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

Introduction

In this module, we will be looking at web applications. Web applications are application software that are assessed 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 date 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.

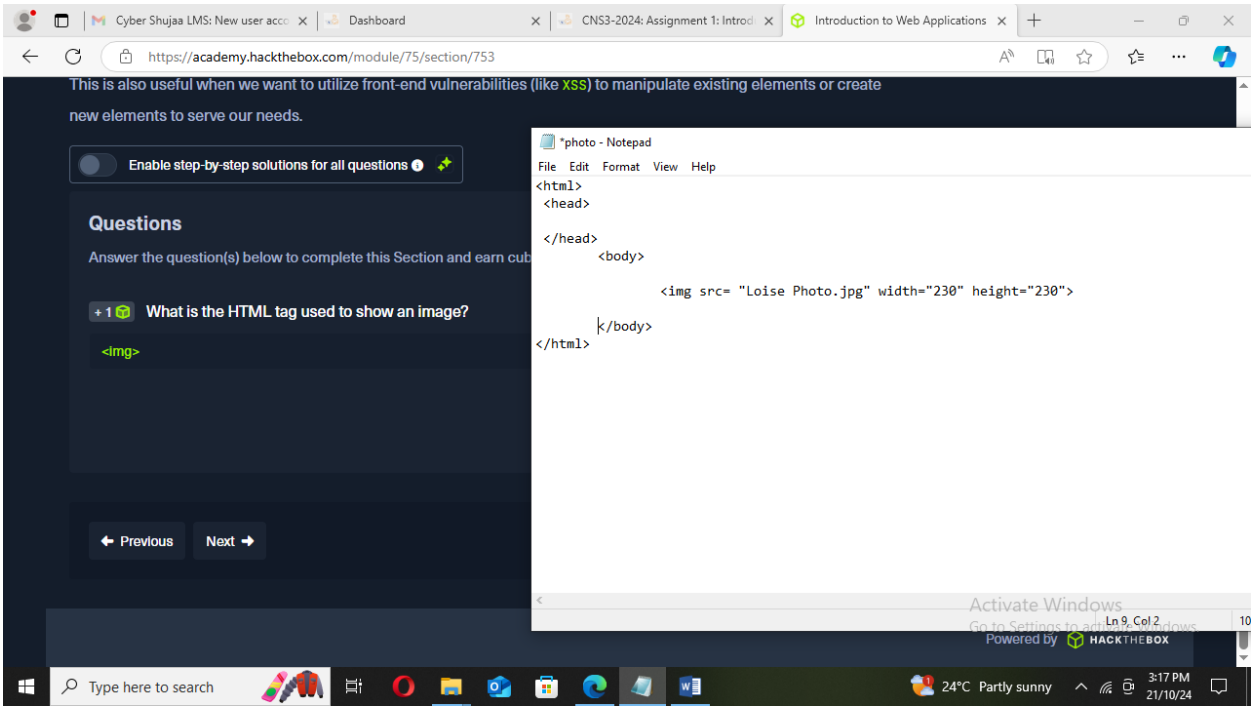
Week 5 Assignment 1: Introduction to Web Applications

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.

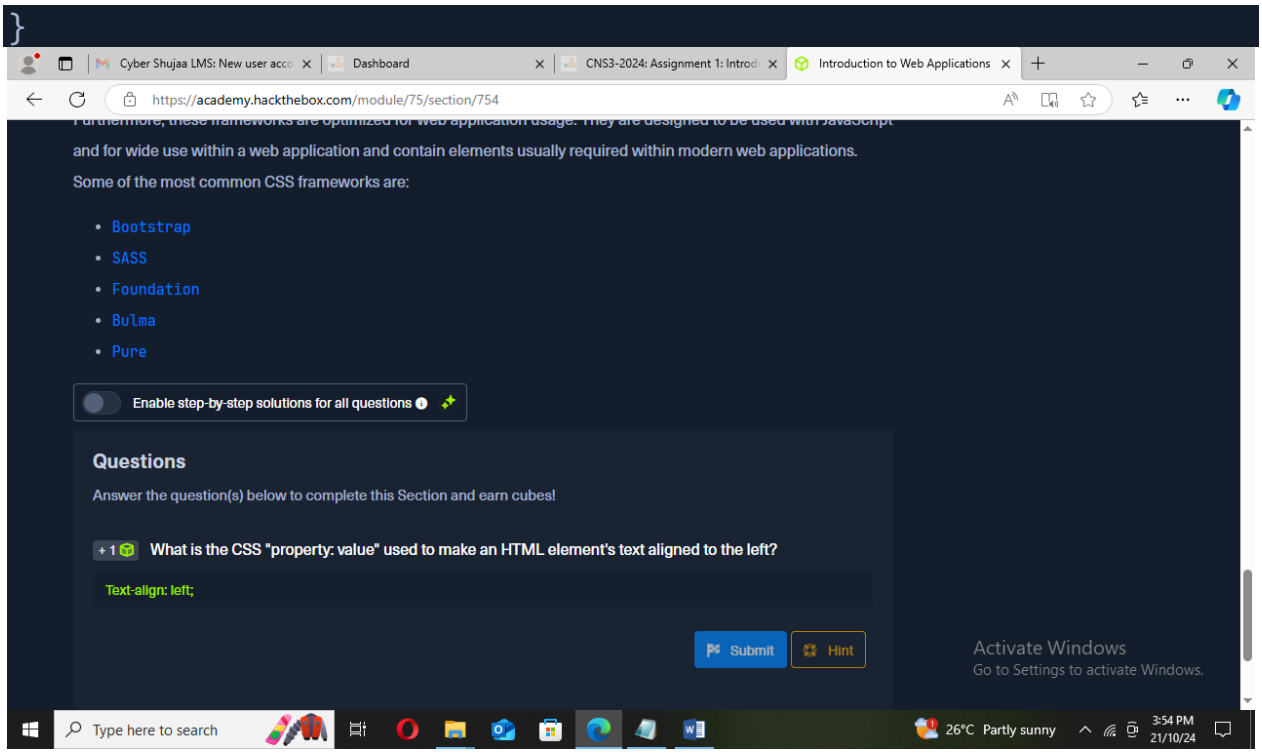
What is the CSS “property; value” used to make a HTML element’s tax aligned to the left

```
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



