Fachbereich Informatik
Prof. Dr. Reiner Hüttl

IT-Security

Exercise 9

In this exercise, we will cover the topic of attacks on a web application

For the exercise we use the "OWASP Mutillidae 2 Web Pen Test Training Environment". This application is freely available on the web and has vulnerabilities to all TOP 10 OWASP.

Task 1: Installation of the application

All information about the Mutillidae project you find here:
https://owasp.org/www-project-mutillidae-ii/

There are three ways to install the Mutillidae PHP application on your computer:

- Installation on LAMP stack
- **Installation on Docker**
- Installallation with DockerHub

We take the **installation on Docker**, so we have a virtual environment for our attcks to the application, wich is more safe for our computer.

Go to the Mutillidae-Docker projekt
https://github.com/webpwnized/mutillidae-docker

There you can find the code and installation hints and videos.

You need on your compter the Docker Engine, the Docker CLI and Docker Compose.
If you install Docker Desktop https://www.docker.com/products/docker-desktop/ you get all in one and additional a Docker Desktop GUI.

Next step is to clone the Mutillidae-Docker project from GitHub.

Next step is to navigate in CMD Shell (or Terminal-App on MAC) to the directory with the file *docker-compose.yml*

Start the 5 containers (www-Apache, database-MySQL, daabase_admin-PHPAdmin, ldap-OpenLDAP, ldap_admin-PHPLDAPAdmin) with the command:
docker-compose up
On Mac the command is: *docker compose up*

Start the Application in your Browser under http://127.0.0.1
or in Docker Desktop with the container www

Task 2: Explore and attack the application

Now you can explore the Mutillidae application and try to exploit the vulnerabilities.