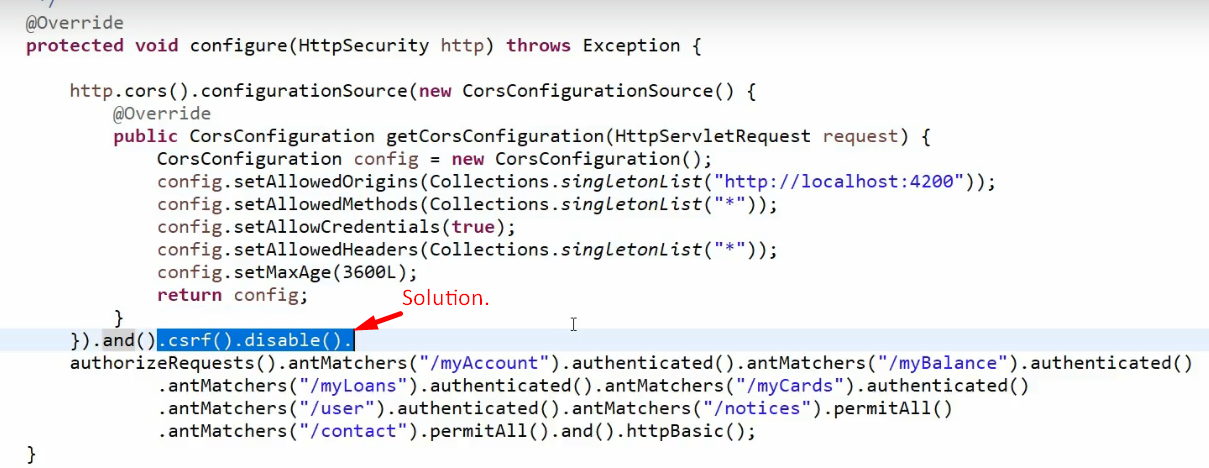
1. In last lecture, we saw
   1. What is CSRF issue?
   2. How a Hacker can perform CSRF attack?
2. **Agenda:**
   1. Handling the CSRF issue.
3. By default, Adding Spring Security dependency enforces the enabling of CSRF meaning no Destructive HTTP methods are allowed if anyone no matter who it is tries to make PUT, DELETE, POST requests, the requests would be responded with 403 FORBIDDEN.
4. **SOLUTION**: The simplest solution is to disable the CSRF.
5. **Scenarios where this can be possible solutions:**
   1. When your app links are not exposed to external world because you have all the firewalls inside your organization.
6. ****
7. **Disabling CSRF**:
   1. It is not a solution always and it’s not recommended also when your app is open to the outside world.
   2. So for that we should really handle CSRF by leveraging CSRF tokens inside our app.