Poznan University of Technology
Faculty of Computing and Telecommunications

michal.apolinarski[at]put.poznan.pl

Course: Application Security – laboratories

Lecturer: Michał Apolinarski, Ph.D.

Topic: Security audit – black-box approach

Duration (on site): 180 min.

PREREQUISITES:

Knowledge of computer networks, operating systems, cryptography. Knowledge of programming languages, basic knowledge of penetration tests.

GOALS:

- The aim of the class is to perform penetration tests in **a black-box approach** of your / your colleagues' / open-source software to find any vulnerabilities that results in access gain to unauthorized operations and malfunction.
- Preparing a report of the performed tasks.

INSTRUCION (tasks for a group of max 2 persons):

1. As the target of security audit choose:
    a. custom application developed and shared by your colleagues' during this course,
    b. open-source application from previous classes of this course,
    c. your own applications (if you don’t have above options).
2. Penetrations tests should be perform in a black-box approach, and documented by screenshots that’s presents obtained results.
3. Run Kali Linux on your computer – its recommended to use virtual environment like VirtualBox,
4. Familiarize yourself with the available tools available dedicated for web apps / database and password analysis.
5. Perform security tests using tools available in Kali OS:

   a. Burp Suite
   b. Nikto
   c. Maltego
   d. OWASP-ZAP
   e. Paros
   f. skipfish
   g. SQLMap
   h. …
6. Perform tests using other tools like:
   a. HORUSEC
   b. Nessus
   c. Nmap
   d. Salus
   e. Snyk
   f. SonarQube
   g. Wapiti
   h. XSStrike
   i. …
7. Perform own manual tests.
8. Prepare and send to the lecturer a report of performed tests (positive and false), results and your analysis.

REPORT:

- Should include a title page with full details of the student, course and exercise being reported.
- Should be carefully edited and provide evidence of the completion of all exercises confirmed by screenshots, answers and conclusions.
- Complete report should be send to the lecturer.