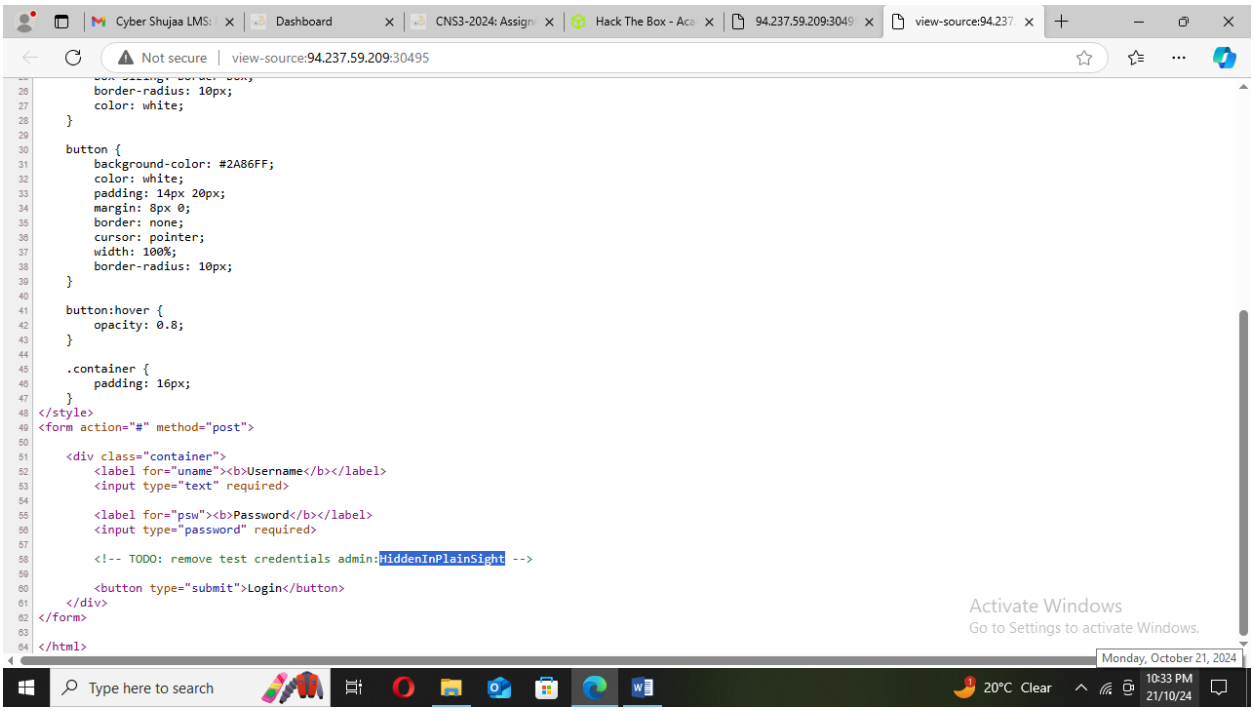
JavaScript

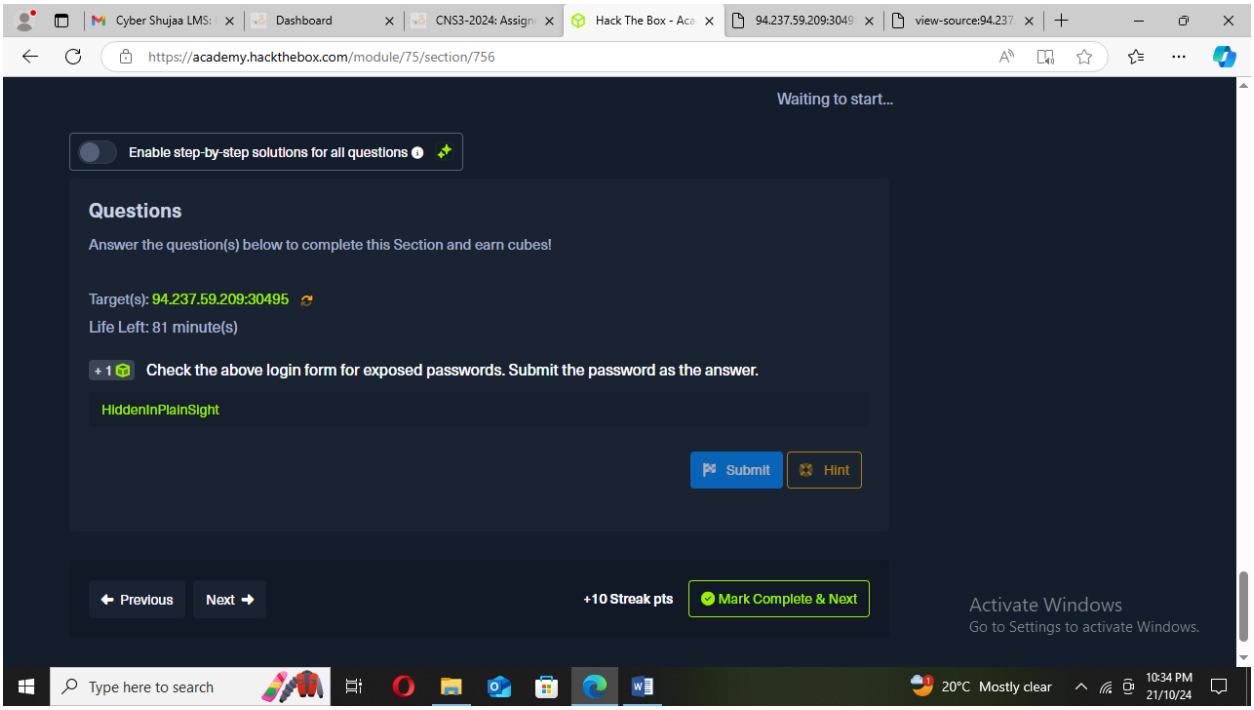
JavaScript is a scripting language that allows you to create dynamic and interactive web pages and are usually used on the front end of an application to be executed within a browser.

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

From the screenshot below, the password is HiddenInPlainSight.

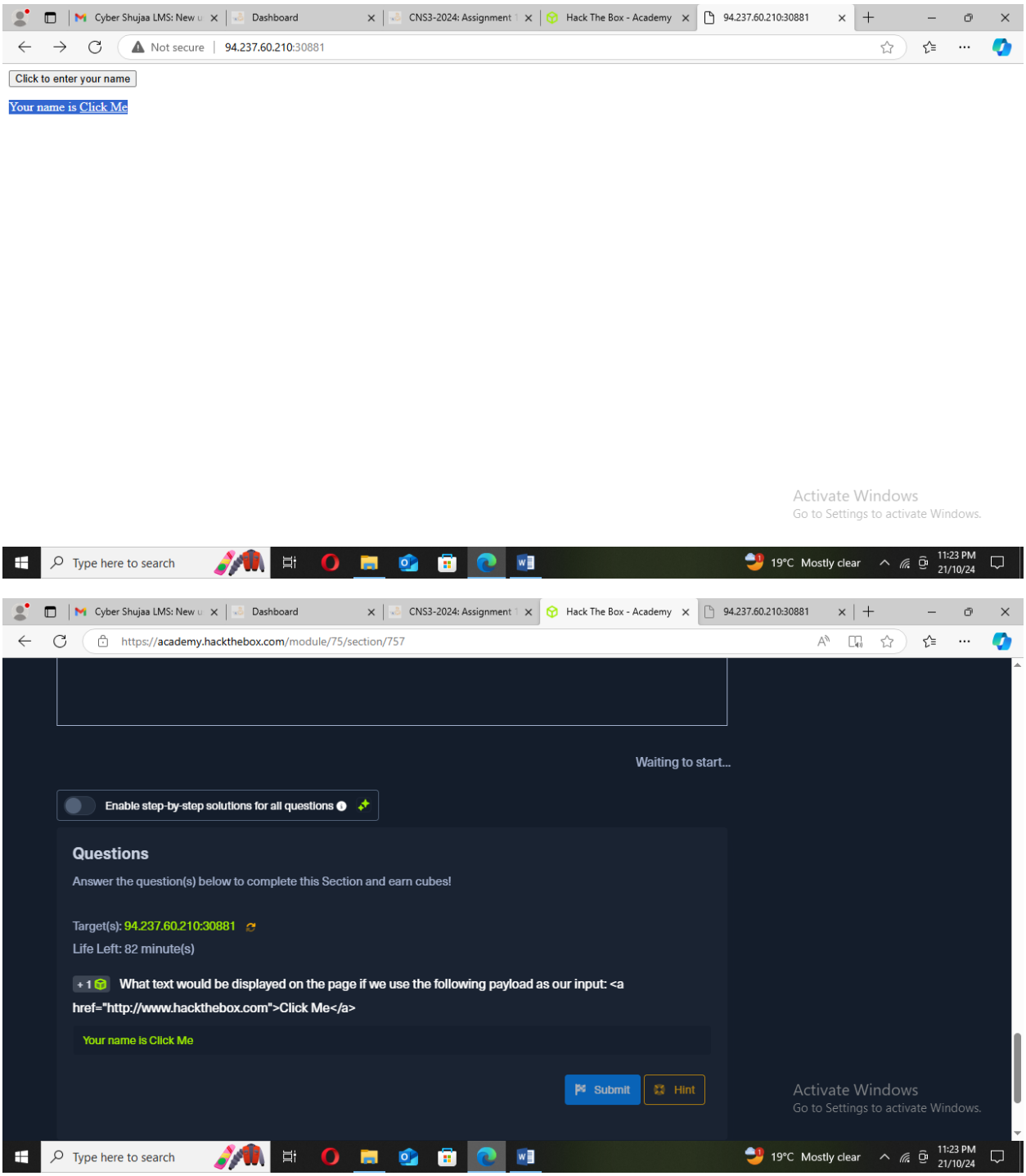
Week 5 Assignment 1: Introduction to Web Applications





What text would be displayed on the page if we use the following payload as our input: Click Me . From the screenshot below when we input the command we get Your name is Click Me.

