Web 3

Lesson 8: Authorization

EXAM QUESTIONS…

- ☑ What is the difference between authentication and authorization?
- ☑ …

AUTHENTICATION

- Check whether a person that logs in can be authenticated.
  - means that it uses the right credentials (username and password for example)

AUTHENTICATION

- demo webshop

AUTHORIZATION

- Check whether a person has the right role to access particular pages of the web application, is this person authorised to see this page
  - means that an administrator can do more on the web application than a normal user for example

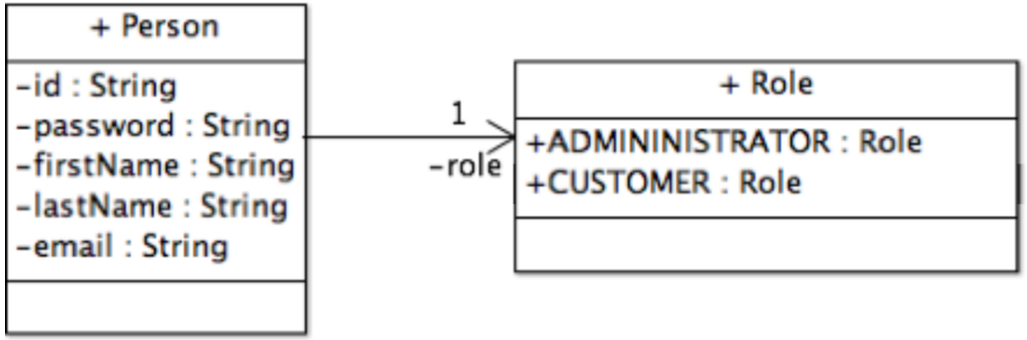
Process of Authorization

- Assign roles
- Log In
- Allow access to specified roles (= authorization)
- Show pages to specified roles

Assign Roles

- treat groups of users as unit
- user can belong to different roles
- specify resources that users in your application are allowed to access

