Excluindo JSESSIONID da sessão

Em aplicações Java Web, quando se abre uma nova sessão entre cliente (navegador) e servidor (tomcat) cada usuário possui sua própria identidade que é baseada em um identificador de sessão gerado pelo lado servidor.

Dessa forma o servidor consegue identificar quem está fazendo a solicitação, já que o identificador de sessão é enviado jundo com a solicitação.

O gerenciamento desse mecanismo no lado cliente resulta em um cookie que fica armazenado no navegador. Teoricamente, quado a sessão é finalizada, entre servidor e cliente, esse cookie de sessão expira alguns segundo depois.

No entanto, há clientes (navegadores) que tem o mecanismo de cookie desativado. Nesse caso, o id da sessão precisa ser enviado via URL (enconding). Por isso, algumas vezes vemos o id de sessão como um parte da url:

`http://www.meusite.com.br;jsessionid=0e394s8a576f67b38s7`

No Java, esse identificador recebe o nome de `JSESSIONID` e é possível forçar a exlusão do identificador via configuração no Spring Security. Ao fazer isso, você terá mais segurança que os processos em que trabalhamos nas últimas aulas não gerem algum tipo de excessão caso uma conexão seja feita ou refeita antes mesmo do identificador anterior ter sido deletado.

Para isso, adicione na configuração referente ao logout a seguinte instrução: `deleteCookies("JSESSIONID")`

Resultando em um código similar a este:

```
.and()
    .logout()
    .logoutSuccessUrl("/")
    .deleteCookies("JSESSIONID")
```