Phase III

- Welcome to the third phase of the project!
- Your task is to fix all the vulnerabilities detected by you or a second group, starting with the most critical.

Moreover, you need to implement some new functionality!

Phase II

- The bank wants to increase Internet-banking security, because of some recent attacks in the current system which sends unique transaction codes via e-mail.
- Therefore, the bank asks you to implement a new feature for the Internet-banking web-application.
- After a client registers on the bank's website s/he can choose to use the TAN system (TANs are sent as an encrypted file) or to download a personalised Smart-Card-Simulator (SCS) program from the Internet-banking website.
- The SCS program must be implemented in Java and must be secure such that malicious end-users will not be able to hack it.
- Whenever a client wants to transfer an amount of money from his/her account s/he must use the SCS.

Phase II

- The SCS requires the following inputs:
- - the client PIN number
- - the sum of money to transfer
- - the target account, which the sum will be transferred to
- The SCS outputs the a unique transaction code, which must be input on the banking web-site to complete the transfer

- NOTE: This assignment requires you to also adjust the server-side of the web-application you developed in Phase 1 of the project, such that is can validate the transaction code output by the SCS.

Deadline:

Friday the 27th of June (no WorldCup match!) Present your fixes and the new functionality and hand in a VM to the external testing group.