Assignment 4

Purpose: XSS vulnerabilities – Web Session Hijack.

In this assignment students must demonstrate theft a the session id cookie.

To complete the assignment, students must record a video of up to 2-4 minutes showing how exploit and obtain the victim`s session id. (some procedure like assignment 1)

Assignment steps:

1.Students will form teams of two. (a student is ATTACKER and another is VICTIM). The both students needs to be in the **same network**.*

2.The VICTIM follows all the steps from Victim Setup.

3.The ATTACKER will download NC.zip, will extract NC.exe from the archive and starts it from the command prompt with the following command: nc -nlvp 81.

4.The ATTACKER accesses the login page on the VICTIM's system: http://VICTIM_IP/login.php and logs in using user=raul, pass=passraul.

5.The ATTACKER posts the XSS message (see below), replacing ATTACKER_IP with the attacker's own machine IP.

6.The ATTACKER logs out of the application (must return to the login page).

7.The VICTIM re-accesses login.php while being logged in (refresh, F5, etc.).

8.The ATTACKER monitors what happens in the Command Prompt, waiting for a request from the VICTIM, which includes the victim's cookie (it should look like in the image hint.).

9.The ATTACKER installs and starts BURP Proxy and sets the following proxy in the browser: 127.0.0.1, port 8080.

10.The ATTACKER refreshes (F5) the login page (the access will be intercepted by the proxy).

11. The ATTACKER analyzes the HTTP request in BURP Proxy (it should look like in image xss_hint.png). They will add the following line in the headers, replacing it with the victim's session ID (collected via NC), then press "Forward":

Cookie: PHPSESSID=xxxxxxxxxxxxxxxxxxxxxxxxxxx

If a Cookie header already exists in the request, only the PHPSESSID value is replaced with the victim's.

12.At this moment, the ATTACKER should be logged in with the same user as the VICTIM.

* The exercise can also be performed by a single student using a virtual machine, in which case the host machine will be the ATTACKER and the virtual machine will be the VICTIM. In this case the video should contains the all above steps (without victim setup).

Victim Setup steps:

1. Download and install XAMPP (google it) (for windows, i suggest to install in c:/xampp with admin rights)

2. Download login.txt and rename it to login.php

3. Put login.php in C:/xampp/htdocs

4. Download tables.sql

5. Start MySQL server and Apache server from XAMPP Controle Panel.

6. Open in browser http://localhost/phpmyadmin

7. Select (or create) 'test' database from the menu on the left

8. From the upper menu, select the SQL option (allows entering SQL commands)

9. Paste the contents of tables.sql file in the text field, and click Go (lower-right corner)

10. Open in browser http://localhost/login.php and login with user=admin, pass=passadmin.

Others:

- Each student will record their own part.
- The videos must be synchronized, with the same date/time and the same session ID visible in both recordings.
- The videos must capture the entire screen, not just some windows.
- These steps were designed for the Windows operating system. If you are using a different operating system, you will need to find and use the appropriate versions of the programs for your operating system.
- Victim setup steps (install and setup the xampp) should not be recorded.

Deadline: 14.01.2026