

Week 5 Assignment 1

Course: [Cloud and Network Security - C1-2026](#)

Student Name: [Bussllus Bertrand](#)

Student Number: [CS-CNS11-26004](#)

Friday, February 20, 2026

[Class Exercise: Introduction to Web Applications](#)

Week 5 Assignment 1

Contents

Introduction	3
Questions and Answers.....	3
HTML	3
Cascading Style Sheets (CSS).....	4
Sensitive Data Exposure.....	4
HTML Injection.....	5
Cross-Site Scripting (XSS)	5
Back End Servers	6
Web Servers	6
Databases.....	7
Development Frameworks & APIs	7
Common Web Vulnerabilities	8
Shareable link.....	9
Verification of Completion	9
Conclusion.....	10

Introduction

This report details the concepts and security principles explored in the Hack The Box Academy module, Introduction to Web Applications. As modern web applications grow in complexity, understanding their underlying architecture is a critical first step for identifying and mitigating security risks. This report will break down the fundamental differences between front-end and back-end environments. On the client side, it explores core front-end components such as HTML, CSS, and JavaScript, alongside critical vulnerabilities including Data Exposure, HTML Injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF). Additionally, the report will examine server-side architecture, detailing the roles of back-end servers, web servers, databases, and development APIs, while highlighting the common web vulnerabilities that threaten these systems.

Questions and Answers

HTML

**What is the HTML tag used to show an image? **

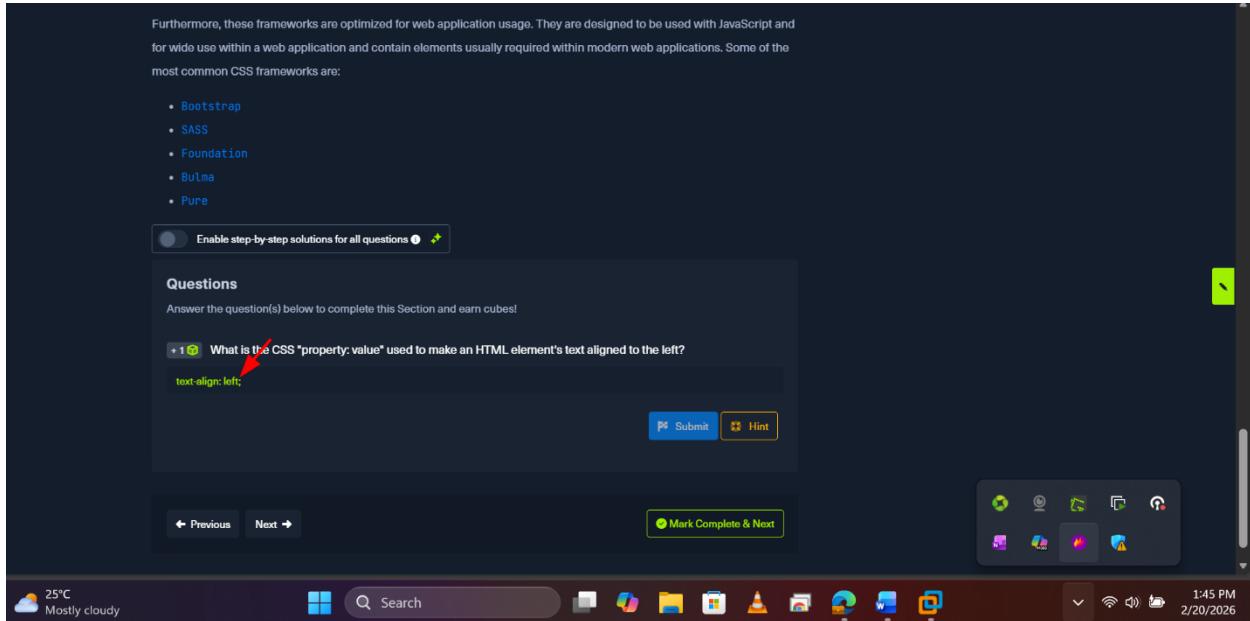
The screenshot shows a dark-themed web application interface for a question. At the top, there is explanatory text about the DOM and how to locate elements. Below this, a button allows users to enable step-by-step solutions. The main area is titled 'Questions' and contains a single question: '+1 What is the HTML tag used to show an image?'. A red arrow points to the word '' in the question text. At the bottom of the question card are 'Submit' and 'Hint' buttons. Below the question cards, there are navigation buttons for 'Previous' and 'Next' and a 'Mark Complete & Next' button. The bottom of the screen shows a Windows taskbar with various icons and system status indicators.

