COURSE: CLOUD AND NETWORK SECURITY

NAME: DENISE SOPHY ONDISO MUTAYI

STUDENT NO: CS-CN09-25047

INTRODUCTION TO WEB APPLICATIONS

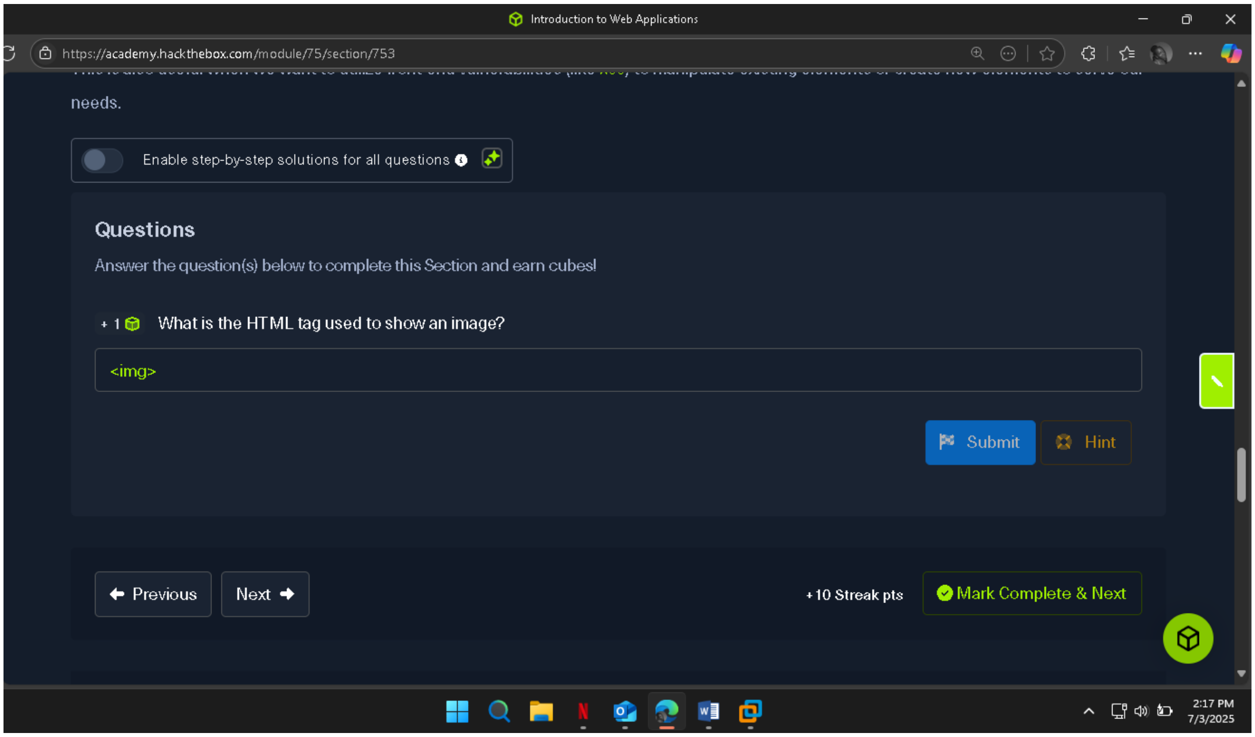
TABLE OF CONTENTS

INTRODUCTION TO WEB APPLICATIONS

This lab provides a comprehensive walkthrough of web application architecture, exploring both the front-end and back-end components that make modern web platforms function. It introduces essential technologies like HTML, CSS, JavaScript, and dives into how web servers, databases, and development frameworks collaborate to serve dynamic content. The lab also highlights major security risks that impact web applications—including HTML Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection, and Command Injection. Through practical examples and vulnerability analysis, the lab underscores the importance of input validation, secure coding practices, and understanding how public CVEs like Shellshock (CVE-2014-6271) and EternalBlue (CVE-2017-0144) can be exploited in real-world scenarios.