Week 5 Assignment 1: Introduction to Web Applications

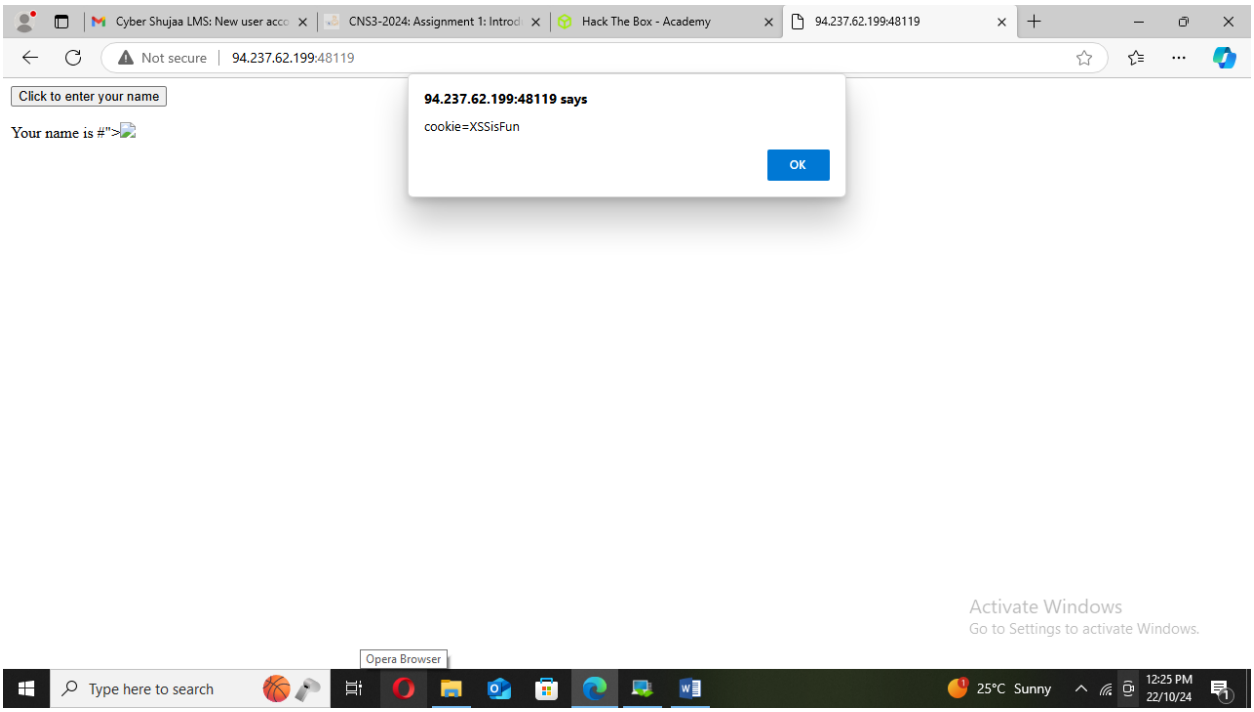


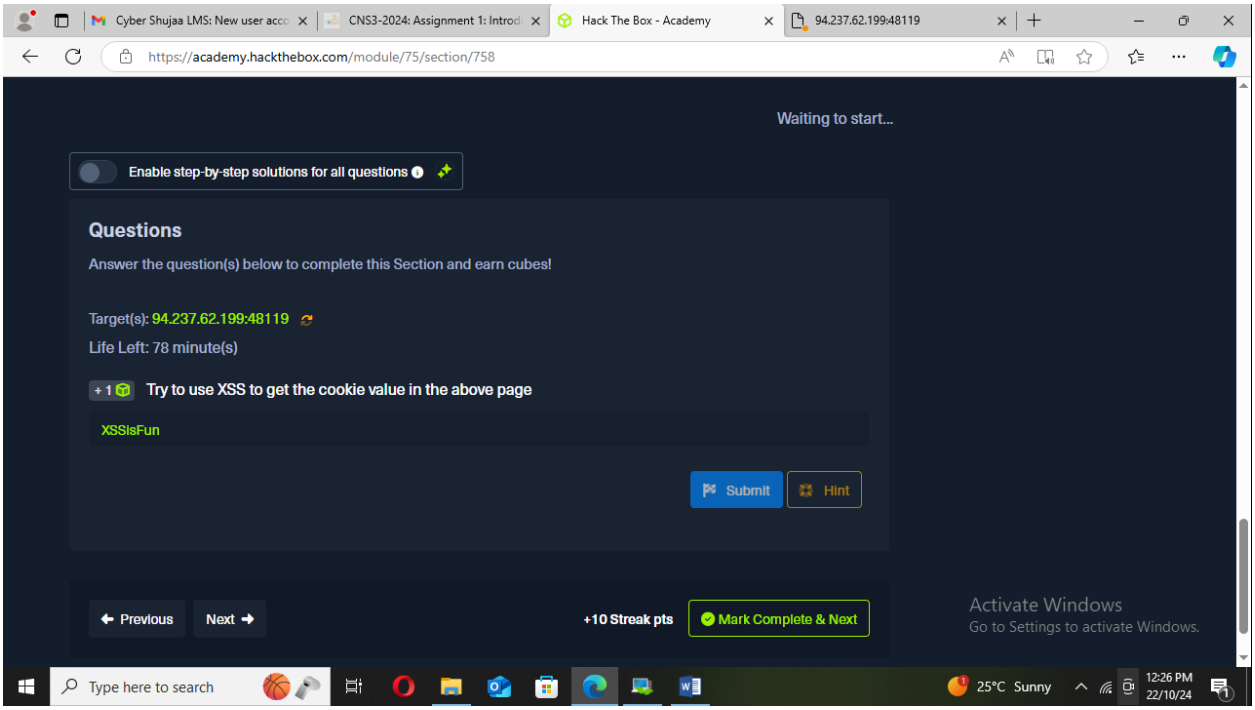
Cross-Site Scripting XSS

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 #"><img src=/ onerror=alert (document. cookie)>. 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.

