Project WAS 2015

In groups of 2 or 3 persons, choose one of the following items containing security risks from top-ten OWASP (www.owap.org):

- A1+A3: Injection and XSS
- A2: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5+A6: Security Misconfiguration and Sensitive Data Exposure
- A7+A9: Missing Function Level Access Control
- A10: Unvalidated Redirects and Forwards

The project consists in a research work that should at least include, but not be limited to, the following items:

- A high-level pedagogical description of the security risk(s)
- Code for server and client illustrating an attack (code should not be generated, should be simple, and should be written in php)
- A list of defenses against the attack, starting by the most standard ones. Defenses should be classified into browser/web server/application (cookies and http headers included in this category)
- A study of 5 sites showing if the most common defenses are used
- A study that answers the following question: Do common frameworks/languages/web server implement defenses for this security risk?
- A conclusion

The project deliverable consists of two parts:

- Report: format PDF max 20 pages, sent by email on 19/10/15 before 8am (-1 point for a delay up to 6hours).

- Presentation: 40 minutes+ 10 minutes questions, 21/10 (A1..A4) , 28/10 (A5..A10). Presentations should include at least:
  - A high-level pedagogical description of the security risk(s)
  - Execution of code illustrating the attack
  - A summary of all the results

All students must be present for all presentations: final exam on 18/11 might include questions on the top ten owasp security risks. In particular, please pay attention and take notes on the high-level pedagogical descriptions and the code illustrating the attack. The project will be grade and its grade will be weighted as 1/2 of the final note.