HTML

HTML (HyperText Markup Language) is the foundational language used to structure and display content on web pages. It defines elements like headings, paragraphs, forms, and images, which are interpreted by browsers to render a complete web interface. HTML follows a hierarchical structure where tags like <head> and <body> organize the page's metadata and visible content, respectively. Understanding the Document Object Model (DOM) is crucial for identifying and manipulating page elements, especially in web development and cybersecurity contexts. Additionally, URL encoding ensures that special characters are correctly transmitted over the web, enhancing both functionality and security.



Introduction to Web Applications
https://academy.hackthebox.com/module/75/section/753

needs.

Enable step-by-step solutions for all questions

Questions

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

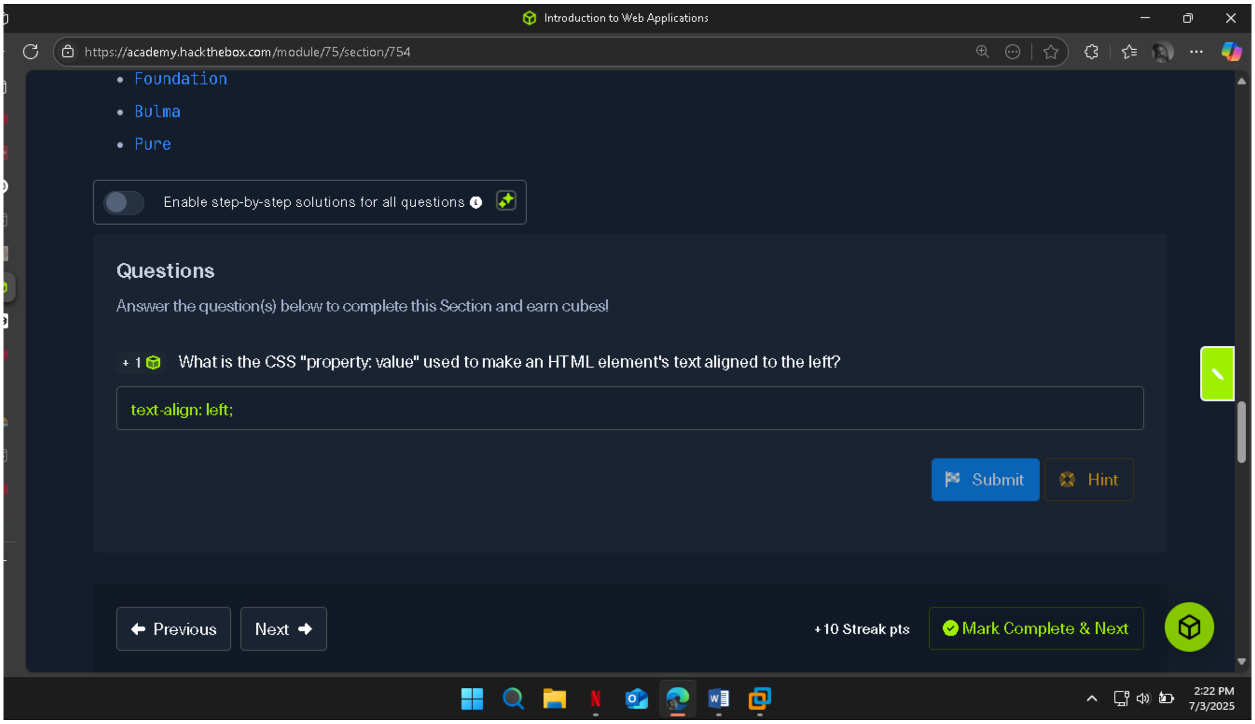
+ 1 What is the HTML tag used to show an image?

<img>

Submit
Hint
Previous
Next
+10 Streak pts
Mark Complete & Next
2:17 PM
7/3/2025

CASCADING STYLE SHEETS (CSS)

It is the stylesheet language used alongside HTML to format and set the style of HTML elements. Like HTML, there are several versions of CSS, and each subsequent version introduces a new set of capabilities that can be used for formatting HTML elements. Browsers are updated alongside it to support these new features.


Introduction to Web Applications
https://academy.hackthebox.com/module/75/section/754
2:22 PM
7/3/2025

- Foundation
- Bulma
- Pure

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

text-align: left;

Submit
Hint
Previous
Next
+10 Streak pts
Mark Complete & Next

JAVASCRIPT

Most common web applications heavily rely on JavaScript to drive all needed functionality on the web page, like updating the web page view in real-time, dynamically updating content in real-time, accepting and processing user input, and many other potential functionalities.

