

EN4720: Security in Cyber-Physical Systems

Exercise — Application Security

Name: Thalagala B. P.
Index No: 180631J

June 15, 2023

This is an individual exercise!
Due Date: 20 June 2023 by 11.59 PM

This exercise has to be carried out using a **Linux-based virtual machine**. Read all the instructions and questions before attempting the exercise. Add answers under each question in the Questions section and submit the resulting PDF.

Instructions

1. Objective of this exercise is to perform a web application security assessment using OWASP ZAP (Zed Attack Proxy) on Ubuntu and identify potential vulnerabilities based on the OWASP Top 10 (2017) list. Download and install the latest version of OWASP ZAP from the official OWASP ZAP website (<https://www.zaproxy.org/download/>).
2. Make sure you are using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode.
3. Download and install DVWA (Damn Vulnerable Web Application) on your Ubuntu system. You can find the installation instructions and the necessary files on the official [DVWA GitHub repository](#). Please follow the steps carefully in the GitHub repository.
4. Configure Proxy Settings: Configure your web browser or system network settings to use OWASP ZAP as a proxy. This will allow OWASP ZAP to intercept and analyze the web application's traffic.
5. Scan for Vulnerabilities: Use OWASP ZAP to perform an active, automated scan on the DVWA application. OWASP ZAP will analyze the captured traffic and identify potential vulnerabilities within DVWA. You will have to analyze the results and detect which OWASP Top 10 category each vulnerability belongs to.

Questions

For all the questions in this section, add a screenshot of the terminal (including all the commands you ran to perform the task) unless specified otherwise. The evaluator should be able to see each step that you followed to perform each task. In all screenshots, the areas marked (which are unique to your terminal display) in Figure 1 (the sample answer to Question 1) must be visible.

1. View the currently logged in user.

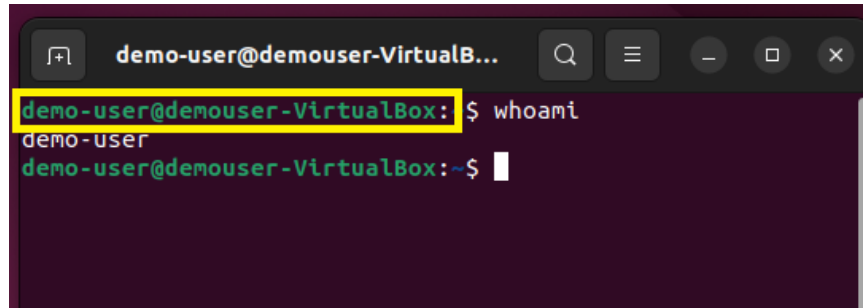
A screenshot of a terminal window with a dark background. The title bar at the top shows 'demo-user@demouser-VirtualB...'. The terminal content shows the prompt 'demo-user@demouser-VirtualBox: \$' followed by the command 'whoami'. The output 'demo-user' is displayed on the next line. The prompt then changes to 'demo-user@demouser-VirtualBox:~\$'.

Figure 1: Sample Terminal Output

2. Using the **ifconfig** command, check your network settings and determine if your network is configured to use NAT (Network Address Translation). Provide a screenshot of the ifconfig output and explain how to identify the use of NAT by examining the network information displayed in the **ifconfig** output.

Your answer here

3. Follow the instructions in github repository and add a screenshot of the database credentials. You may use vim command to check default credentials in **./config/config.inc.php** file.

Your answer here

4. Add a screenshot of the list of detected vulnerabilities.

Your answer here

5. Briefly describe each detected vulnerability.

Your answer here

6. Complete the below table by identifying each vulnerability, including its impact, detected source paths, evidence, and potential OWASP top 10 attack scenarios.

Table 1: Vulnerability details

Vulnerability	Impact	Evidence	Potential OWASP top 10 attack scenarios
Absence of Anti-CSRF Tokens	Medium	<form action="#" method="post">	CSRF

7. Identify solutions for each listed vulnerability.

Your answer here