Week 5 Assignment 1

Cascading Style Sheets (CSS)

What is the CSS "property: value" used to make an HTML element's text aligned to the left?

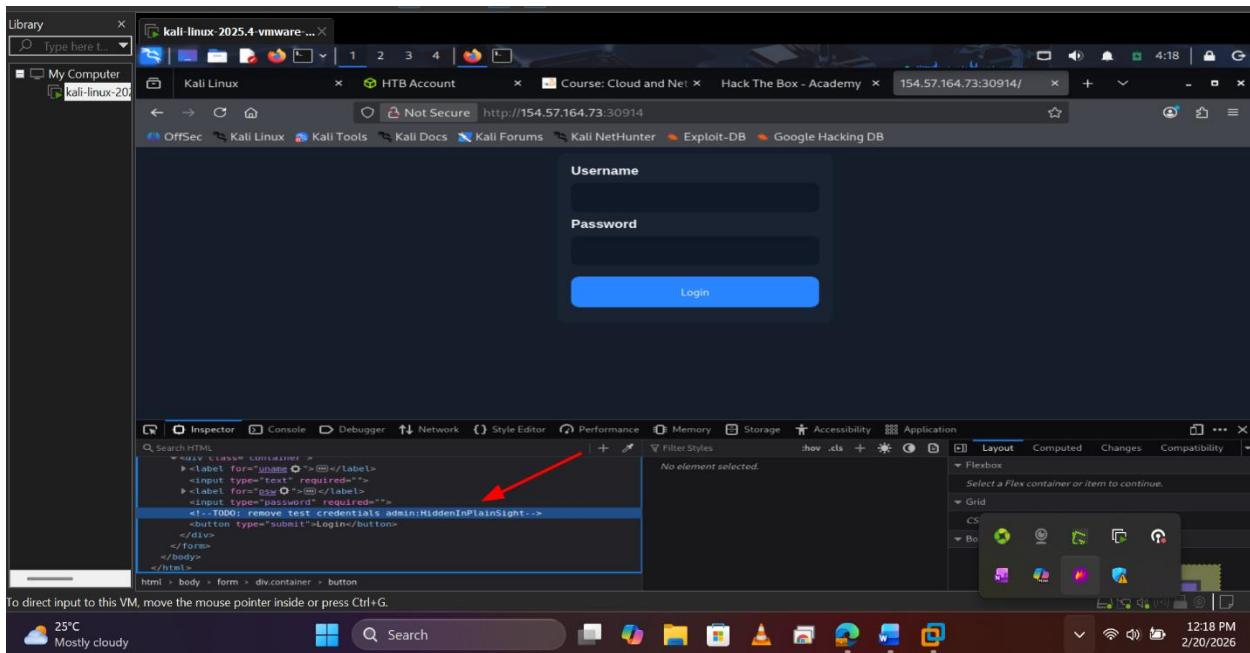
text-align: left;



