**Manual code analysis:**

**Login Authentication:**

We selected some of the majors CWE’s related to the login authentication, for manual code review using previous misuse cases done earlier on the semester. In this analysis we will be focusing on finding code faults related with credential appropriation using brute force attacks, dictionary attacks or by insufficiently protected credentials.

As par of this, we selected a few login authentication related CWE’s, [CWE-798](https://cwe.mitre.org/data/definitions/798), [CWE-307](https://cwe.mitre.org/data/definitions/307.html) and [CWE-259](http://cwe.mitre.org/data/definitions/259). We analyzed mostly of the user and a few admin login related codes for the previous mentioned login attacks. We started by checking the weakness mentioned in CWE-798 and CWE-259 at the same time, since CWE-259 is a child of CWE-798. From this two CWE’s we understand that the threats have two main variation, inbound and outbound, but due to time constrains and the group language ineptitude we were only able to check for the first variation, leaving this analysis incomplete. Latter on, the team checked weakness mention in CWE-307, by checking if the system restricts the number of authentication attempts.

During our manual code analysis on login authentication, we did not notice any hard-code credentials, on the inbound variation, nor we founded errors with the restrictions of excessive authentication attempts. The analysis was based on the weak code suggested from the corresponding CWE.