AS Lab Assignment

Web Security

In this assignment, you will get familiar with the common security issues on the web and how they are performed. The OWASP community provides a number of exercises that demonstrate such issues in their Security Knowledge Framework.
Labs: https://demo.securityknowledgeframework.org/labs/view
Sources: https://github.com/blabla1337/skf-labs

Follow mini-labs provided by Security Knowledge Framework. You can launch labs in the cloud or in your local environment from sources.

Mini-lab list:

- Cross site scripting
- Cross site scripting (attribute)
- Cross site scripting (href)
- CSS Injection
- XSSI
- Cross site request forgery
- Cross site request forgery (same site)
- Cross site request forgery weak
- Clickjacking
- Content security policy
- CORS exploitation
- Path traversal (LFI)
- Remote file inclusion (harder)
- Remote file inclusion (hard)
- Open redirect
- Open redirect (hard)
- Insecure file upload
- Remote file inclusion
- SQLI (union select)
- SQLI - like
- SQLI - blind
- Insecure direct object reference

- Right to left override attack
- Rate-limiting
- Regex Ddos
- Command injection
- Command injection (easy)
- Command injection (harder)
- Information disclosure 1
- Information disclosure 2
- Authentication bypass (easy)
- Authentication bypass
- Authentication bypass (harder)
- Authentication bypass (hard)
- Authentication bypass
- HttpOnly (session hijacking)

For each lab, perform exploitation and briefly describe how to fix the issue in the particular code of the mini-lab. For that you may need to look at the source code and reference information about prevention that can be found at the end of corresponding lab write-up.

Submission should contain:

- report with descriptions of your proposed fixes for each lab

In addition, there is number of materials that also my help you to understand concepts better:
https://cheatsheetseries.owasp.org/cheatsheets/
https://developer.mozilla.org/en-US/docs/Web/Security
https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns
https://infosec.mozilla.org/guidelines/web_security
https://developer.mozilla.org/en-US/docs/Learn/Server-side/First_steps/Website_security
https://owasp.org/www-community/