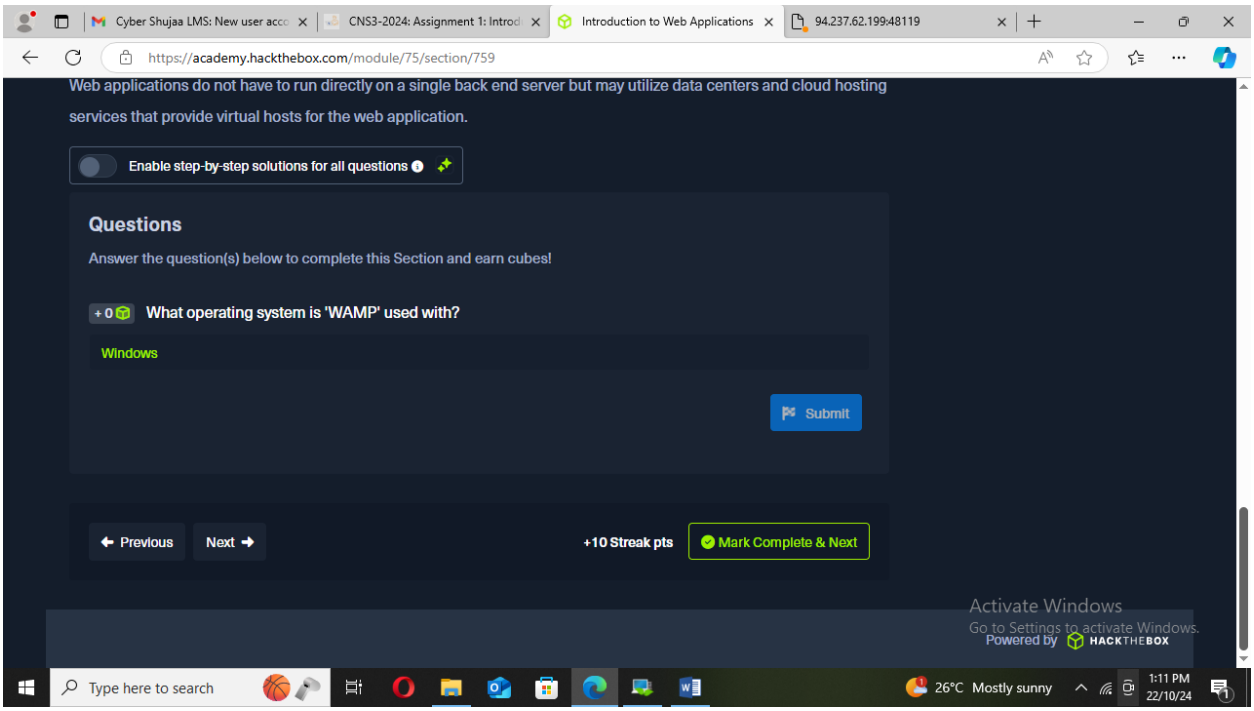
What operating system is WAMP used with? Windows. This is the operating system layer of the stack

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

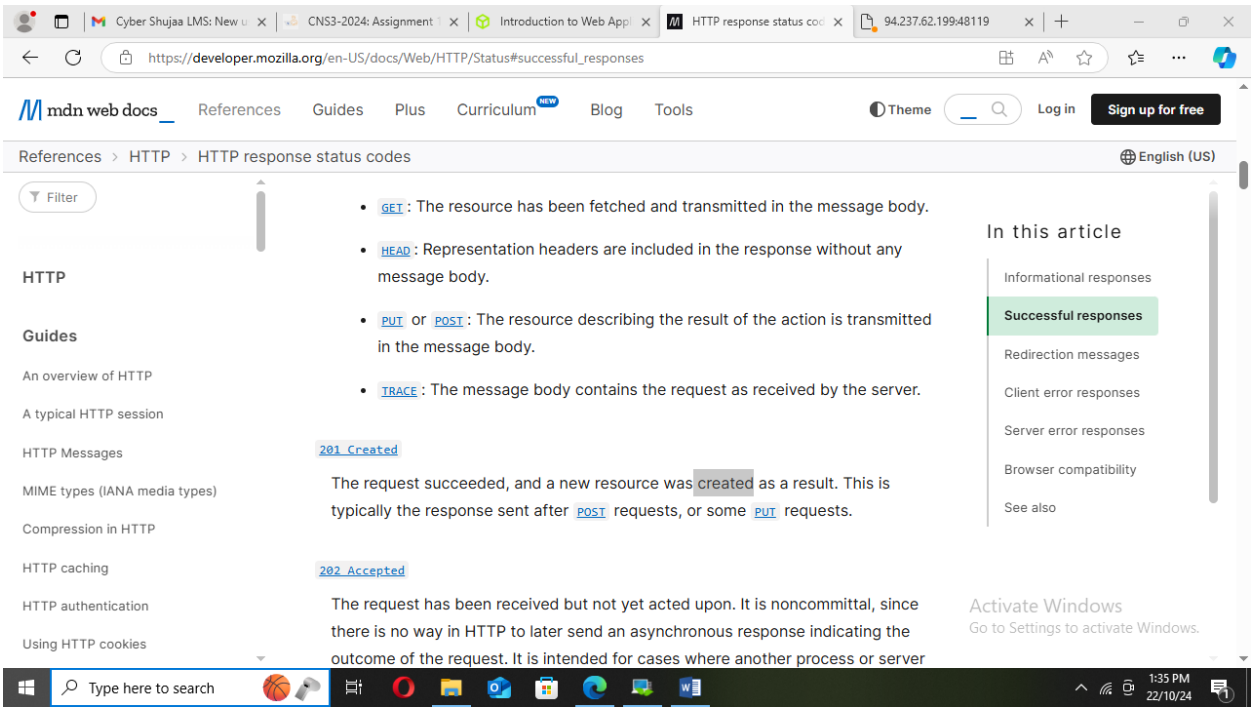


Web Servers

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

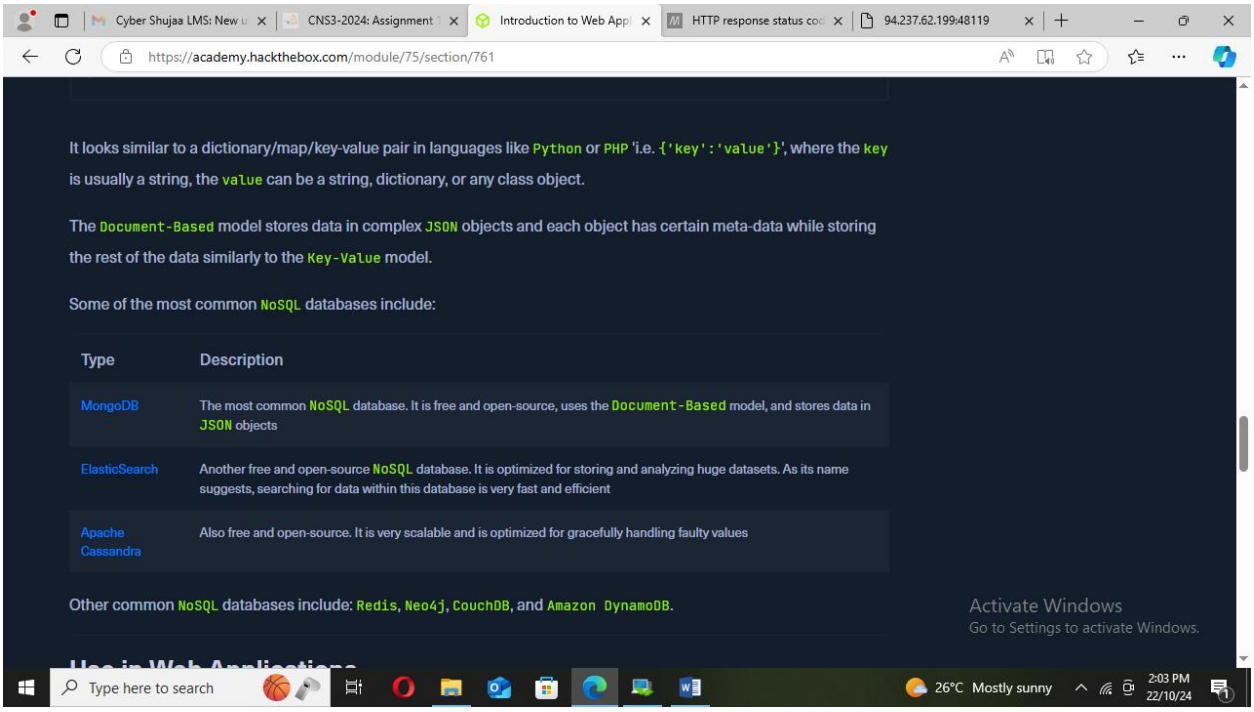
