

Week 5 Assignment 1: Introduction to Web Applications

Course: Cloud and Network Security C3-2024

Student Name: **Loise Murugi Murage**

Student No: **CS-CNS07-24115.**

Friday, October 25, 2024

Week 5 Assignment 1

Class Exercise: Introduction to Web Applications

Week 5 Assignment 1: Introduction to Web Applications

Contents

Class Exercise: Introduction to Web Applications	1
Introduction	3
Questions	4
HTML	4
CSS	4
JavaScript	5
Cross-Site Scripting XSS	7
Cross-Site Request Forgery	9
Web Servers	10
Databases	11
Development Frameworks & APIs	12
Common Web Vulnerabilities	13
Public Vulnerabilities	15
Conclusion	16

Introduction

In this module, we will be looking at web applications. Web applications are application software that are accessed through a web browser without installing or downloading them e.g. the G Suite, Microsoft Office 365, while websites are typically more static, focusing on providing information and showcasing content. There are many open source web applications used by organizations that can be customized to meet the organization's needs e.g. Joomla, opencart and WordPress. There are closed source web applications developed by organizations and sold to other organizations through subscription plan methods.

We will look at the web application divided into four types that is the client server; The server hosts the web application in a client-server model and distributes it to any client trying to access it, one server; the web applications and their components, databases are hosted on a single server. Many servers one database; This model separates the database onto its own database server and allows the web applications' hosting server to access the database server to store and retrieve data. Many servers many databases; each web application's data is hosted in a separate database, the web application can access private data and only common data is shared across web applications.

The web application architecture is divided into three Layers; Presentation layer consists UI process components that enable communication with the application and the system, these can be accessed by the client via web browser and are returned in the form of HTML, JavaScript and CSS, Application layer ensures that all client requests (web requests) are correctly processed. Various criteria are checked such as authorization, privileges and data passed on the client. Data Layer works closely with the application layer to determine exactly where the required data stored and can be accessed.

Frontend refers to the graphical user interface (GUI) that your users can directly interact with, such as navigation menus, design elements, buttons, images, and graphs while the backend sometimes called the server side, the backend of your application manages your web application's overall functionality. When your user interacts with the frontend, the interaction sends a request to the backend in HTTP format. The backend processes the request and returns a response.

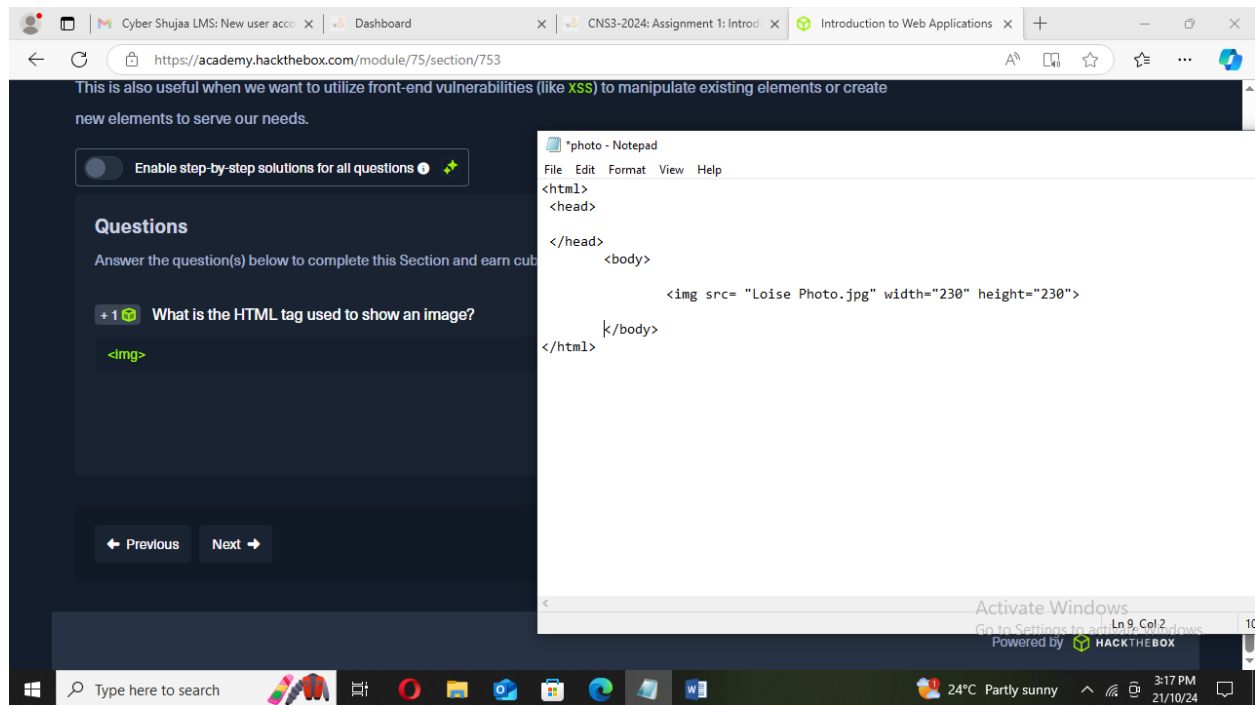
Week 5 Assignment 1: Introduction to Web Applications

Questions

HTML

HTML (Hyper Text Markup Language) is the standard markup language for documents designed to be displayed in a web browser. It defines the content and structure of web content.

What is the HTML tag used to show an image?