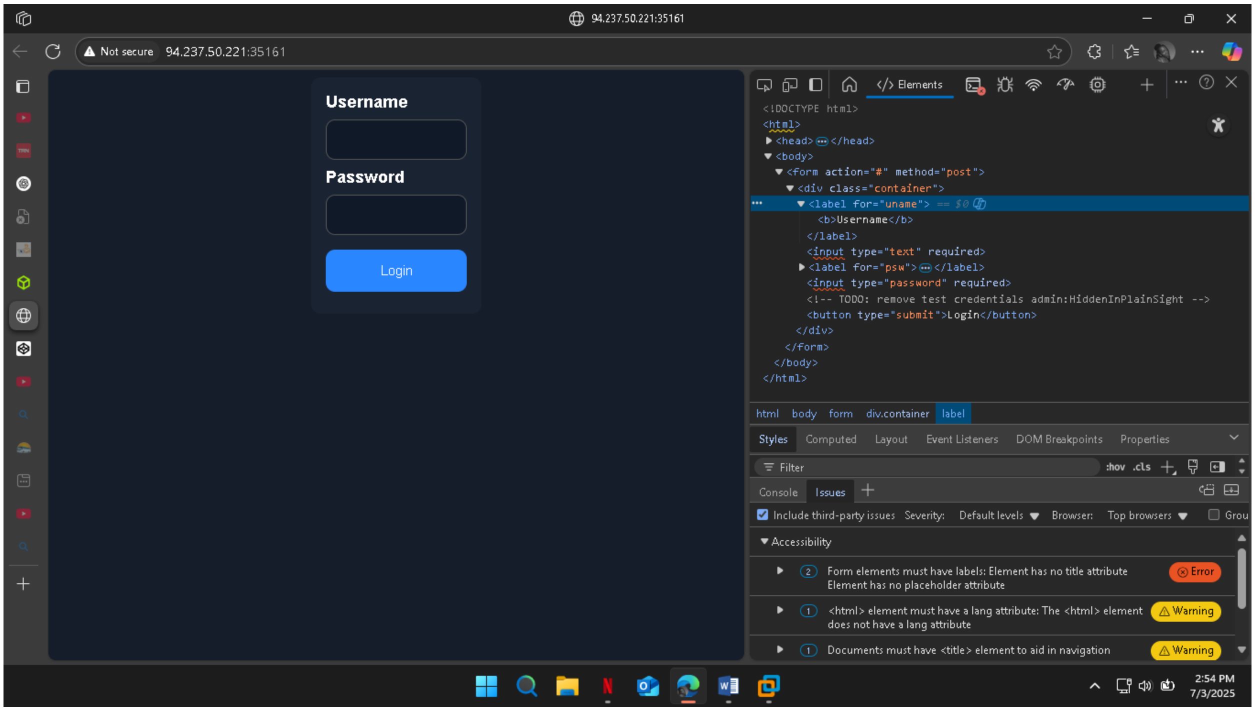
JavaScript is also used to automate complex processes and perform HTTP requests to interact with the back end components and send and retrieve data, through technologies like Ajax.

In addition to automation, JavaScript is also often used alongside CSS, as previously mentioned, to drive advanced animations that would not be possible with CSS alone. Whenever we visit an interactive and dynamic web page that uses many advanced and visually appealing animations, we are seeing the result of active JavaScript code running on our browser.

All modern web browsers are equipped with JavaScript engines that can execute JavaScript code on the client-side without relying on the back end webserver to update the page. This makes using JavaScript a very fast way to achieve a large number of processes quickly.

SENSITIVE DATA EXPOSURE

It refers to the availability of sensitive data in clear-text to the end-user.