Sensitive Data Exposure

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

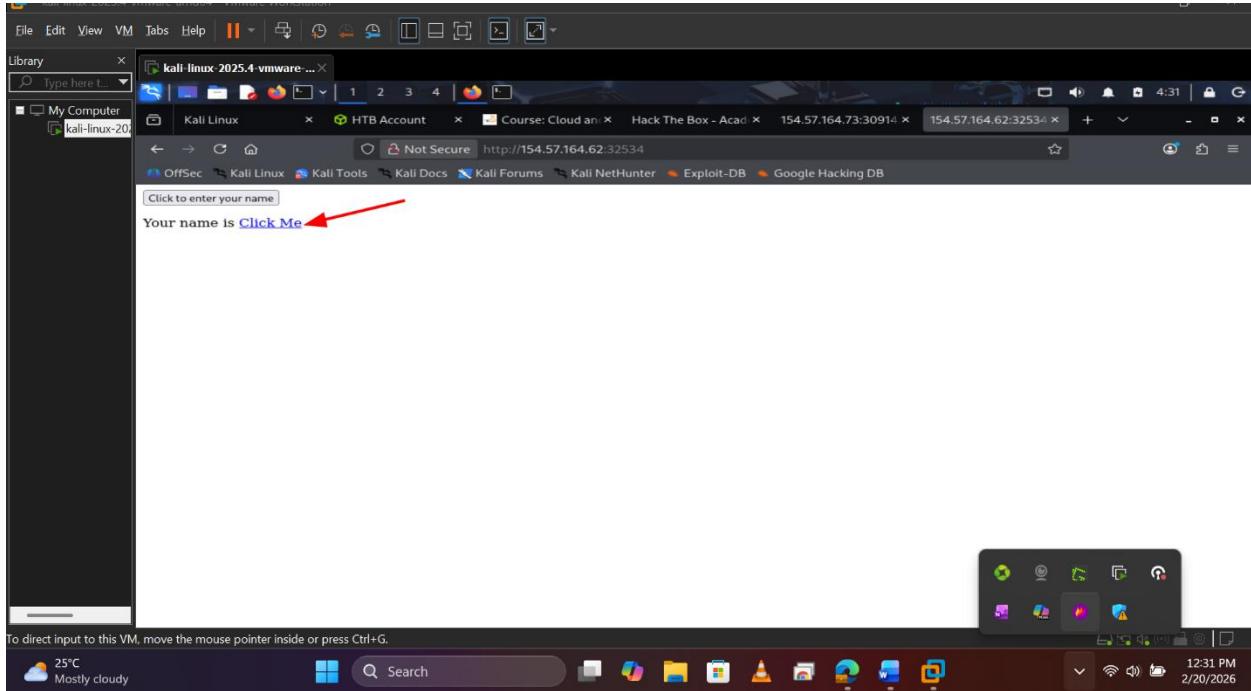
HiddenInPlainSight



Week 5 Assignment 1

HTML Injection

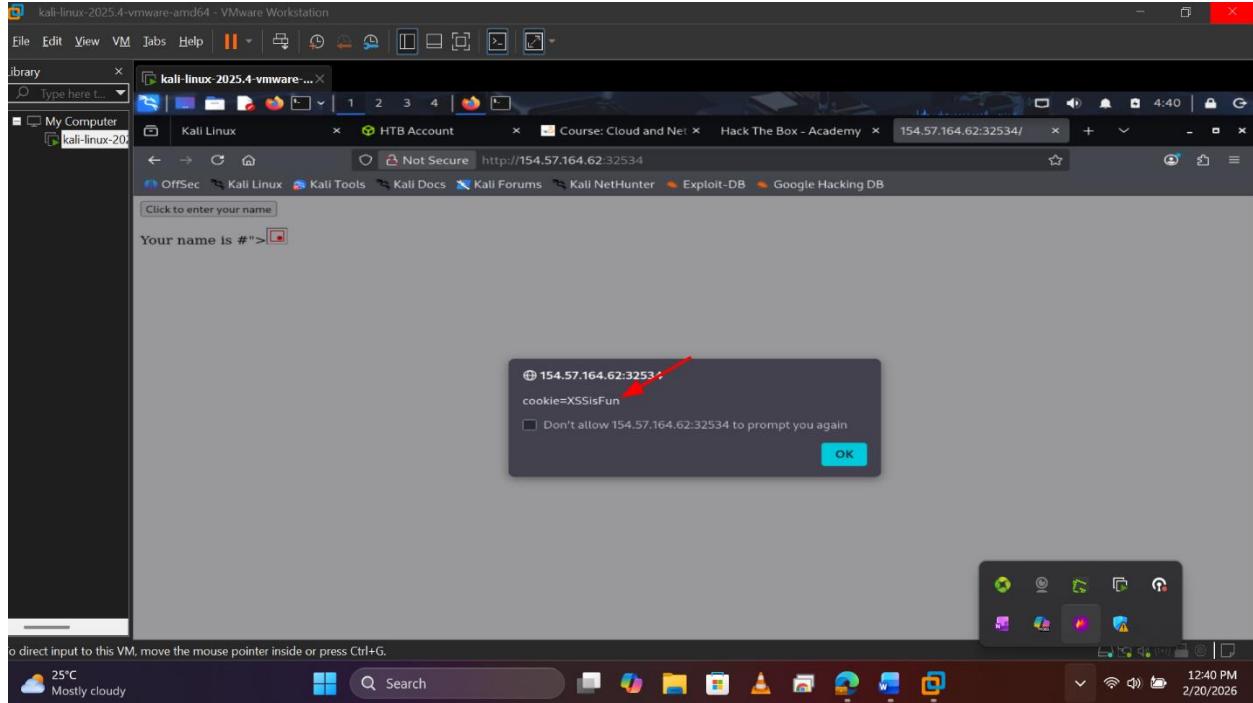
What text would be displayed on the page if we use the following payload as our input: Click Me Your name is click Me



Cross-Site Scripting (XSS)

Try to use XSS to get the cookie value in the above page XSSisFun

Week 5 Assignment 1



Back End Servers

What operating system is 'WAMP' used with? Windows

A screenshot of a web page titled 'Cross-Site Request Forgery (CSRF)' which discusses back-end server stacks. The page is divided into sections: 'Web Server' (Apache, NGINX, IIS), 'Web Application' (PHP, C#, Java), and 'Database' (MySQL, MS SQL, Oracle). It lists common combinations like LAMP, WAMP, WINS, MAMP, and XAMPP. A red arrow points to the 'Windows, Apache, MySQL, and PHP.' entry under the WAMP section. The page also includes a sidebar with sections like 'Back End Components' (Back End Servers, Web Servers, Databases, Development Frameworks & APIs), 'Back End Vulnerabilities' (Common Web Vulnerabilities, Public Vulnerabilities), 'Next Steps', and 'My Workstation' (status: OFFLINE).

Web Servers

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

Week 5 Assignment 1

The screenshot shows a browser window displaying the MDN Web Docs page for 'HTTP response status codes'. The left sidebar has a tree view with 'HTTP response status codes' expanded. A red arrow points to the '201 Created' section in the main content area. The content describes it as a success code for creating a new resource.