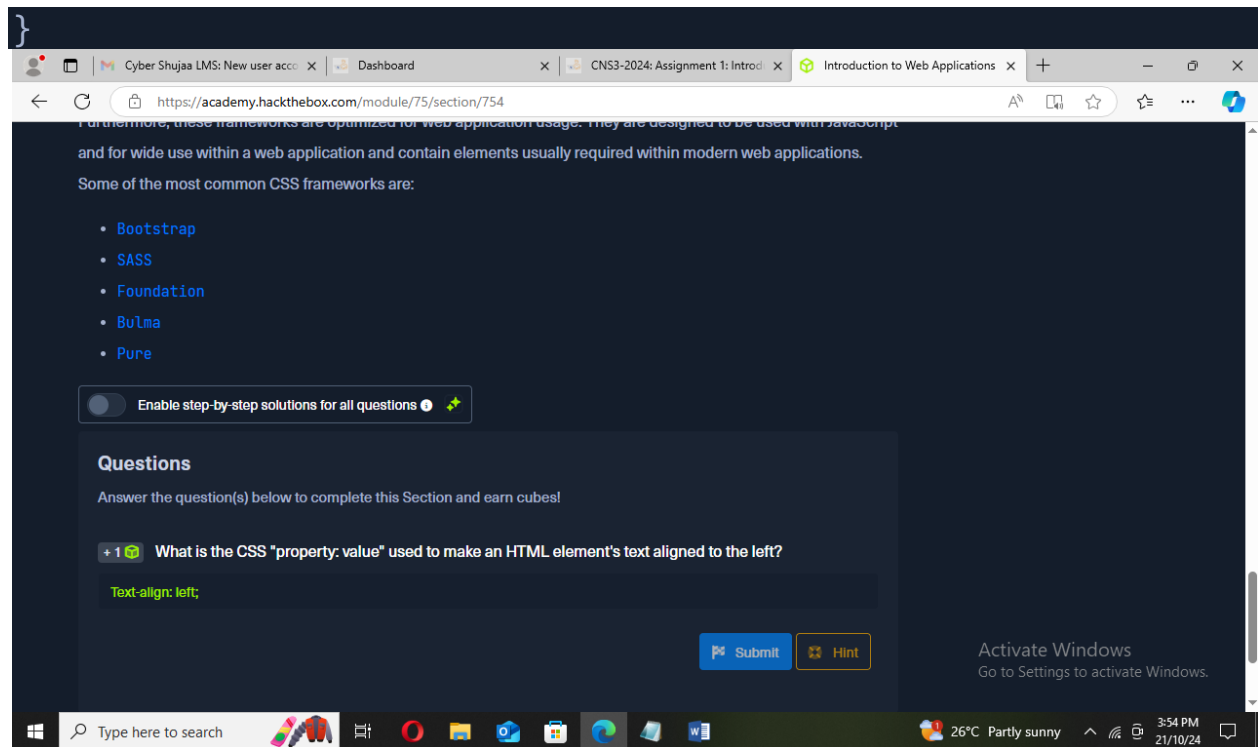
CSS

CSS (Cascading Style Sheets) is a style sheet language used for describing the look and formatting of a document written in a markup language.

What is the CSS “property; value” used to make a HTML element’s text aligned to the left

```
body {  
  background-color: black;  
}  
  
h1 {  
  color: white;  
  text-align: left;  
}  
  
p {  
  font-family: helvetica;  
  font-size: 10px;  
}
```

