❖ **TryHackMe Labs - OWASP Top 10:**

1. Insecure Direct Object Reference

- Description: IDOR or Insecure Direct Object Reference refers to an access control vulnerability where you can access resources you wouldn't ordinarily be able to see. This occurs when the programmer exposes a Direct Object Reference, which is just an identifier that refers to specific objects within the server. By object, we could mean a file, a user, a bank account in a banking application, or anything really.
- Exploitation: Deploy the machine and go to http://MACHINE_IP - Login with the username noot and the password test1234
- Lab: Look at other users' notes. What is the flag?
- Solution: flag{fivefourthree}

2. Cryptographic Failures

- Description: A cryptographic failure refers to any vulnerability arising from the misuse (or lack of use) of cryptographic algorithms for protecting sensitive information. Web applications require cryptography to provide confidentiality for their users at many levels.
- Exploitation: Have a look around the web app. The developer has left themselves a note indicating that there is sensitive data in a specific directory.
- Lab: What is the name of the mentioned directory?
- Solution: /assets
- Lab: Navigate to the directory you found in question one. What file stands out as being likely to contain sensitive data?
- Solution: webapp.dp
- Lab: Use the supporting material to access the sensitive data. What is the password hash of the admin user?
- Solution: 6eea9b7ef19179a06954edd0f6c05ceb
- Lab: Crack the hash.What is the admin's plaintext password?
- Solution: qwertyuiop
- Lab: Log in as the admin. What is the flag?
- Solution: THM{Yzc2YjdkMjE5N2VjMzNhOTE3NjdiMjdl}

3. Command Injection

- Description: Command Injection occurs when server-side code (like PHP) in a web application makes a call to a function that interacts with the server's console directly. An injection web vulnerability allows an attacker to take advantage of that call to execute operating system commands arbitrarily on the server. The possibilities for the attacker from here are endless: they could list files, read their contents, run some basic commands to do some recon on the server or whatever they wanted, just as if they were sitting in front of the server and issuing commands directly into the command line.
- Exploitation:To complete the questions below, navigate to http://MACHINE_IP:82/ and exploit the cowsay server.
- Lab: What strange text file is in the website's root directory?
- Solution: drpepper.txt
- Lab: How many non-root/non-service/non-daemon users are there?
- Solution: 0
- Lab: What user is this app running as?
- Solution: apache
- Lab: What is the user's shell set as?
- Solution: /sbin/nologin
- Lab: What version of Alpine Linux is running?
- Solution: 3.16.0

4. Insecure Design

- Description: Insecure design refers to vulnerabilities which are inherent to the application's architecture. They are not vulnerabilities regarding bad implementations or configurations, but the idea behind the whole application (or a part of it) is flawed from the start.
- Exploitation:Navigate to http://MACHINE_IP:85 and get into joseph's account. This application also has a design flaw in its password reset mechanism.
- Lab: What is the value of the flag in joseph's account?
- Solution: THM{Not_3ven_c4tz_c0uld_sav3_U!}

5. Security Misconfiguration

- Description: Security Misconfigurations are distinct from the other Top 10 vulnerabilities because they occur when security could have been appropriately configured but was not. Even if you download the latest up-to-date software, poor configurations could make your installation vulnerable.
- Exploitation:Navigate to http://MACHINE_IP:86 and try to exploit the security misconfiguration to read the application's source code.
- Lab: Use the Werkzeug console to run the following Python code to execute the ls -l command on the server:import os; print(os.popen("ls -l").read())What is the database file name (the one with the .db extension) in the current directory?
- Solution: todo.db
- Lab: Modify the code to read the contents of the app.py file, which contains the application's source code. What is the value of the secret_flag variable in the source code?
- Solution: THM{Just_a_tiny_misconfiguration}

6. Vulnerable and Outdated Components

- Description:Occasionally, you may find that the company/entity you're pen-testing is using a program with a well-known vulnerability.Recall that since this is about known vulnerabilities, most of the work has already been done for us. Our main job is to find out the information of the software and research it until we can find an exploit. Let's go through that with an example web application.
- Exploitation:Navigate to http://MACHINE_IP:84 where you'll find a vulnerable application. All the information you need to exploit it can be found online.
- Lab: What is the content of the /opt/flag.txt file?
- Solution: THM{But_1ts_n0t_my_f4ult!}

7. Identification and Authentication Failures

- Description:Authentication and session management constitute core components of modern web applications. Authentication allows users to gain access to web applications by verifying their identities. The most common form of authentication is using a username and password mechanism.
- Exploitation:Go to http://MACHINE_IP:8088 and try to register with darren as your username. You'll see that the user already exists, so try to register " darren" instead, and you'll see that you are now logged in and can see the content present only in darren's account, which in our case, is the flag that you need to retrieve.
- Lab: What is the flag that you found in darren's account?
- Solution: fe86079416a21a3c99937fea8874b667
- Lab: What is the flag that you found in arthur's account?
- Solution: d9ac0f7db4fda460ac3edeb75d75e16e

8. Software and Data Integrity

- Description:When talking about integrity, we refer to the capacity we have to ascertain that a piece of data remains unmodified. Integrity is essential in cybersecurity as we care about maintaining important data free from unwanted or malicious modifications.
- Exploitation:You can go to https://www.srihash.org/ to generate hashes for any library
- Lab: What is the SHA-256 hash of https://code.jquery.com/jquery-1.12.4.min.js?
- Solution: sha256-ZosEbRLbNQzLpnKIkEdrPv7lOy9C27hHQ+Xp8a4MxAQ=
- Exploitation:Navigate to http://MACHINE_IP:8089/ and follow the instructions in the questions.
- Lab: Try logging into the application as guest. What is guest's account password?
- Solution: guest
- Lab: What is the name of the website's cookie containing a JWT token?
- Solution: jwt-session
- Lab: What is the flag presented to the admin user?
- Solution: THM{Dont_take_cookies_from_strangers}

9. Security Logging and Monitoring Failures

- Description:When web applications are set up, every action performed by the user should be logged. Logging is important because, in the event of an incident, the attackers' activities can be traced. Once their actions are traced, their risk and impact can be determined. Without logging, there would be no way to tell what actions were performed by an attacker if they gain access to particular web applications.
- Exploitation: You can download it by clicking the Download Task Files button at the top of the task.
- Lab: What IP address is the attacker using?
- Solution: 49.99.13.16
- Lab:What kind of attack is being carried out?
- Solution: Brute Force

10. Server-Side Request Forgery

- Description:This type of vulnerability occurs when an attacker can coerce a web application into sending requests on their behalf to arbitrary destinations while having control of the contents of the request itself. SSRF vulnerabilities often arise from implementations where our web application needs to use third-party services.
- Exploitation: Navigate to http://MACHINE_IP:8087/, where you'll find a simple web application. After exploring a bit, you should see an admin area, which will be our main objective. Follow the instructions on the following questions to gain access to the website's restricted area!.
- Lab: Explore the website. What is the only host allowed to access the admin area?
- Solution: localhost

- Lab: Check the "Download Resume" button. Where does the server parameter point to?
- Solution: secure-file-storage.com
- Lab:Using SSRF, make the application send the request to your AttackBox instead of the secure file storage. Are there any API keys in the intercepted request?
- Solution:THM{Hello_Im_just_an_API_key}