Week 5 Assignment 1: Introduction to Web Applications



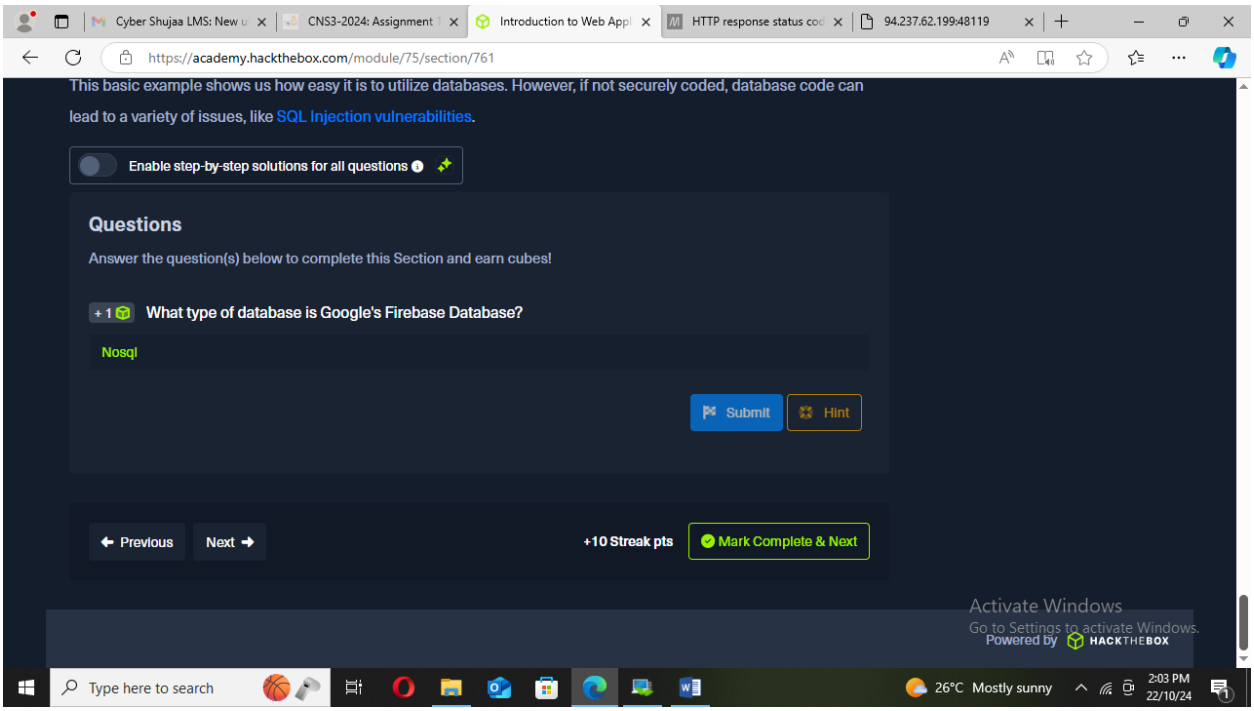
Databases

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?



Week 5 Assignment 1: Introduction to Web Applications

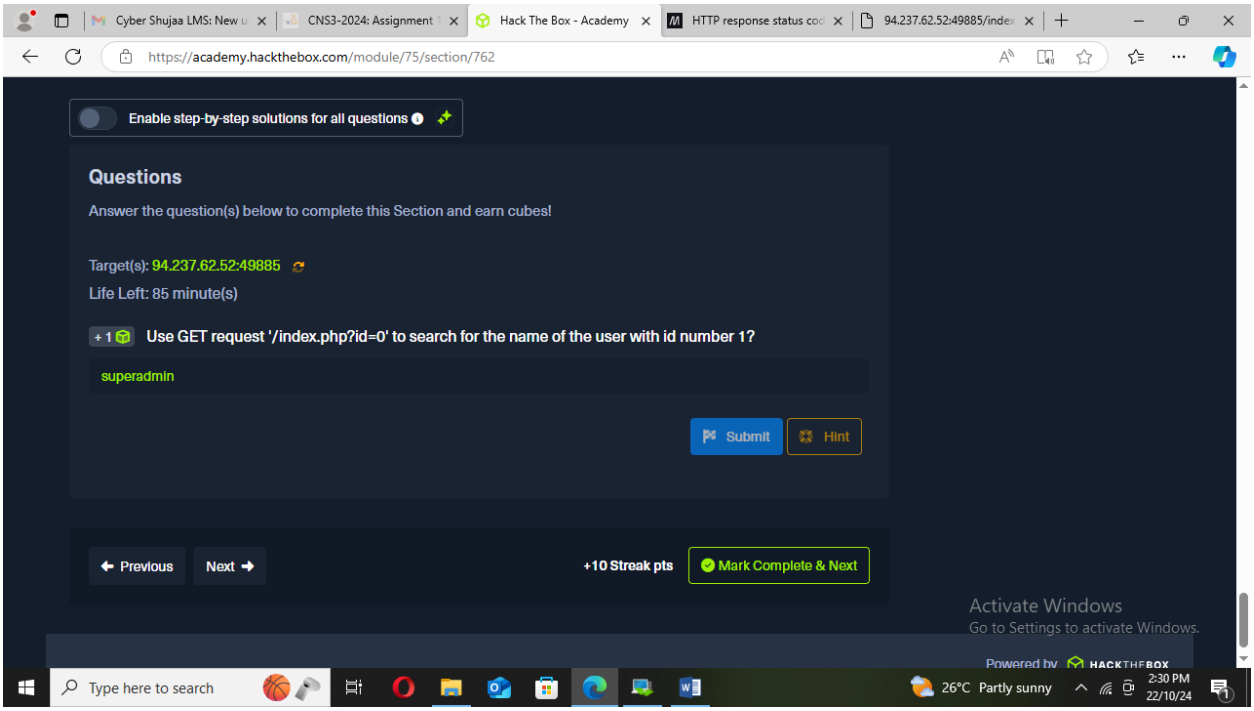


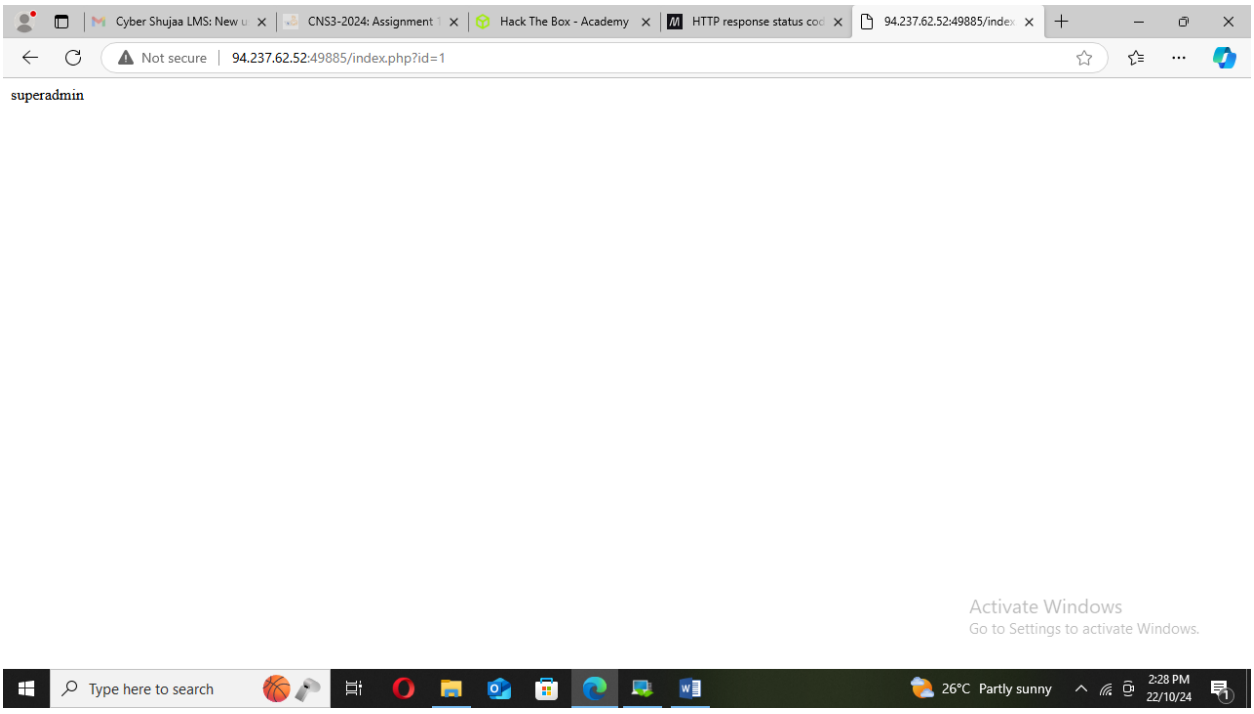
Development Frameworks & APIs

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

below.