Week 5 Assignment 1: Introduction to Web Applications



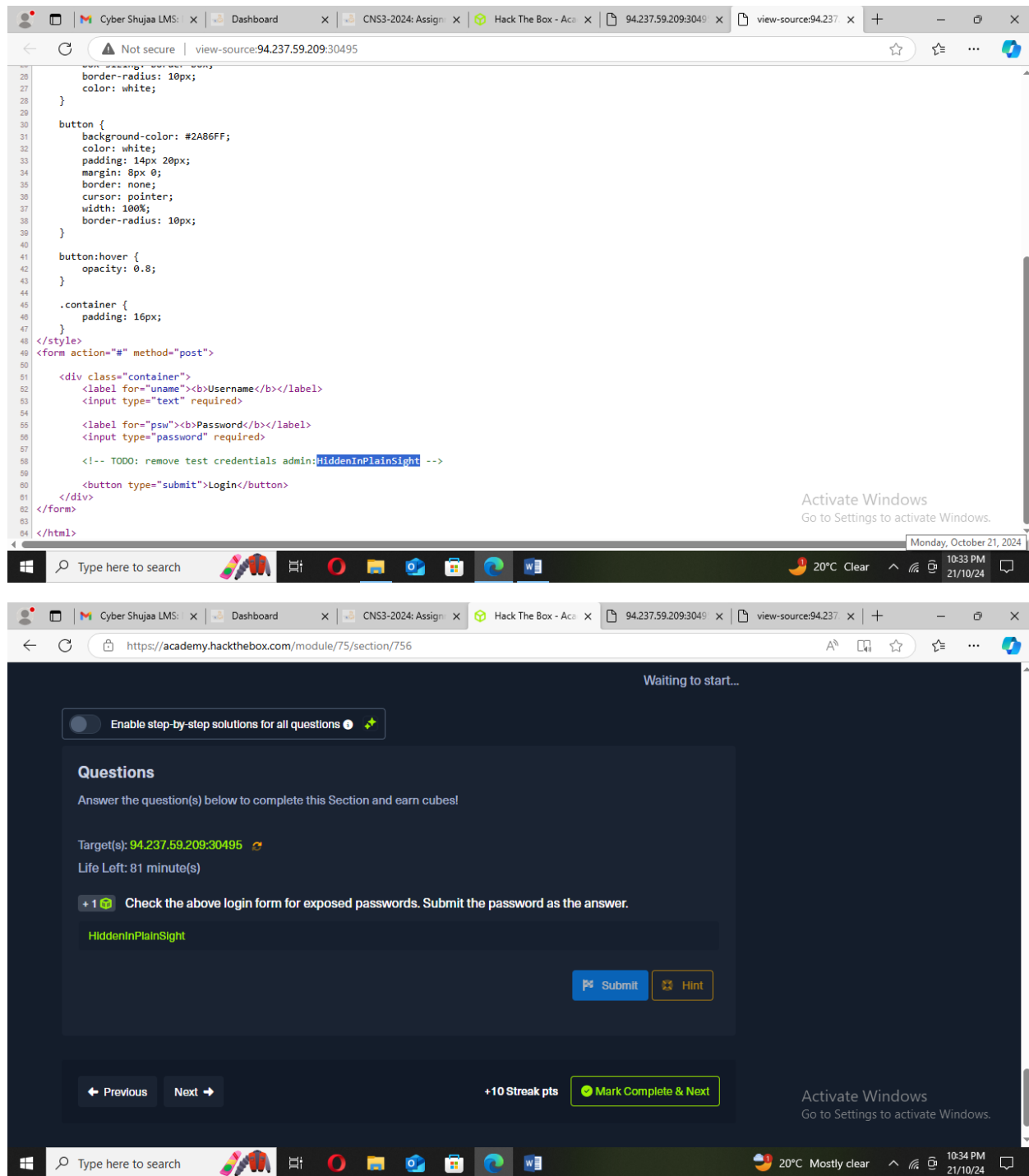
JavaScript

JavaScript is a scripting language that allows you to create dynamic and interactive web pages and are usually used on the front end of an application to be executed within a browser.

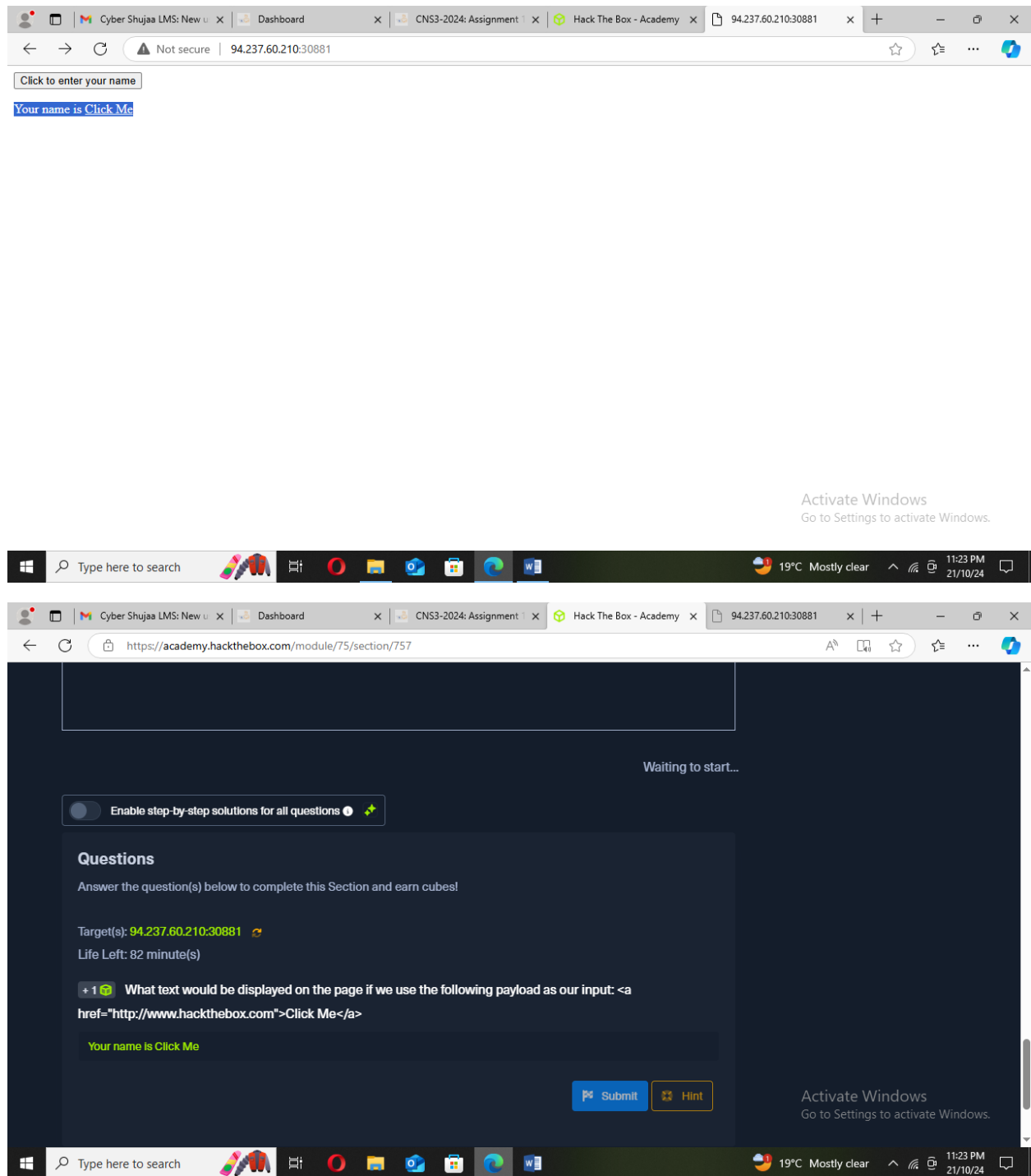
Check the above login form for exposed passwords. Submit the passwords as the answer.

From the screenshot below, the password is HiddenInPlainSight.