Assign Roles

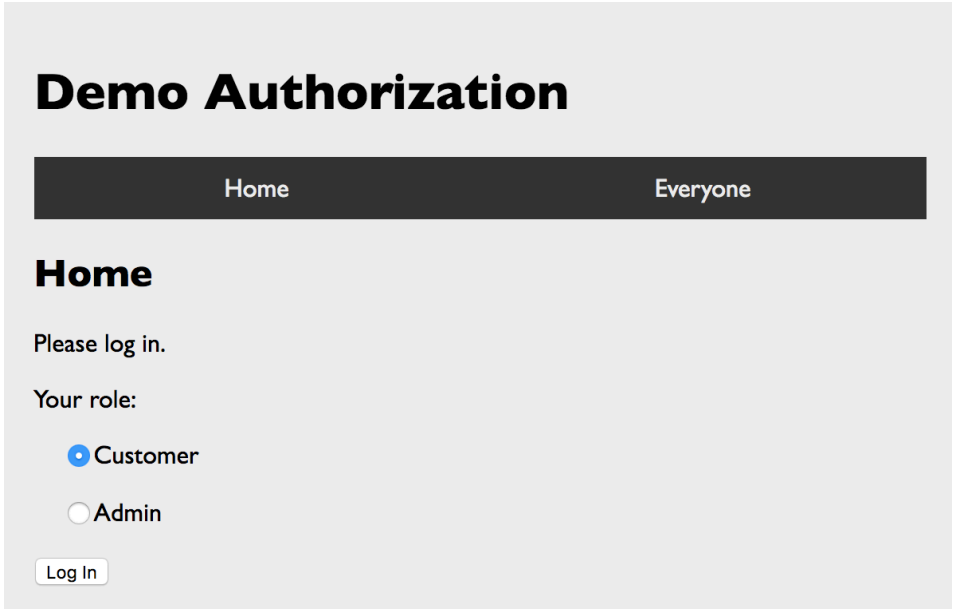


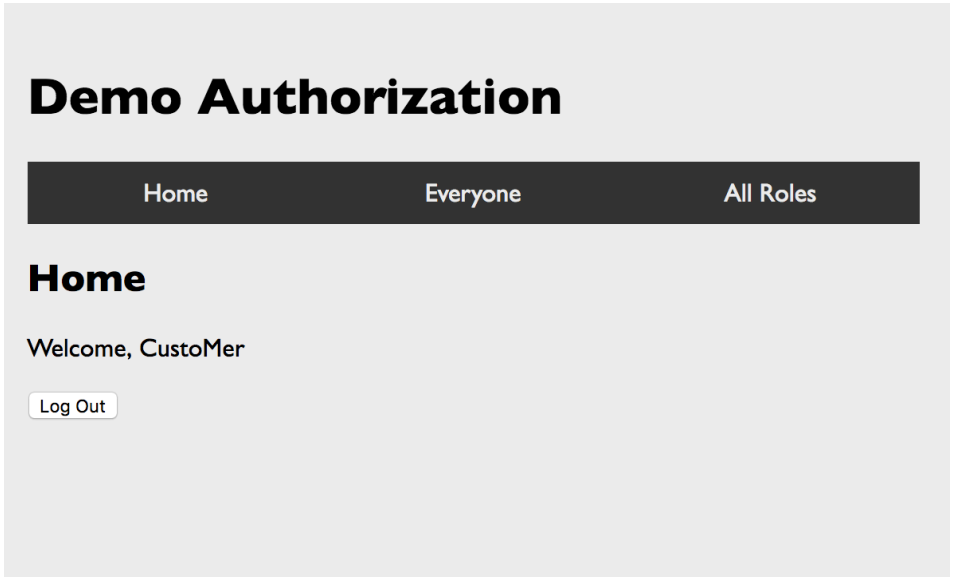

```
public class User {
    String name;
    Role role;

    public User() {

    }

    public User(String name, Role role)
    {
        this.setName(name);
        this.setRole(role);
    }

    …

}
```

```
public enum Role {
    ADMIN, CUSTOMER;

}
```

Log In

- check password
- create session
- store user in session





Log In

```
// Controller
private void logIn(HttpServletRequest request, HttpSession session) {
  // find authenticated user in database
  session.setAttribute("user", user);
}

private void logOut(HttpSession session) {
  session.invalidate();
}
```

```
// index.jsp
…
<p>Welcome, ${sessionScope.user.name }</p>
…
<p>Please log in.</p>
…
```

AUTHORIZATION

- read role from user in session
- if role has access to resource: show page
- if not: throw exception

AUTHORIZATION

```
// Controller

private String admin(HttpServletRequest request) {
    // only Admin has access to “admin.jsp”
    Role[] roles = {Role.ADMIN };
    checkRole(request, roles);
    return "admin.jsp";
}
```

AUTHORIZATION

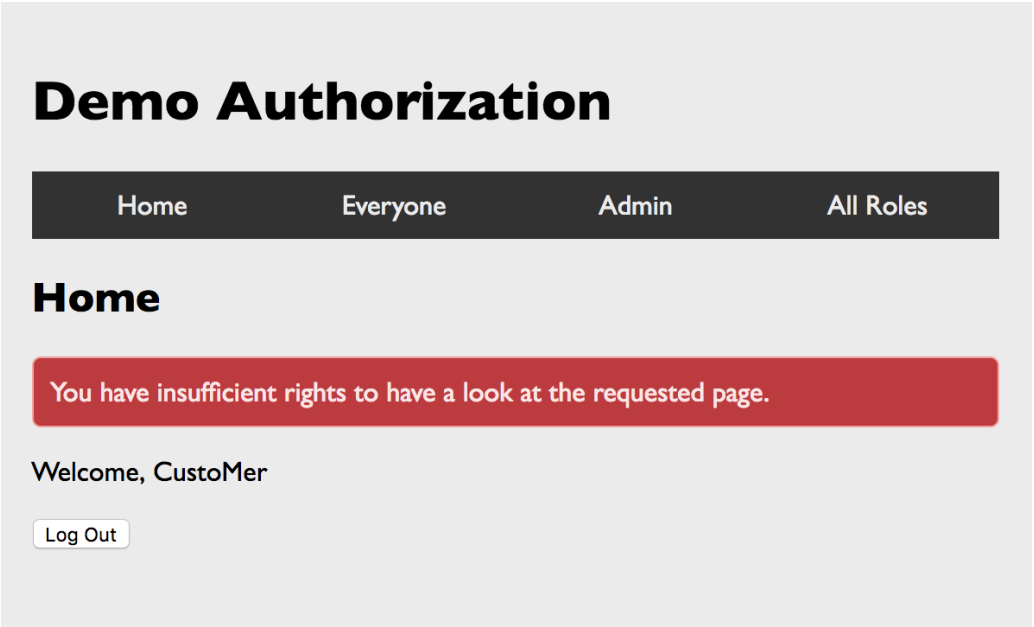
```
public class NotAuthorizedException extends RuntimeException {

    private static final long serialVersionUID = 1L;

    public NotAuthorizedException() {
         super();
    }

    public NotAuthorizedException (String message) {
        super(message);
    }

}
```

AUTHORIZATION

```
// Controller

String destination = "index.jsp";

try {
    switch (action) {
    …
    case "admin":
        destination = admin(request);
        break;
    …
    }
} catch (NotAuthorizedException e) {
    request.setAttribute("notAuthorized",
      "You have insufficient rights to have a look at the requested page.");
}
```

AUTHORIZATION

- handle exception: errorpage/errormessage



Sow pages to specified roles

- show only accessible links