|  |  |
| --- | --- |
| **Practicum Case** |  |
| COMP6548  Programming for Penetration Testing |
| **Cyber Security** | **O221-COMP6548-WU01-11** |
| ***Valid on*** *Odd Semester Year 2021/2022* | **Revision 00** |

## Learning Outcomes

* Socket Network Program for Penetration Testing
* Web Vulnerability with Programming
* Additional tools for Penetration Testing

## Topic

* Web Application Attack

## Subtopics

* Basic SQL Injection Attack for MySQL
* Create SQL Injection Automation Tool
* Dump SQL Data through SQL Injection using Python

## Soal

*Case*

**SQLMap**

You are asked again to attack a website, but this time you need to test how the website can handle SQL Injection. You need to make tool like SQLMap, but simpler by using **Python Programming Language**. Here are the requirements:

1. There is a folder called 11-web in the zip, you need to copy it to your **Document Root** folder (the default folder is in “C:/xampp/htdocs”).
2. Open XAMPP Control Panel.
3. Press “Start” button on a module called “Apache”.
4. Try opening the website on your browser.
5. Open your **phpMyAdmin** on your browser.
6. Create a database called **progpentest1011**.
7. Import the **.sql** file in **11-web** folder (**file.sql**).
8. Open the website on the browser, it should look like below.

A picture containing text, person, posing, group

Description automatically generated

Figure 1. The Website after Configuration

1. You can add an **argument parser** (with **getopt** for example), it is optional.
2. The Program can retrieve the following information from the database:
   1. Database Name (the one that website uses currently)
   2. Table Name
   3. Every Table’s Column Name
   4. Every Data from Every Table in that Database

Graphical user interface, application, table, Excel

Description automatically generated

Figure 2. Dumping Data from Database\*

\* The table format was made with **Pandas** and **Tabulate**. It is also optional. You can use default **print()** method if you want.