Week 5 Assignment 1: Introduction to Web Applications



Week 5 Assignment 1: Introduction to Web Applications

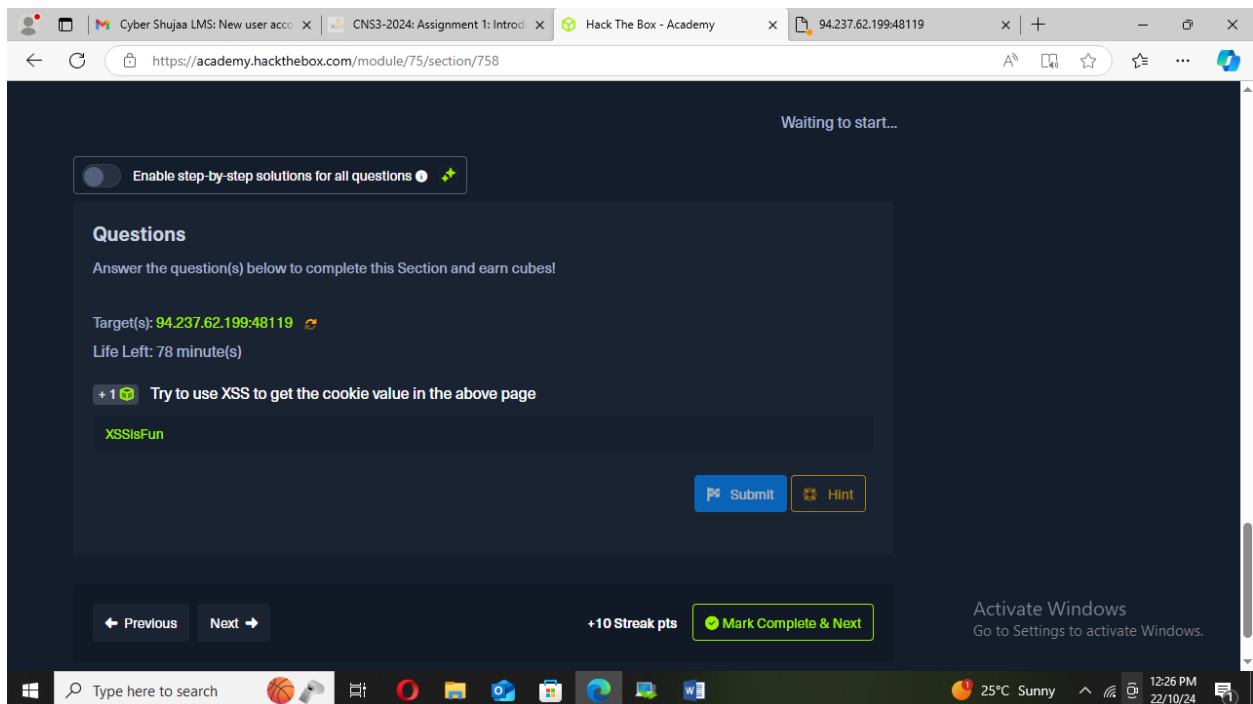
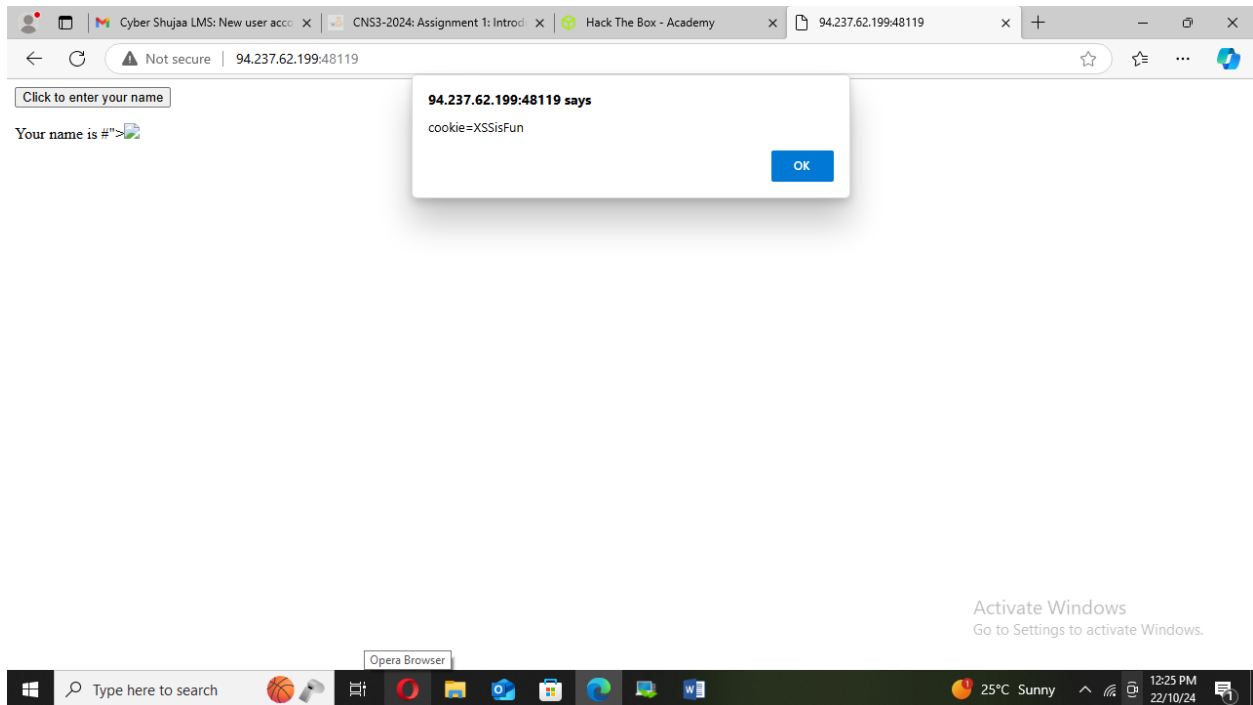


Cross-Site Scripting XSS

This is a type of security vulnerability that can be found in some web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

Week 5 Assignment 1: Introduction to Web Applications

Try to use XSS to get the cookie value in the above page. When we input the code `#">`. The cookie=`XSSisFun` as seen below.



