Application Security

Exercise Set 2

In order to solve the following problems all technologies are allowed.

1. Prepare a simple web application vulnerable to SQL injection. Trace the execution and demonstrate the malicious behaviour. Show how to fix the application, i.e. demonstrate the valid scheme which prevents SQL injection.
[2p]

2. Prepare three simple web applications vulnerable to: reflected XSS, stored XSS and DOM XSS. Trace the execution and demonstrate the malicious behaviour. Check libraries and capabilities of the selected technology to prevent XSS.
[2p]

3. Prepare an example web application which demonstrate how the *Content-Security-Policy* and *Content-Security-Policy-Report-Only* headers work and prevent XSS. Check at least 4 directives including *report-uri* and *connect-src.*
[2p]

4. Prepare an example web application which demonstrate how the *X-XSS-Protection* header works and prevents XSS.
[2p]

5. Prepare an example web application which stores sensitive data in a cookie. Show how to manipulate the cookie content. Extend the example in the following ways:

- by applying a MAC to secure the integrity,
- by applying an encryption to secure the confidentiality,
- by applying both a MAC and an encryption secure both requirements.

[2p]

Paweł Rajba