**CIT 485 ADVANCED CYBERSECURITY-**

**Lab11: ﻿** **Attack Types and Automation Concepts**

## **Lab11-1 Attack Types(70-points)**

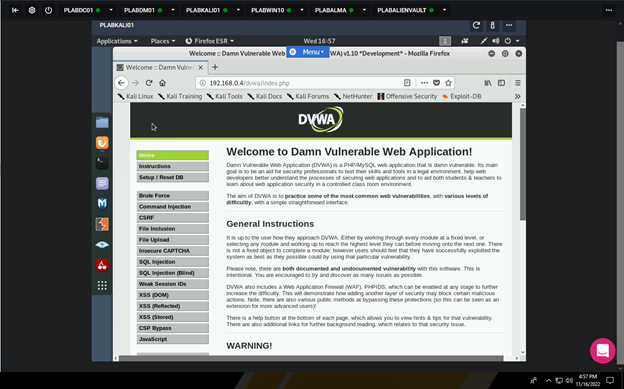
**Lab Submission**

**Exercise 1 - Web Application Exploits**

**Task 1 - Verify that the DVWA is running**

Perform the Step 1 - Step 15 Verify that the DVWA is runningand copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

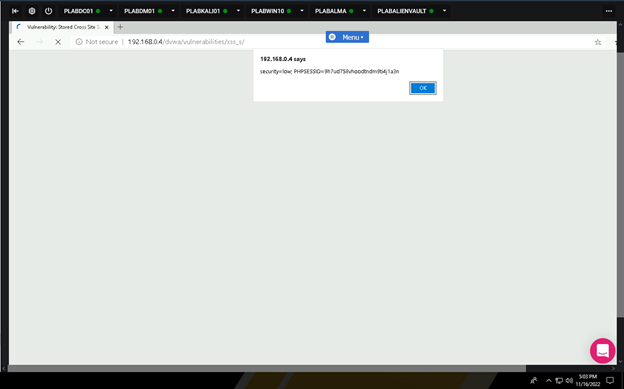
**Verifying that the DVWA is running**



**Task 2 - Perform a Cross-site scripting attack (XML)**

Perform the Step 1 - Step 18 Perform a Cross-site scripting attack (XML)and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

**Performing a Cross-site scripting attack (XML)**

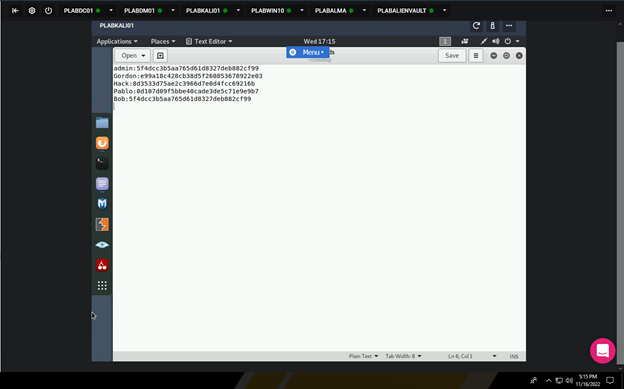


**Exercise 2 - Database Attack Types and Exploits**

**Task 1 - Conducting a SQL injection exploit**

Perform the Step 1 - Step 27 Conducting a SQL injection exploit and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

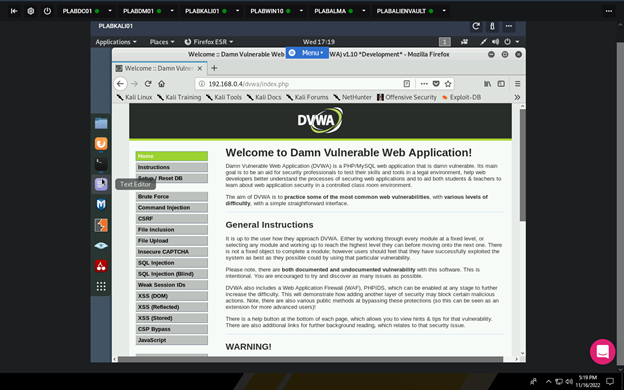
**Conducting a SQL injection exploit**



**Task 2 - Cracking the captured password hashes using John the Ripper**

Perform the Step 1 - Step 11 Cracking the captured password hashes using John the Ripper and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

**Cracking the captured password hashes using John the Ripper**



· **Save the report as a docx file (first name and last name: ex. Awad\_Mussa1.docx)**

· **Keep this file as you will upload it when you take the lab10’s quiz.**