Week 5 Assignment 1: Introduction to Web Applications

Cross-Site Request Forgery

This is a type of malicious exploit of a website or web application where unauthorized commands are submitted from a user that the web application trusts. There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript fetch or XMLHttpRequests.

What operating system is WAMP used with? Windows. This is the operating system layer of the stack

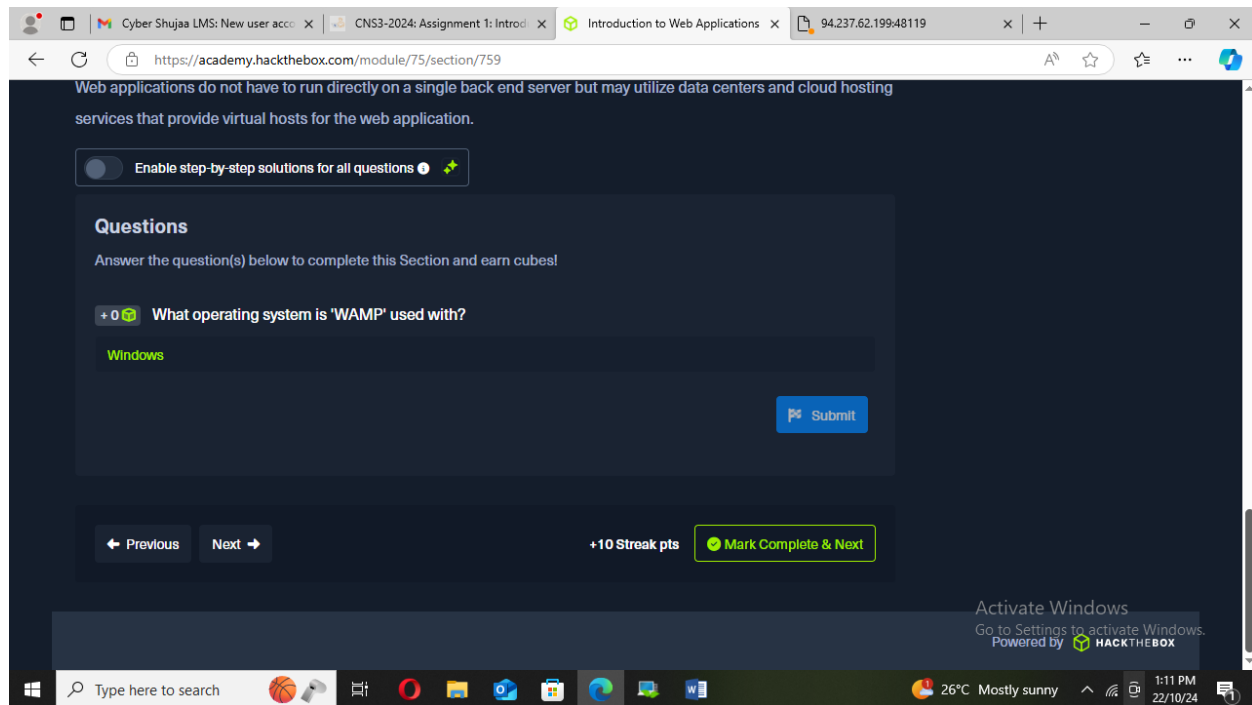
Apache. Apache HTTP Server is the web server component of WAMP.

MySQL. MySQL is the database management system used in the WAMP stack.

PHP / Perl / Python. This component refers to the programming languages the WAMP stack supports for developing dynamic web content.



Week 5 Assignment 1: Introduction to Web Applications



Web Servers

This is a computer software and underlying hardware that accepts requests via HTTP or its secure variant HTTPS. A user agent, commonly a web browser or web crawler, initiates communication by making a request for a web page or other resource using HTTP, and the server responds with the content of that resource or an error message.

If a web server returns an HTTP code 201, what does it stand for? Created

Week 5 Assignment 1: Introduction to Web Applications

The screenshot shows the MDN Web Docs page for "HTTP response status codes". The page is in English (US) and has a search bar at the top. The main content area lists several status codes with their descriptions:

- 201 Created**: The request succeeded, and a new resource was created as a result. This is typically the response sent after `POST` requests, or some `PUT` requests.
- 202 Accepted**: The request has been received but not yet acted upon. It is noncommittal, since there is no way in HTTP to later send an asynchronous response indicating the outcome of the request. It is intended for cases where another process or server

On the right side, there is a sidebar titled "In this article" with a list of links: Informational responses, **Successful responses** (highlighted), Redirection messages, Client error responses, Server error responses, Browser compatibility, and See also.

Databases

This is an organized collection of data or a type of data store based on the use of a database management system, the software that interacts with end users, applications, and the database itself to capture and analyze the data.

What type of database is Google's Firebase Database?