Databases

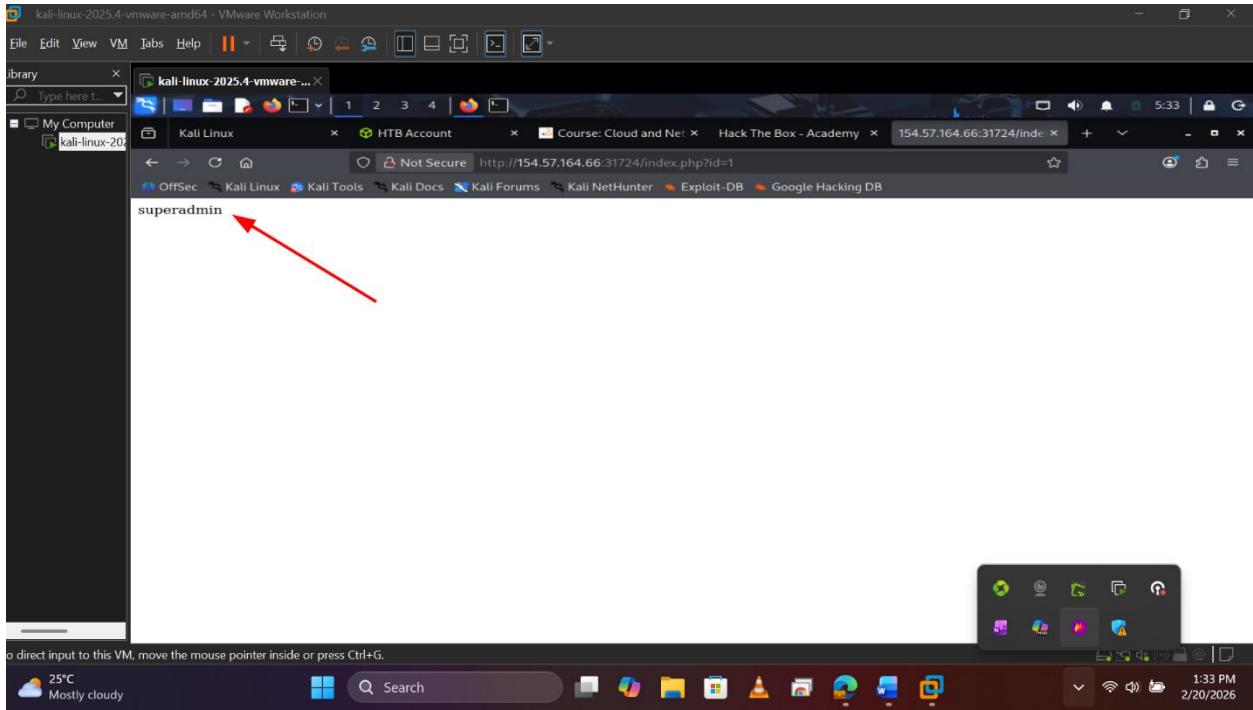
What type of database is Google's Firebase Database? NoSQL

The screenshot shows a Codecademy challenge for 'Firebase Database'. It includes a code editor with PHP code, a question section with a question about the database type, and a feedback section. A red arrow points to the question 'What type of database is Google's Firebase Database?' where 'NoSQL' is selected as the answer.

Development Frameworks & APIs

Use GET request '/index.php?id=0' to search for the name of the user with id number 1?
superadmin

Week 5 Assignment 1



Common Web Vulnerabilities

To which of the above categories does public vulnerability 'CVE-2014-6271' belongs to?

Command injection

A screenshot of a web-based learning platform. The question asks: "To which of the above categories does public vulnerability 'CVE-2014-6271' belong to?". A red arrow points from the question text to the input field where the user has typed "command injection". The response is correct, indicated by a green success message: "Success Congratulations! You earned 1 cubes!". The desktop environment at the bottom shows the date and time.

What is the CVSS v2.0 score of the public vulnerability CVE-2017-0144? 9.3

Week 5 Assignment 1

The most critical vulnerabilities for back-end components are found in web servers, as they are publicly accessible over the **TCP** protocol. An example of a well-known web server vulnerability is the **ShellShock**, which affected Apache web servers released during and before 2014 and utilized **HTTP** requests to gain remote control over the back-end server.

As for vulnerabilities in the back-end server or the database, they are usually utilized after gaining local access to the back-end server or back-end network, which may be gained through **external** vulnerabilities or during internal penetration testing. They are usually used to gain high privileged access on the back-end server or the back-end network or gain control over other servers within the same network.

Although not directly exploitable externally, these vulnerabilities are still critical and need to be patched to protect the entire web application from being compromised.

Enable step-by-step solutions for all questions ⓘ

Questions

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

+1 🎁 What is the CVSS v2.0 score of the public vulnerability CVE-2017-0144?