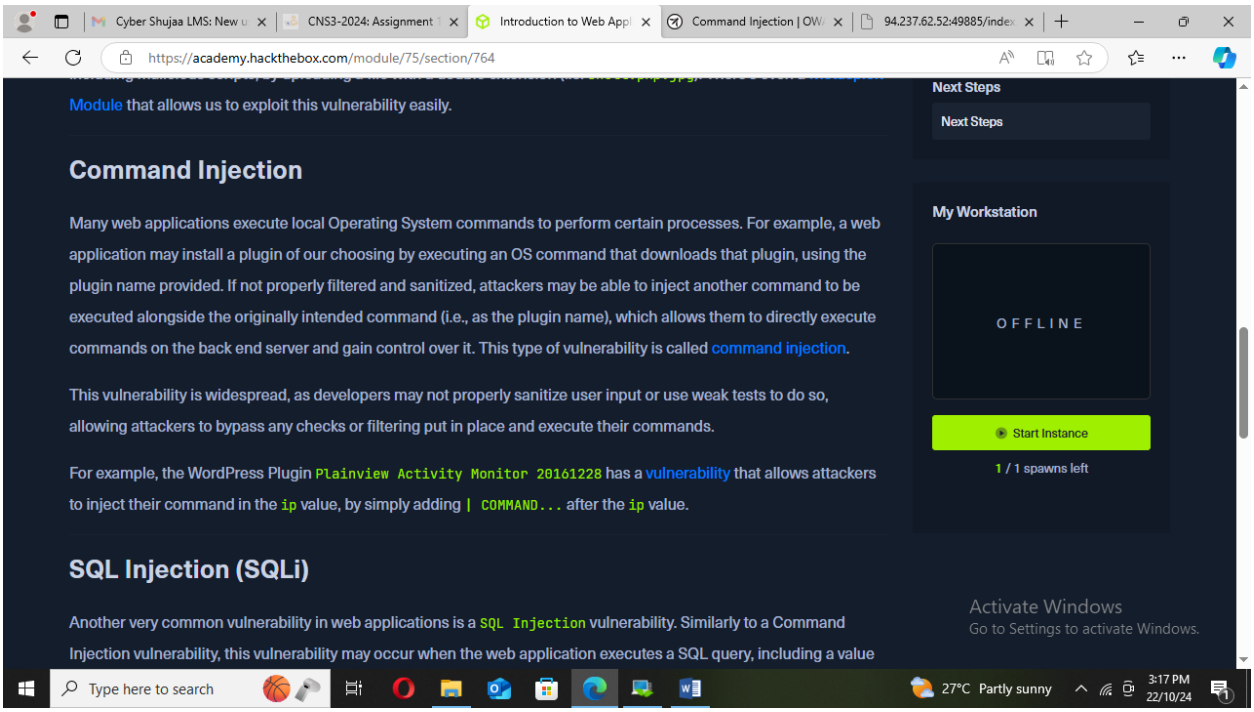
Common Web Vulnerabilities

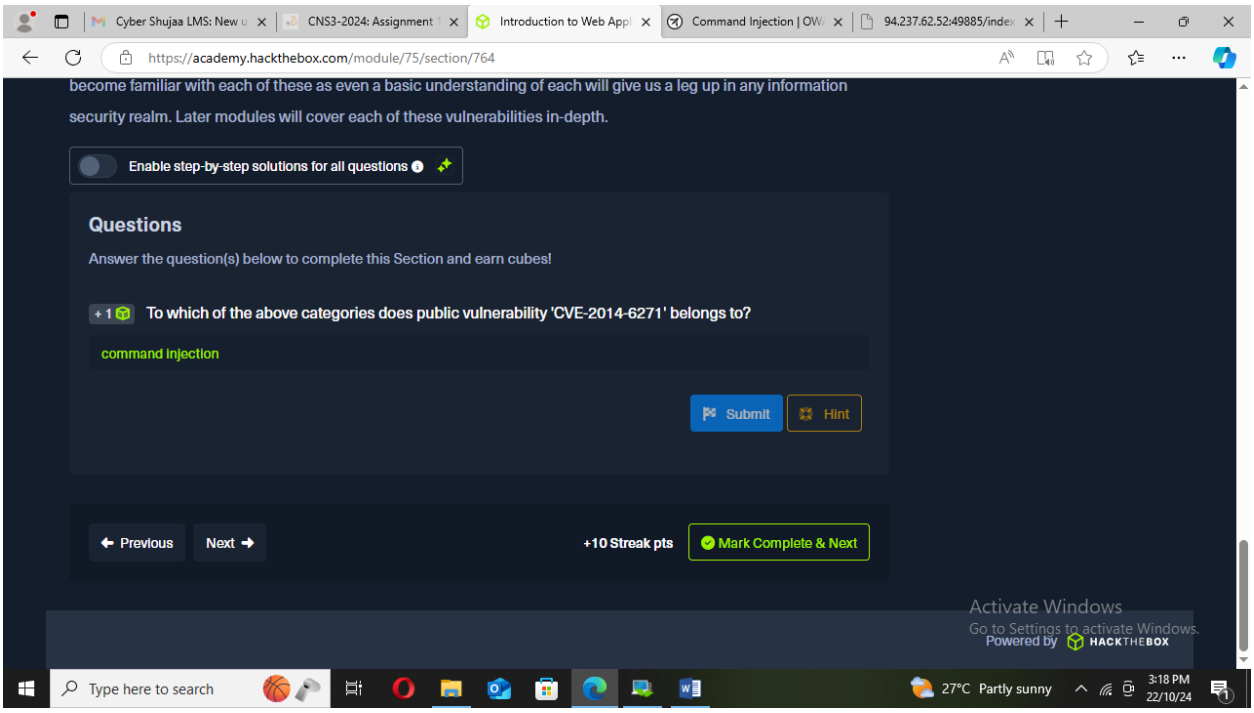
Broken Authentication refers to vulnerabilities that attackers exploit to impersonate legitimate users online.