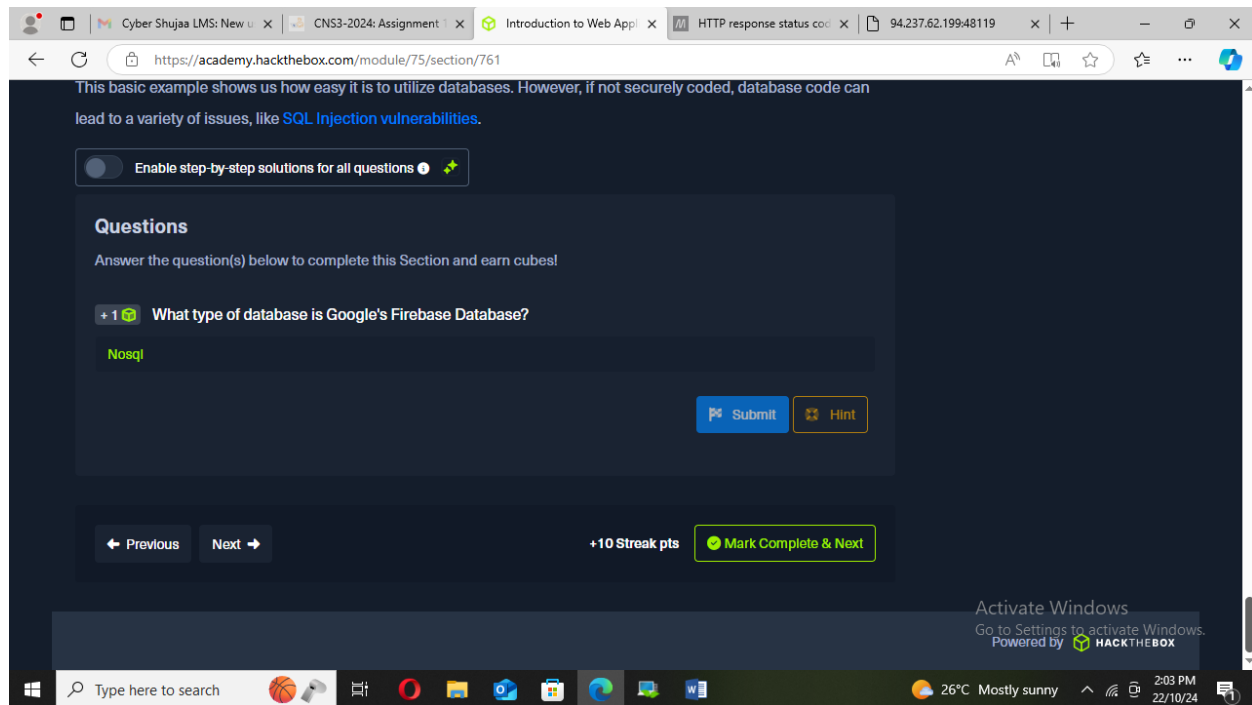
The screenshot shows a HackTheBox Academy module page titled "NoSQL databases". The page explains that NoSQL databases store data in a key-value pair format, where the key is usually a string and the value can be a string, dictionary, or any class object. It also mentions that the Document-Based model stores data in complex JSON objects.

Some of the most common NoSQL databases include:

Type	Description
MongoDB	The most common NoSQL database. It is free and open-source, uses the Document-Based model, and stores data in JSON objects.
ElasticSearch	Another free and open-source NoSQL database. It is optimized for storing and analyzing huge datasets. As its name suggests, searching for data within this database is very fast and efficient.
Apache Cassandra	Also free and open-source. It is very scalable and is optimized for gracefully handling faulty values.

Other common NoSQL databases include: Redis, Neo4j, CouchDB, and Amazon DynamoDB.

Week 5 Assignment 1: Introduction to Web Applications



Development Frameworks & APIs

The framework is the skeleton holding the library or libraries. The API is the programming interface allowing you to interact with another application or operating system. It pulls from sources of code within the framework to work with other sources of code or applications of the code.

Use GET request `"/index.php?id=0"` to search for the name of the user with id number 1? When we input the code 94.237.62.52:49885/index.php?id=1 we get superadmin as the user as seen

Week 5 Assignment 1: Introduction to Web Applications

below.

The screenshot shows the Hack The Box Academy interface. At the top, there's a navigation bar with tabs for 'Cyber Shujaa LMS: New u...', 'CNS3-2024: Assignment 1', 'Hack The Box - Academy', 'HTTP response status cod...', and '94.237.62.52:49885/index...'. The main content area is titled 'Questions' and contains the following text: 'Answer the question(s) below to complete this Section and earn cubes!'. Below this, it says 'Target(s): 94.237.62.52:49885' and 'Life Left: 85 minute(s)'. The question is: '+1 Use GET request \'/index.php?id=0\' to search for the name of the user with id number 1?'. The answer 'superadmin' is entered in the input field. There are 'Submit' and 'Hint' buttons. At the bottom, there are 'Previous' and 'Next' buttons, a '+10 Streak pts' indicator, and a 'Mark Complete & Next' button. A Windows taskbar is visible at the bottom with the search bar, taskbar icons, and system tray showing '26°C Partly sunny' and '2:30 PM 22/10/24'.

The screenshot shows a web browser window with the address bar displaying '94.237.62.52:49885/index.php?id=1'. The page content shows the text 'superadmin'. The browser's status bar at the bottom indicates 'Not secure'.

superadmin

Common Web Vulnerabilities

Broken Authentication refers to vulnerabilities that attackers exploit to impersonate legitimate users online.

Week 5 Assignment 1: Introduction to Web Applications

Broken Access Control ; This can lead to unauthorized information disclosure, modification, or destruction of data or business functions.

