Phase II

- Welcome to the second phase of the project!
- Your task is to assess the security of the application of Phase I in a Black Box fashion and present your results on Tuesday the 24th of June.
- That is, try to find vulnerabilities in the OWASP Top 10 just by interacting with the application front-end (don't look at the sources! we will do that later).
- In particular:
  - Is the application managing sessions securely?
  - SQL-i?
  - XSS? Stored XSS?
  - OS command injections?
  - Secure connections?
  - CSRF?
  - Access control logic?
  - Other logical flaws?

Phase II

- You might use any testing tool in Samurai, or any tool you like. Recommended:
  - Use any proxy (burp, webscarab, ZAP) to understand the actual requests.
  - Use **ZAP** for automatic scanning while navigating the application (setup in firefox similar to what we did with burp)
  - Use **w3af** for automatic testing of common vulnerabilities
  - Use **nikto** to detect configuration vulnerabilities of the system
  - Use **dirbuster** to find hidden files
  - Try to understand the logic of the application and think like an attacker: Can I violate the intuitive security requirements? (steal money, access other persons accounts etc.)

Phase II

- Remember, focus on vulnerabilities as opposed to full fledged exploits.
  - For instance, if the application crashes with a MySQL error when inserting quotes, this is a vulnerability.
  - However if you have time and the vulnerability looks easy to exploit, go for it!
  - Classify the vulnerabilities you find according to its criticality (you decide what is critical, justify it).

Important:

- The tools will report many false positives: verify all findings!
- Report what you found and what you did to find it
- Don't worry if you don't find anything in some category, document your effort (Used Tool X for Y hours)
- Report broken/missing functionality. This must be fixed in the next development phase.
- Prepare a 10 min presentation and a brief document with what you did.

Phase II

- You have to test the application of your own group plus:
  - Group 1 tests Group 3
  - Group 2 tests Group 5
  - Group 3 tests Group 7
  - Group 4 tests Group 8
  - Group 5 tests Group 4
  - Group 6 tests Group 2
  - Group 7 tests Group 8
  - Group 8 tests Group 6

Give the other group a copy of your VM and explain to them briefly how to use the application and provide credentials for privileged system users by the latest on Saturday the 21th at noon.