Exercise sheet 01

Submit individually (1 person) or as a group (max. 3 persons).

1. Web Application Vulnerabilities (Without Time Constraints)

1.1. Create an account with root-me.org.
1.2. Solve 2 of the challenges in the category Challenges => Web-Client that have a name starting with "XSS". [Groups: 2 challenges per group member, e.g., 6 challenges for 3 persons]
1.3. Solve 5 of the challenges in the category Challenges => Web-Server that have a name starting with "HTTP". [Groups: All challenges starting with “HTTP”]
1.4. Document for each challenge what you did, what tools you used, what worked and what did not work.

2. Web Application Vulnerabilities (With Time Constraints)

2.1. Pick a Capture the flag (CTF) event from ctftime.org in Jeopardy format.
2.2. Participate in a CTF event, solve 2 of the challenges in the “web” category and 1 challenge in another category of your choice. [Groups: 3 challenges per group member; large groups may participate in multiple CTFs to solve enough challenges]]
2.3. Document for each challenge what you did, what tools you used, what worked and what did not work.
2.4. Prove your participation in the CTF event with a screenshot of the scoreboard.

3. Known Real-World Software Vulnerabilities

The NVD National Vulnerability Database is a compilation of known vulnerabilities in products. What are known vulnerabilities published for openssl in 2024? (Note that date of discovery and date of publication might be different.)

3.1. List all vulnerabilities with CVE ID and severity and select one for the following tasks.
3.2. Show the vulnerability in the source code version before detection of the vulnerability.
3.3. Show how the vulnerability was fixed/removed based on a source code version released after the vulnerability was discovered. Describe how the fix works.
3.4. For the vulnerability, point out the type of vulnerability using an appropriate CWE ID.
3.5. What can developers learn from the vulnerability? Could that type of vulnerability have been avoided/found earlier? If so, how? If not, why is it hard?

Answers must be submitted in Moodle as a single PDF file following the naming convention:
Exercise01-YourLastName-YourFirstName.pdf
Example: Exercise01-Mustermann-Erika.pdf
For groups, the submission must include names and student numbers of all group members and the naming convention for the pdf file is different:
Exercise01-YourLastName1-YourLastName2-YourLastName3-YourLastName4.pdf
Example: Exercise01-Schmidt-Mueller-Meier-Schulze.pdf