To which of the above categories does public vulnerability 'CVE-2014-6217' belongs to?
Command Injection

The screenshot shows a web browser window with the URL <https://academy.hackthebox.com/module/75/section/764>. The page title is "Command Injection". The content explains that many web applications execute local Operating System commands to perform certain processes. For example, a web application may install a plugin by executing an OS command that downloads that plugin, using the plugin name provided. If not properly filtered and sanitized, attackers may be able to inject another command to be executed alongside the originally intended command (i.e., as the plugin name), which allows them to directly execute commands on the back end server and gain control over it. This type of vulnerability is called **command injection**. The text also states that this vulnerability is widespread, as developers may not properly sanitize user input or use weak tests to do so, allowing attackers to bypass any checks or filtering put in place and execute their commands. An example is given: the WordPress Plugin **Plainview Activity Monitor 20161228** has a **vulnerability** that allows attackers to inject their command in the **ip** value, by simply adding **| COMMAND...** after the **ip** value. Below the text is a section titled "SQL Injection (SQLi)" which starts with "Another very common vulnerability in web applications is a **SQL Injection** vulnerability. Similarly to a Command Injection vulnerability, this vulnerability may occur when the web application executes a SQL query, including a value". On the right side of the page, there is a "Next Steps" section and a "My Workstation" section showing "OFFLINE" status with a "Start Instance" button and "1 / 1 spawns left". At the bottom right, there is an "Activate Windows" watermark.

The screenshot shows a web browser window with the URL <https://academy.hackthebox.com/module/75/section/764>. The page title is "Questions". The content asks the user to "Answer the question(s) below to complete this Section and earn cubes!". The question is: "+1 🟢 To which of the above categories does public vulnerability 'CVE-2014-6217' belongs to?". The answer "command injection" is entered in the text box. Below the text box are "Submit" and "Hint" buttons. At the bottom of the page, there are "Previous" and "Next" buttons, a "+10 Streak pts" indicator, and a "Mark Complete & Next" button. At the bottom right, there is an "Activate Windows" watermark.

Week 5 Assignment 1: Introduction to Web Applications

Public Vulnerabilities

These vulnerabilities are usually caused by coding mistakes made during the development of a web application's backend components.

What is the CVSS score of the public vulnerability CVE-2017-0144? The CVSS score is 9.3 as seen below.

The image shows two screenshots from a web browser. The top screenshot is from the NVD CVSS calculator for CVE-2017-0144. It displays the CVSS Base Score of 9.3, with sub-scores for Impact (10.0) and Exploitability (8.6). The Temporal, Environmental, and Modified Impact scores are all NA. The overall CVSS score is 9.3. The bottom screenshot is from the HackTheBox Academy interface, showing a question: "What is the CVSS score of the public vulnerability CVE-2017-0144?". The answer "9.3" is entered, and the user has earned 1 cube for completing the question.

Score.

As of July 13th, 2022, the NVD no longer generates new information for CVSS v2.0. Existing CVSS v2.0 information will remain in the database but the NVD will no longer actively populate CVSS v2.0 for new CVEs. This change comes as CISA policies that rely on NVD data fully transition away from CVSS v2.0. NVD analysts will continue to use the reference information provided with the CVE and any publicly available information at the time of analysis to associate Reference Tags, CVSS v3.1, CWE, and CPE Applicability statements.

Base Scores

Category	Score
Base	9.3
Impact	10.0
Exploitability	8.6

Temporal

Category	Score
Temporal	NA

Environmental

Category	Score
Environmental	NA

Overall

Category	Score
Overall	9.3

CVSS Base Score: 9.3
Impact Subscore: 10.0
Exploitability Subscore: 8.6
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 9.3

Show Equations

CVSS v2.0 Vector
(AV:N/AC:M/Au:N/C:C/I:C/A:C)

Base Score Metrics

Exploitability Metrics

Impact Metrics

Success
Congratulations! You earned 1 cube!

Questions

Answer the question(s) below to complete this Section and earn cubes!

+1 What is the CVSS score of the public vulnerability CVE-2017-0144?