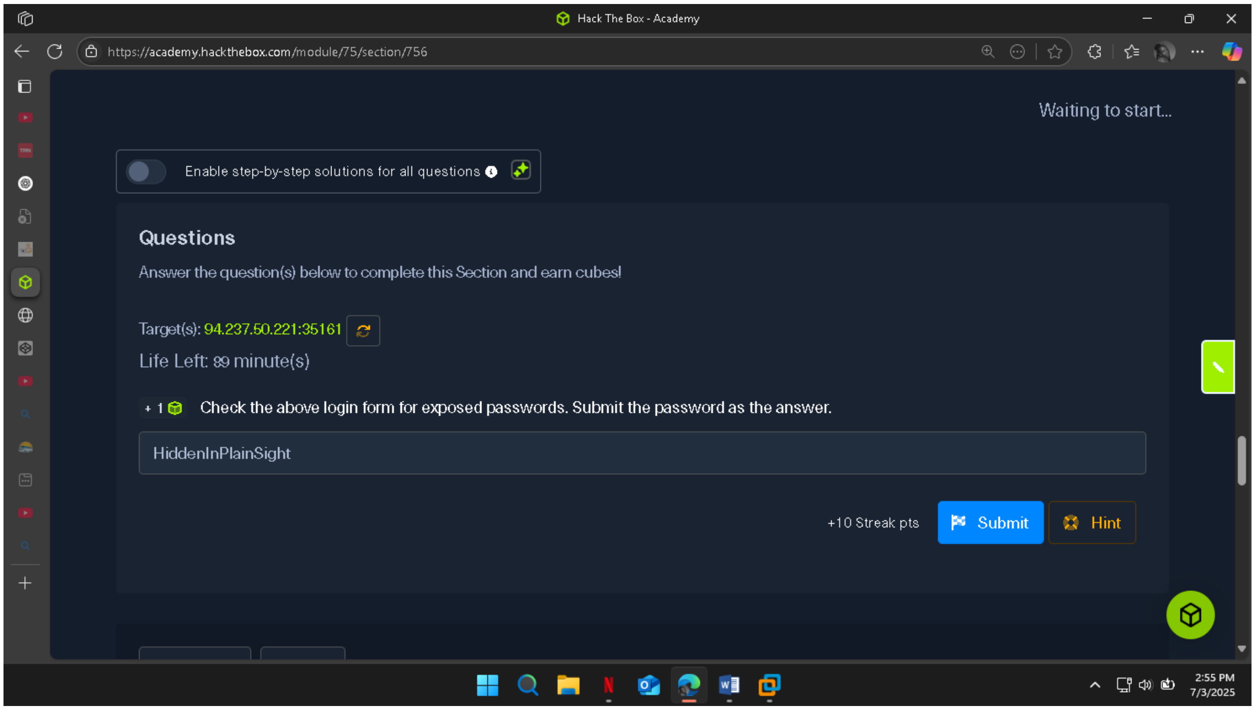

94.237.50.221:35161
Not secure 94.237.50.221:35161
Username
Password
Login
Elements
html body form div.container label
Styles Computed Layout Event Listeners DOM Breakpoints Properties
Filter :hov .cls
Console Issues
2:54 PM
7/3/2025

```
<!DOCTYPE html>
<html>
▶<head>…</head>
▼<body>
  ▼<form action="#" method="post">
    ▼<div class="container">
      ▼<label for="uname"> == $0
          <b>Username</b>
        </label>
        <input type="text" required>
      ▶<label for="psw">…</label>
        <input type="password" required>
        <!-- TODO: remove test credentials admin:HiddenInPlainSight -->
        <button type="submit">Login</button>
      </div>
    </form>
  </body>
</html>
```

☑ Include third-party issues Severity: Default levels Browser: Top browsers □ Grou

▼ Accessibility

- 2 Form elements must have labels: Element has no title attribute Element has no placeholder attribute — Error
- 1 <html> element must have a lang attribute: The <html> element does not have a lang attribute — Warning
- 1 Documents must have <title> element to aid in navigation — Warning


Hack The Box - Academy
https://academy.hackthebox.com/module/75/section/756
Waiting to start...
Enable step-by-step solutions for all questions
+10 Streak pts
Submit
Hint
2:55 PM
7/3/2025

Questions

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

Target(s): 94.237.50.221:35161

Life Left: 89 minute(s)