9.3

Submit **Hint**

◀ Previous Next ▶

+10 Streak pts

Mark Complete & Next

Success
Congratulations! You earned 1 cubes!

25°C
Mostly cloudy

Search

Cloudy icon

Wi-Fi icon

Speaker icon

Battery icon

2/120/2026

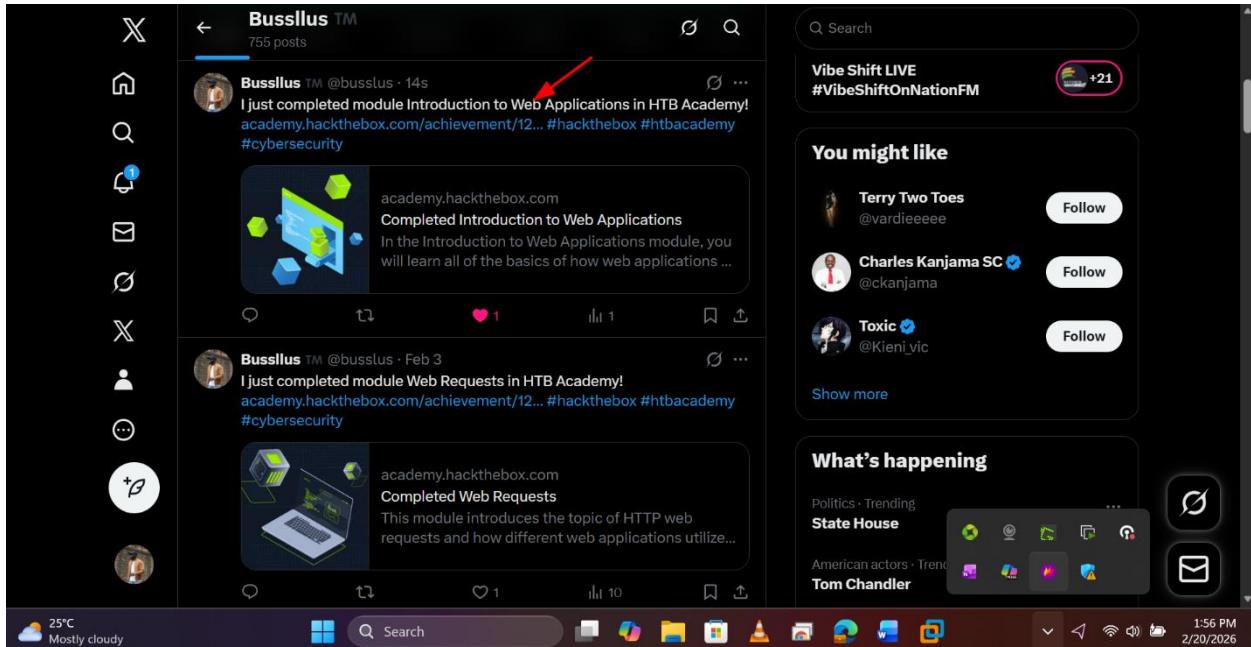
Shareable link

<https://academy.hackthebox.com/achievement/1264364/75>

Verification of Completion

This completion has been shared on professional networks like Twitter to publicly document my commitment to continuous learning in cybersecurity. This section provides the official verification artifacts for the "introduction to web applications" module.

Week 5 Assignment 1



Conclusion

In conclusion, the Hack The Box lab provided a foundational understanding of how web applications operate and where their most significant security weaknesses reside. By analyzing both sides of web application architecture, it is evident that robust security requires a defense-in-depth approach. The front-end remains highly susceptible to user-targeted attacks like HTML Injection and XSS/CSRF, which manipulate how browsers interpret data. Conversely, the back-end infrastructure including databases and web frameworks must be secured against public and common web vulnerabilities that could compromise the entire server environment. Ultimately, mastering the interplay between these front-end and back-end components is essential for effectively securing modern web applications against evolving cyber threats.