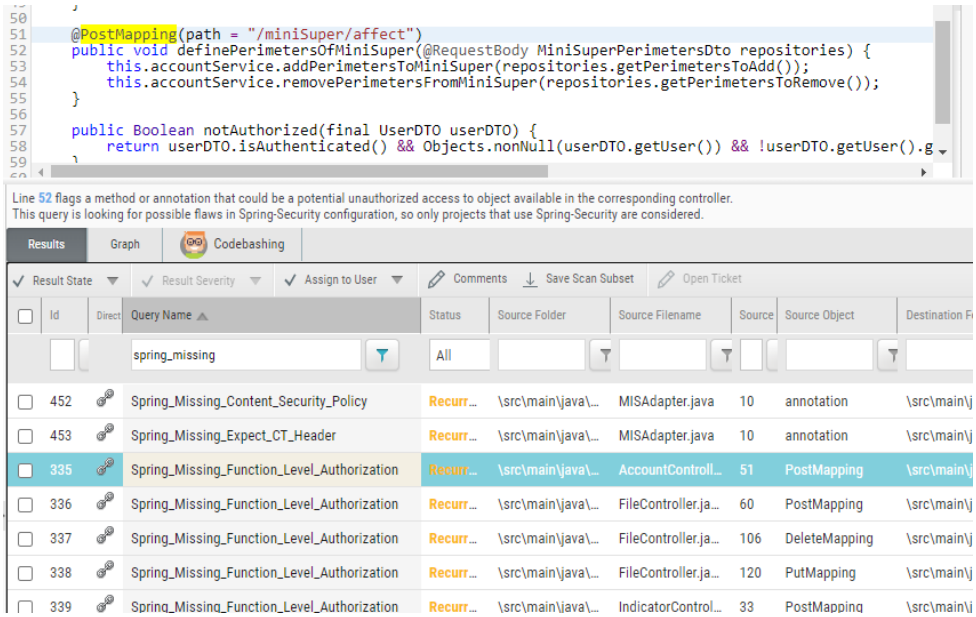
Checkmarx activities – Conduct Backend

Query Name: Improper_Resource_Access_Authorization
Qty: 150 – (37 not exploitable)

Cause: most of them are about sql query and those ones are not exploitable were put with a comment explaining that it is used JPQL with named parameters instead of standard sql language, so I think it is the same for the rest that is similar. Ex.: id 154 and 155 (not exploitable); 245 and 246 (not exploitable).

---------- ********* ----------

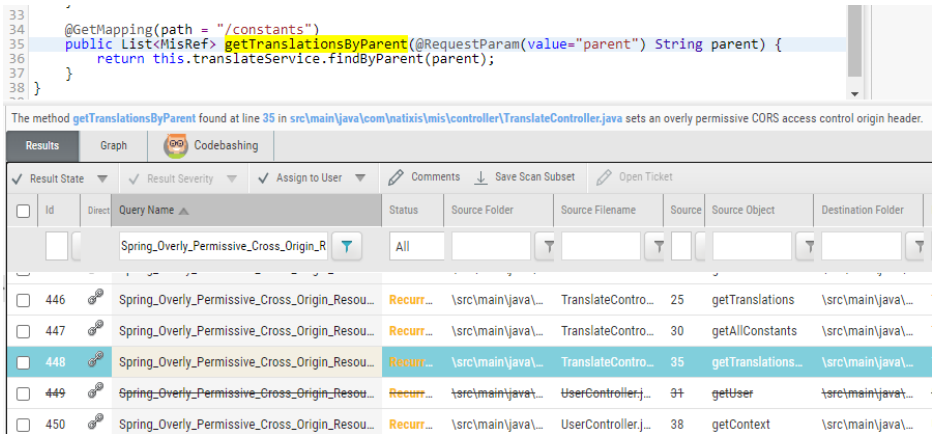
Query Name: Spring_Missing_Object_Level_Authorization and Spring_Missing_Function_Level_Authorization
Qty: 76



Cause: GetMapping annotation. Solutions in the internet point to add the annotation PreAuthorize to check if it is authenticated. Ex.: id 295 and 335.

---------- ********* ----------

Query Name: Spring_Overly_Permissive_Cross_Origin_Resource_Sharing_Policy
Qty: 78



Cause: They are composed by methods in which are annotated with PostMapping and GetMapping. Solutions in the internet point to add white/black list and controlling better instead of using wildcard. Ex.: 448 and 449 (not exploitable – getUser method validates if the user is logged in, if not it redirects to the SSO login page)