9.3

Submit Hint

Previous Next

+10 Streak pts Mark Complete & Next

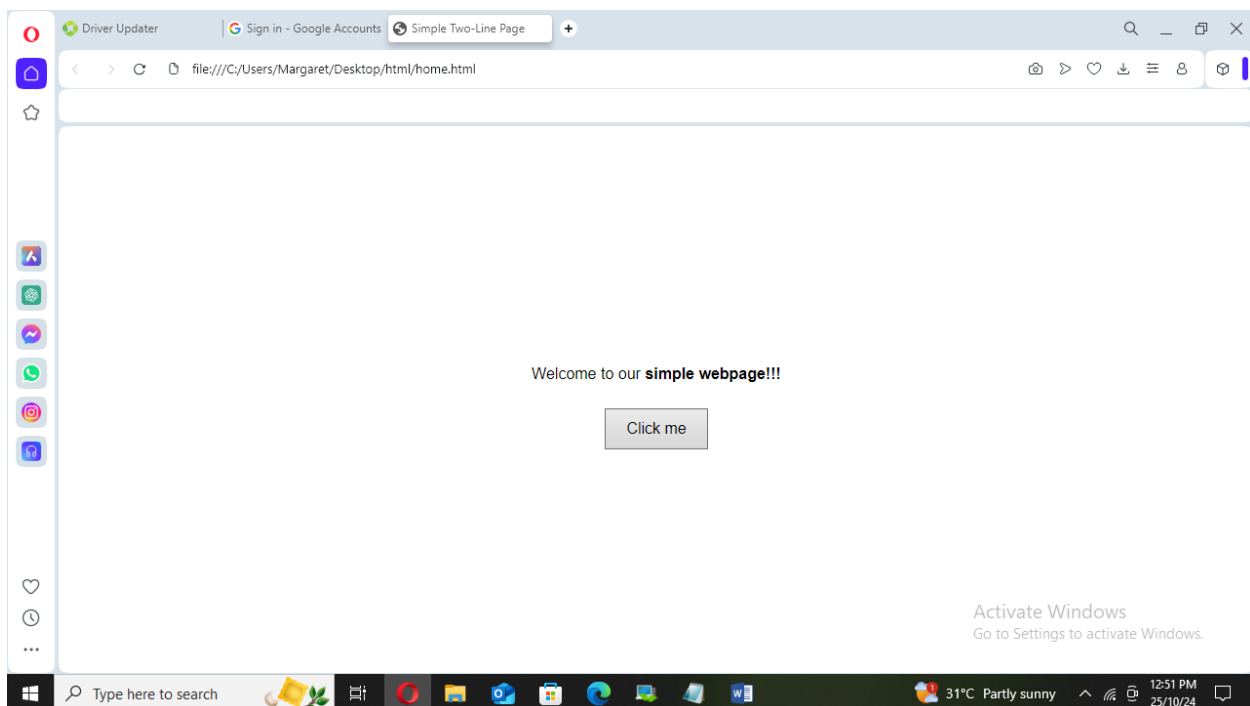
Conclusion

From this module, we have learnt about HTML (Hypertext Markup Language) a standard language used to create the basic structure and content of a webpage and acts as the skeleton of the website. HTML defines elements like headings, paragraphs, images, links, buttons, forms, and more.

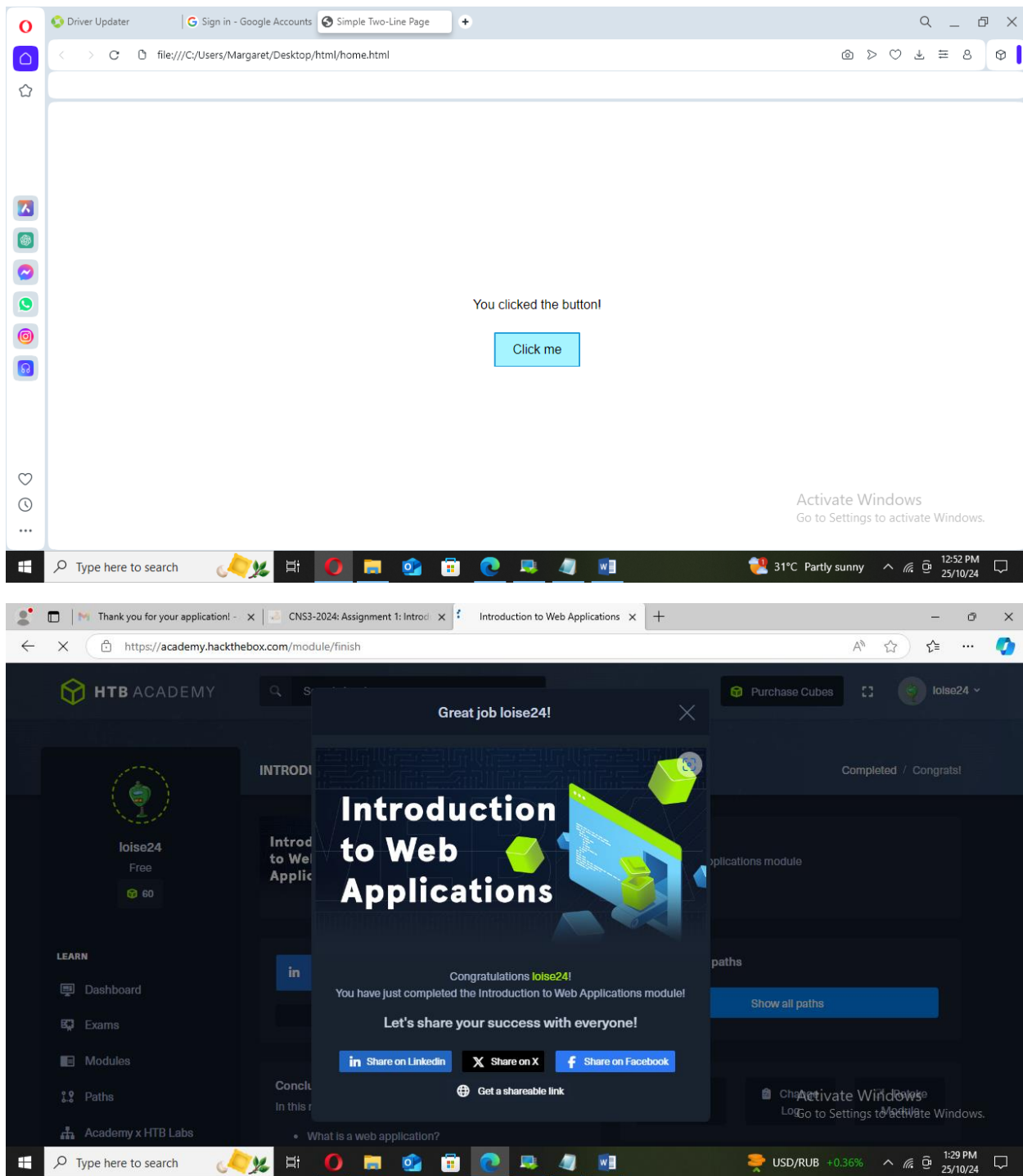
CSS (Cascading Style Sheets) is used to style and layout the HTML elements on a webpage. It is like the makeup and clothing of the webpage. It changes the colors, fonts, spacing, sizes, positioning, and other visual aspects of HTML elements.

JavaScript (JS) is a programming language that enables dynamic, interactive content on webpages. It's like the brain of the webpage, allowing it to react to user interactions (clicks, form submissions, etc.), update content in real-time, validate input, fetch data, and much more.

On that note I created a simple web application webpage incorporating HTML, JS and CSS as seen below.



Week 5 Assignment 1: Introduction to Web Applications



<https://academy.hackthebox.com/achievement/1497649/75>