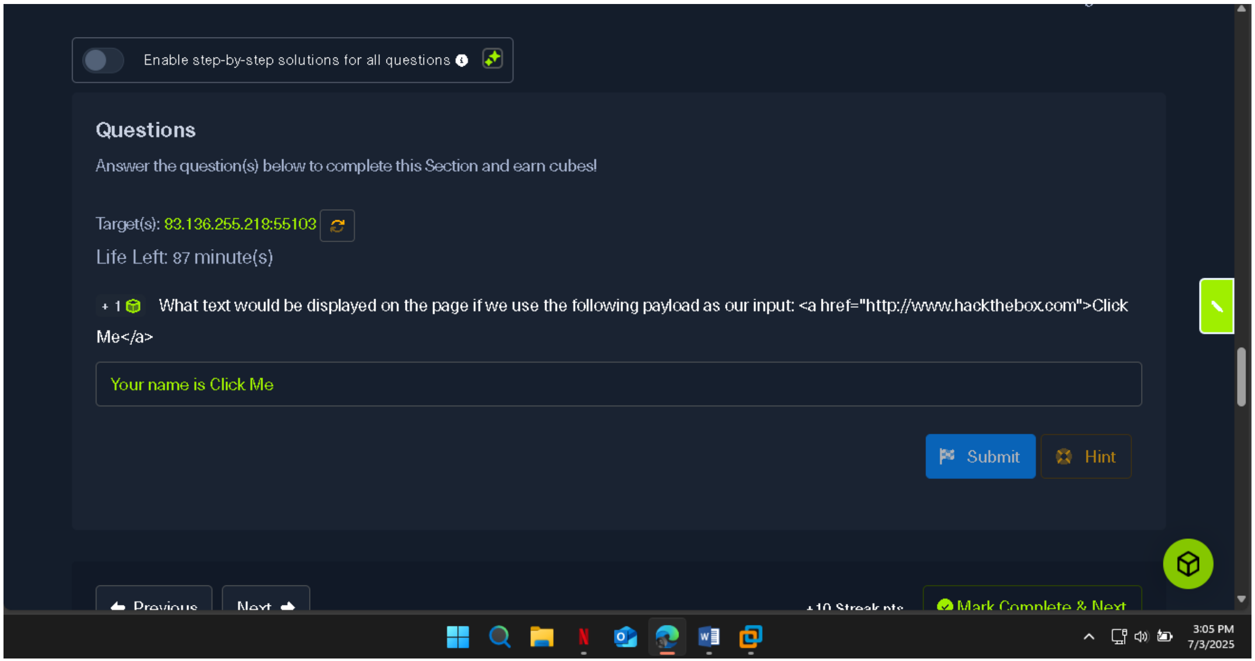
+ 1 Check the above login form for exposed passwords. Submit the password as the answer.

HiddenInPlainSight

HTML INJECTION

HTML injection occurs when unfiltered user input is displayed on the page. This can either be through retrieving previously submitted code, like retrieving a user comment from the back end database, or by directly displaying unfiltered user input through JavaScript on the front end.

When a user has complete control of how their input will be displayed, they can submit HTML code, and the browser may display it as part of the page. This may include a malicious HTML code, like an external login form, which can be used to trick users into logging in while actually sending their login credentials to a malicious server to be collected for other attacks.



