07

Autenticando de modo seguro

Atualmente estamos recuperando o conteúdo de autenticação da sessão, mas não conferimos se realmente existe um usuário logado. Uma alteração manual pode gerar uma autenticação falsa e uma falha de segurança no sistema. Vamos aprofundar um pouco mais na autenticação, aumentando a segurança.

Precisamos conferir se existe mesmo um usuário com o email que inserimos na sessão, então precisamos do **UsuarioDAO**. Confirmando que o usuário existe, retornamos seu nome. Caso contrário, retornamos null!

```
package autenticadores;
import play.mvc.Security.Authenticator;
public class UsuarioAutenticado extends Authenticator {
    @Inject
    private UsuarioDAO usuarioDAO;
    @Override
    public String getUsername(Context context) {
        String email = context.session().get(AUTH);
        Optional<Usuario> possivelUsuario = usuarioDAO.comEmail(email);
        if (possivelUsuario.isPresent()) {
            return possivelUsuario.get().getNome();
        }
        return null;
    }
}
```

Isso nos protege contra a alteração dos dados da sessão por terceiros, mas ainda temos duas falhas de segurança que vamos tratar mais pra frente: a exposição do email do usuário e a possibilidade de controle inadequado de uma conta por outro usuário.