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



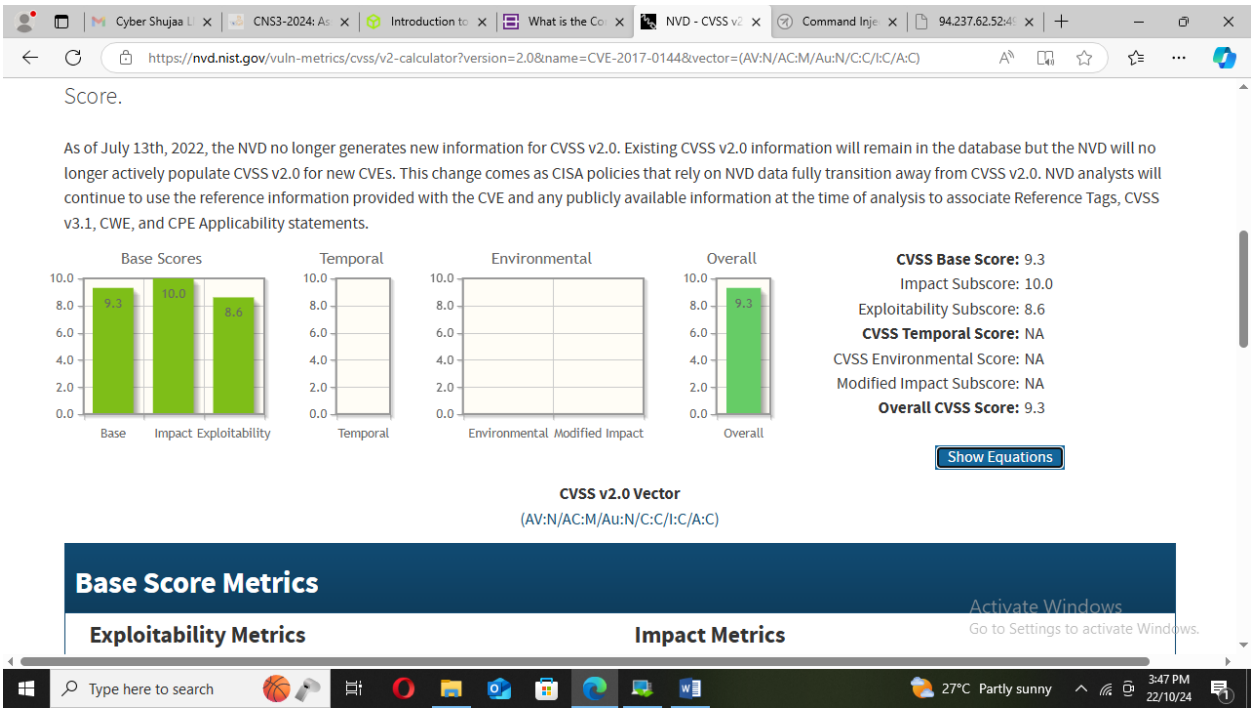


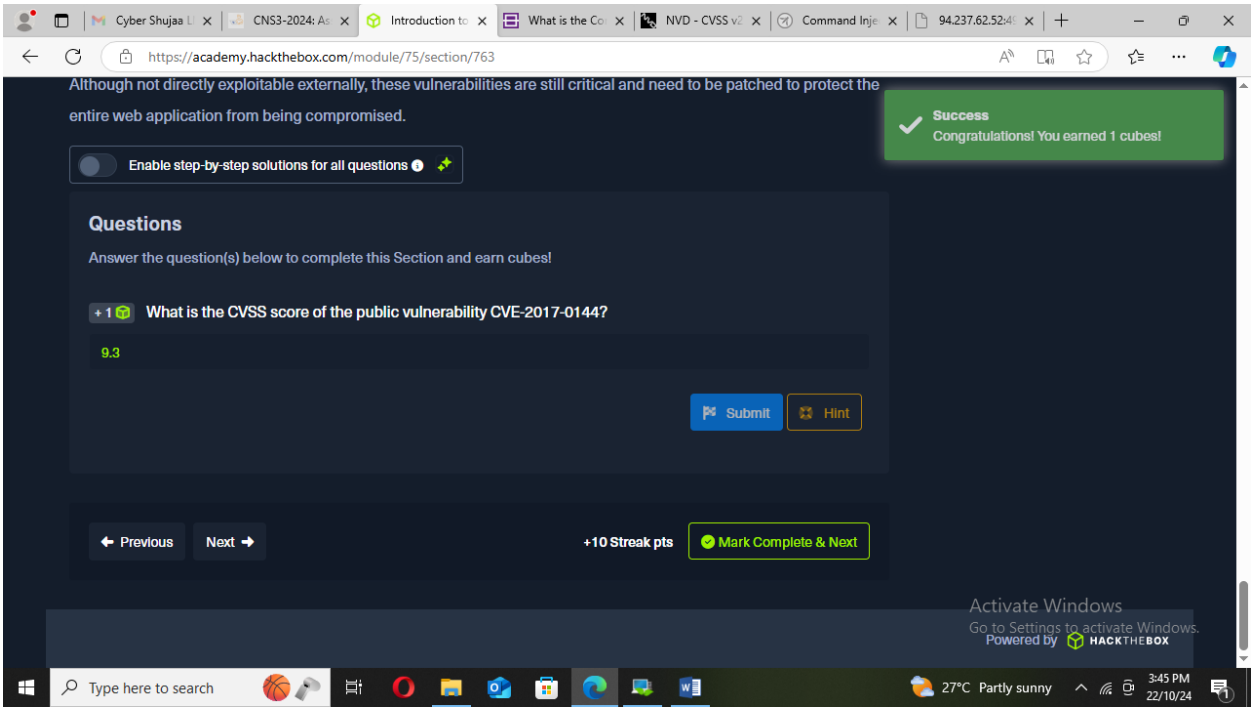
Week 5 Assignment 1: Introduction to Web Applications

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.