Questions

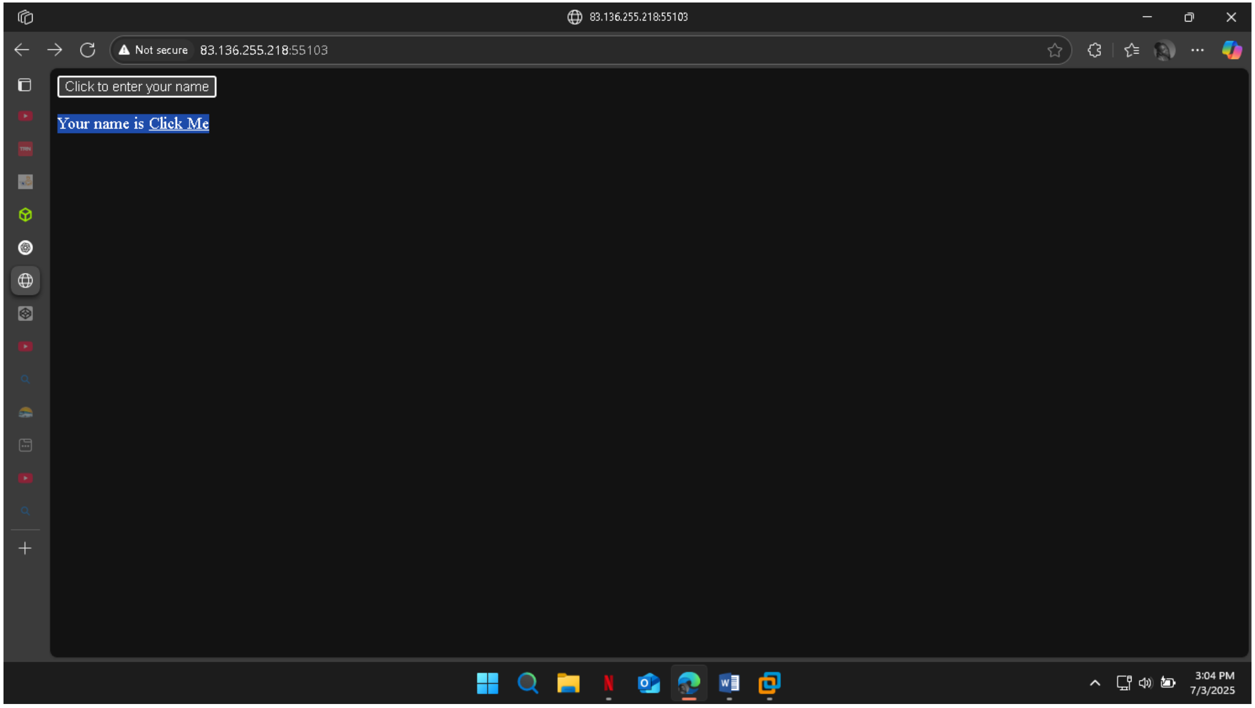
Answer the question(s) below to complete this Section and earn cubes!

Target(s): 83.136.255.218:55103

Life Left: 87 minute(s)

+ 1 What text would be displayed on the page if we use the following payload as our input: <a href="http://www.hackthebox.com">Click Me</a>

