jak zjistit jestli je uživatel přihlášen?

```
#{not empty request.remoteUser}
#{empty request.remoteUser}
```



Java EE Security & JBoss

- Jak v JBoss serveru přidat testovacího uživatele?
  - Spusťte `jboss-eap/bin/add-user`
  - Přidejte uživatele typu `b) Application User`