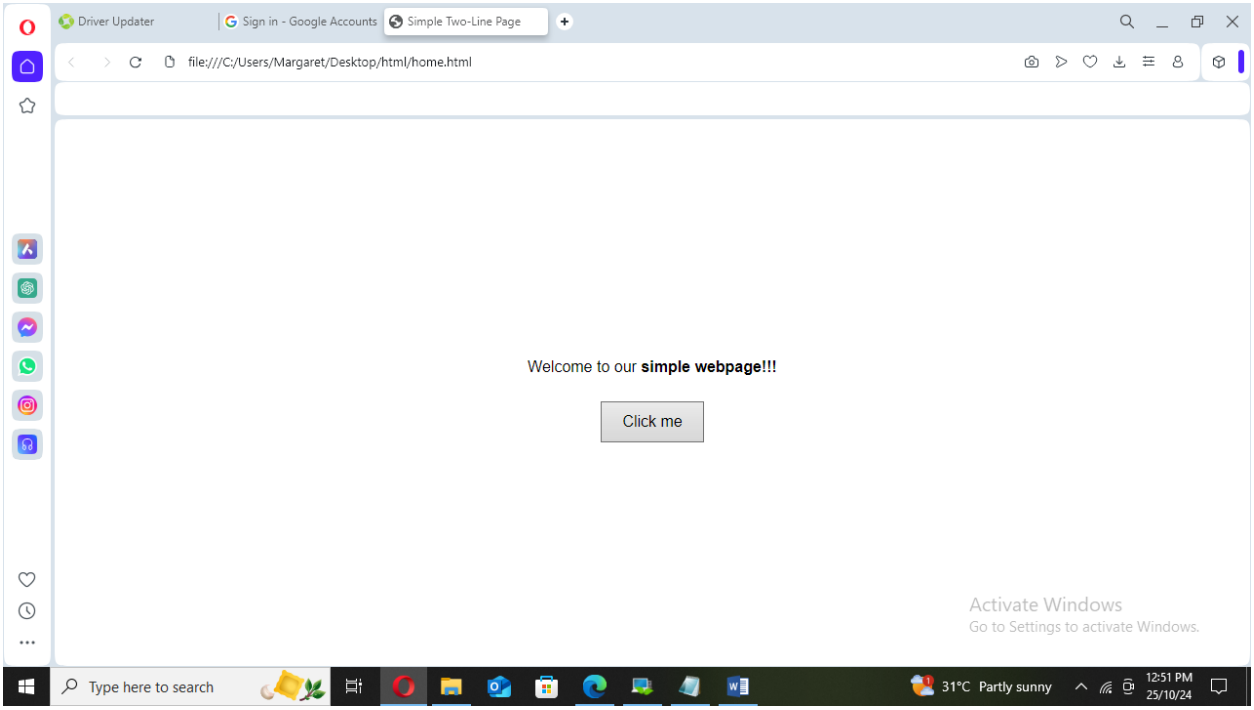


Conclusion

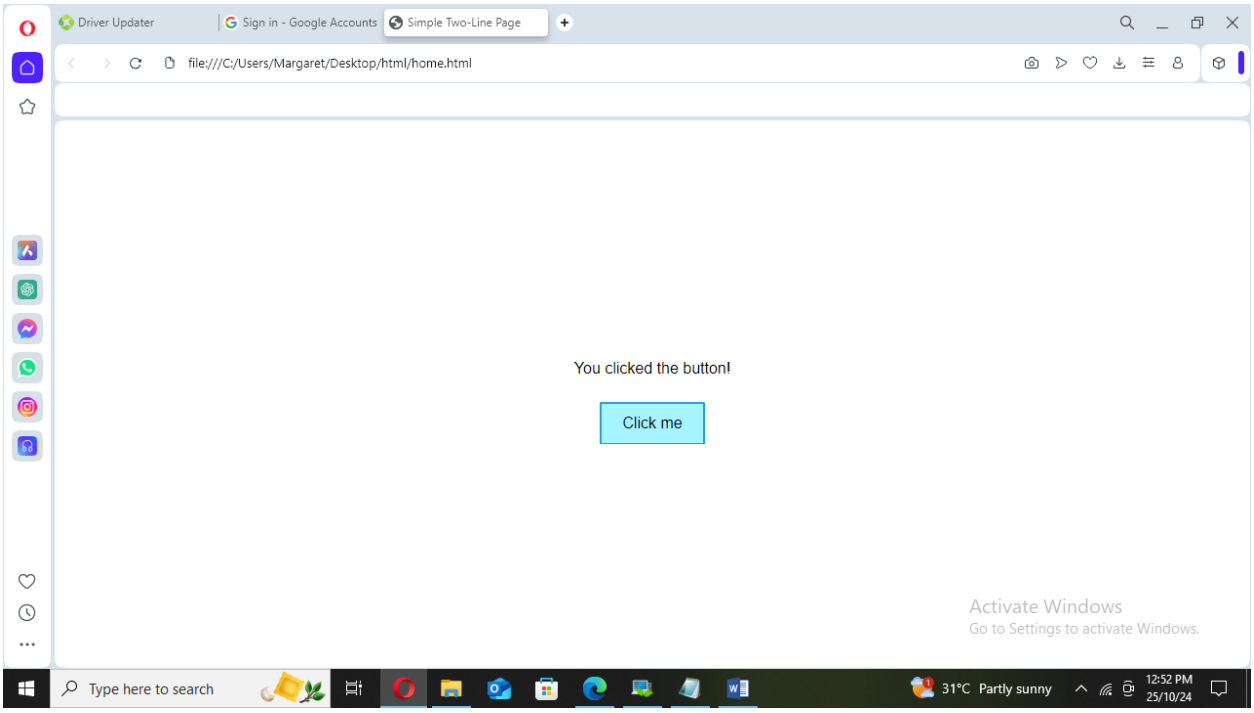
From this module, we have learnt about HTML (Hypertext Markup Language) a standard language used to create the basic structure and content of a webpage and acts as the skeleton of the website. HTML defines elements like headings, paragraphs, images, links, buttons, forms, and more.

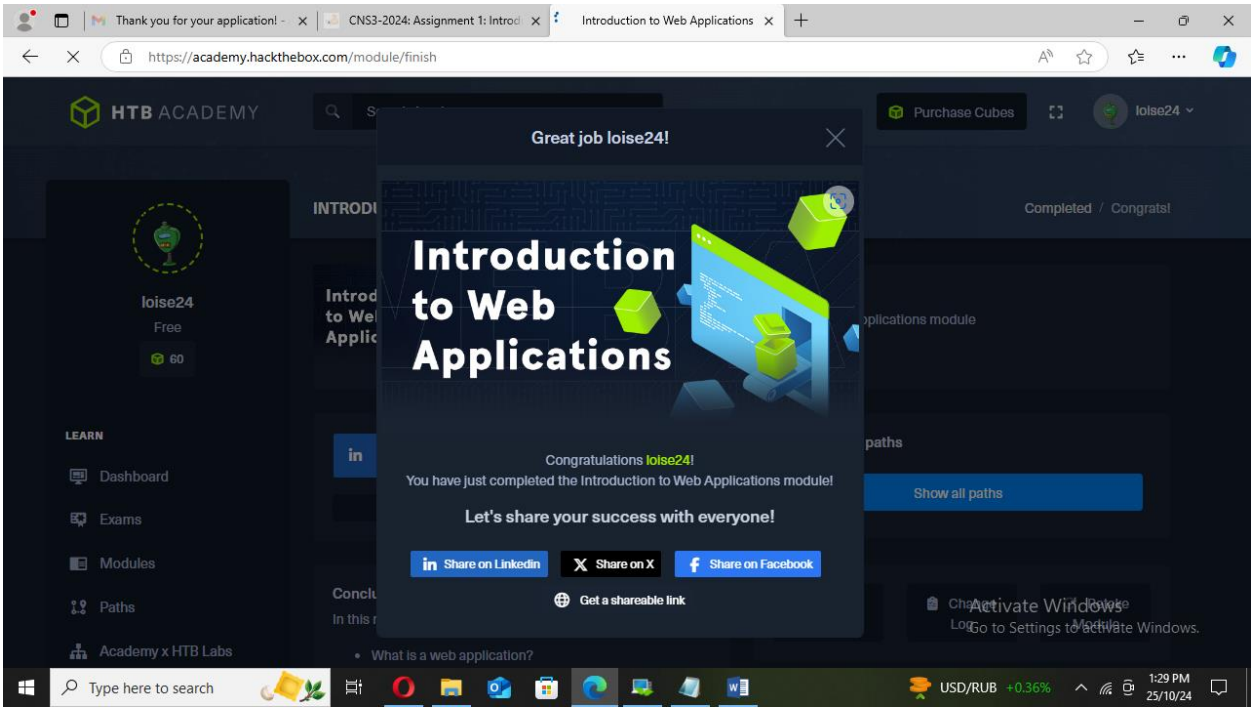
CSS (Cascading Style Sheets) is used to style and layout the HTML elements on a webpage. It is like the makeup and clothing of the webpage. It changes the colors, fonts, spacing, sizes, positioning, and other visual aspects of HTML elements.

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