Your name is Click Me



Not secure 83.136.255.218:55103

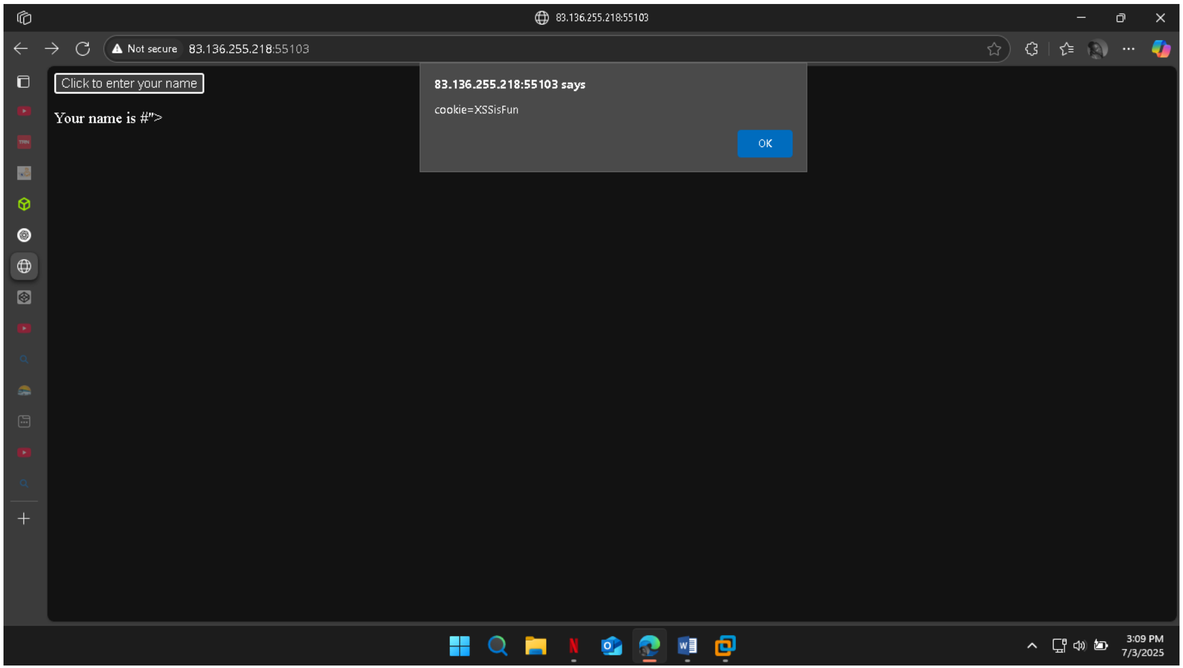
Click to enter your name

Your name is Click Me

CROSS-SITE SCRIPTING (XSS)

Cross-Site Scripting (XSS) attacks by injecting JavaScript code to be executed on the client-side. Once we can execute code on the victim's machine, we can potentially gain access to the victim's account or even their machine. XSS is very similar to HTML Injection in practice. However, XSS involves the injection of JavaScript code to perform more advanced attacks on the client-side, instead of merely injecting HTML code. There are three main types of XSS:

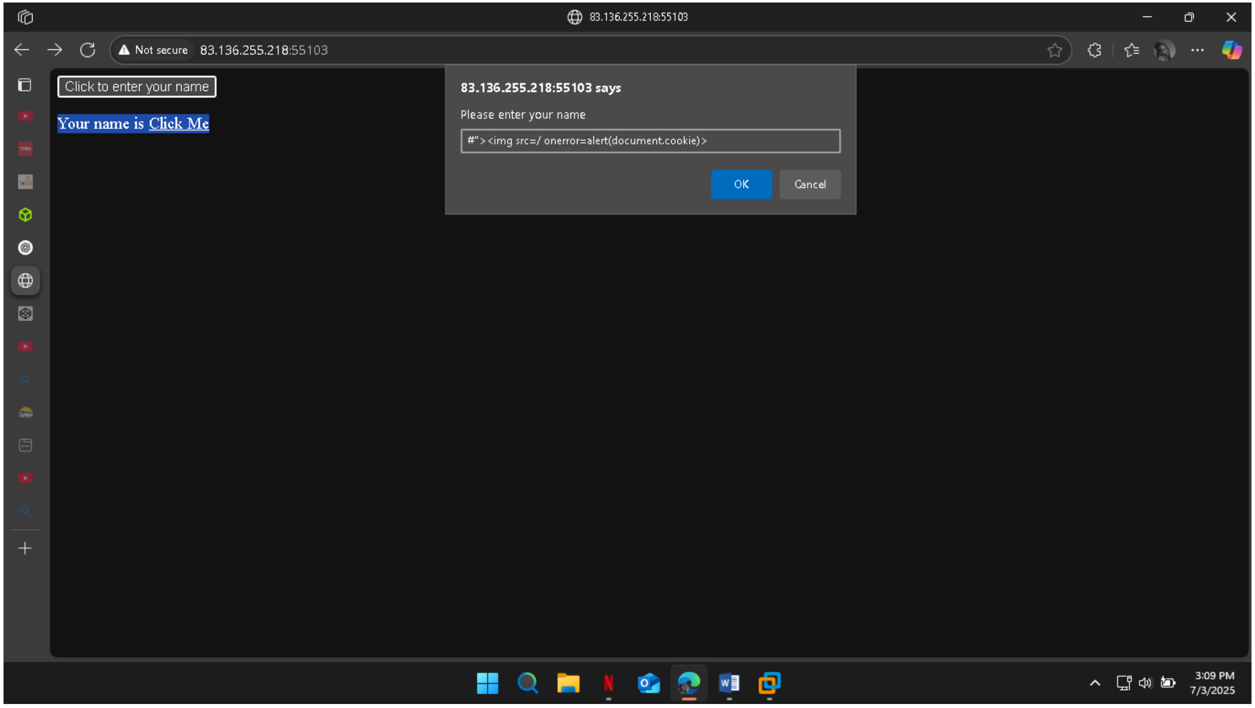
Type	Description
Reflected XSS	Occurs when user input is displayed on the page after processing (e.g., search result or error mes
Stored XSS	Occurs when user input is stored in the back end database and then displayed upon retrieval (e.g
DOM XSS	Occurs when user input is directly shown in the browser and is written to an HTML DOM objec



Your name is #">

83.136.255.218:55103 says

cookie=XSSisFun

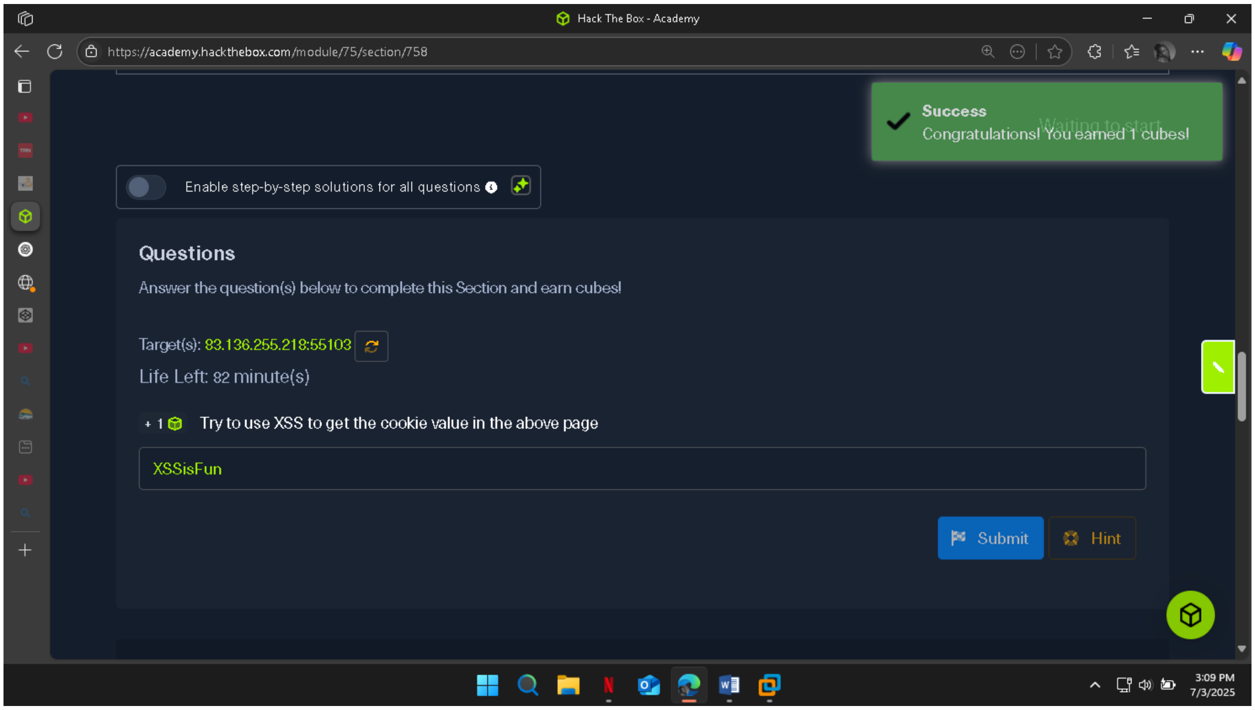


Your name is Click Me

83.136.255.218:55103 says

Please enter your name

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



Hack The Box - Academy
https://academy.hackthebox.com/module/75/section/758
Success
Congratulations! You earned 1 cubes!
Enable step-by-step solutions for all questions
Submit
Hint
3:09 PM
7/3/2025

Questions

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

Target(s): 83.136.255.218:55103

Life Left: 82 minute(s)

+ 1 Try to use XSS to get the cookie value in the above page

XSSisFun

CROSS-SITE REQUEST FORGERY (CSRF)

Cross-Site Request Forgery (CSRF). CSRF attacks may utilize XSS vulnerabilities to perform certain queries, and API calls on a web application that the victim is currently authenticated to. This would allow the attacker to perform actions as the authenticated user. It may also utilize other vulnerabilities to perform the same functions, like utilizing HTTP parameters for attacks.

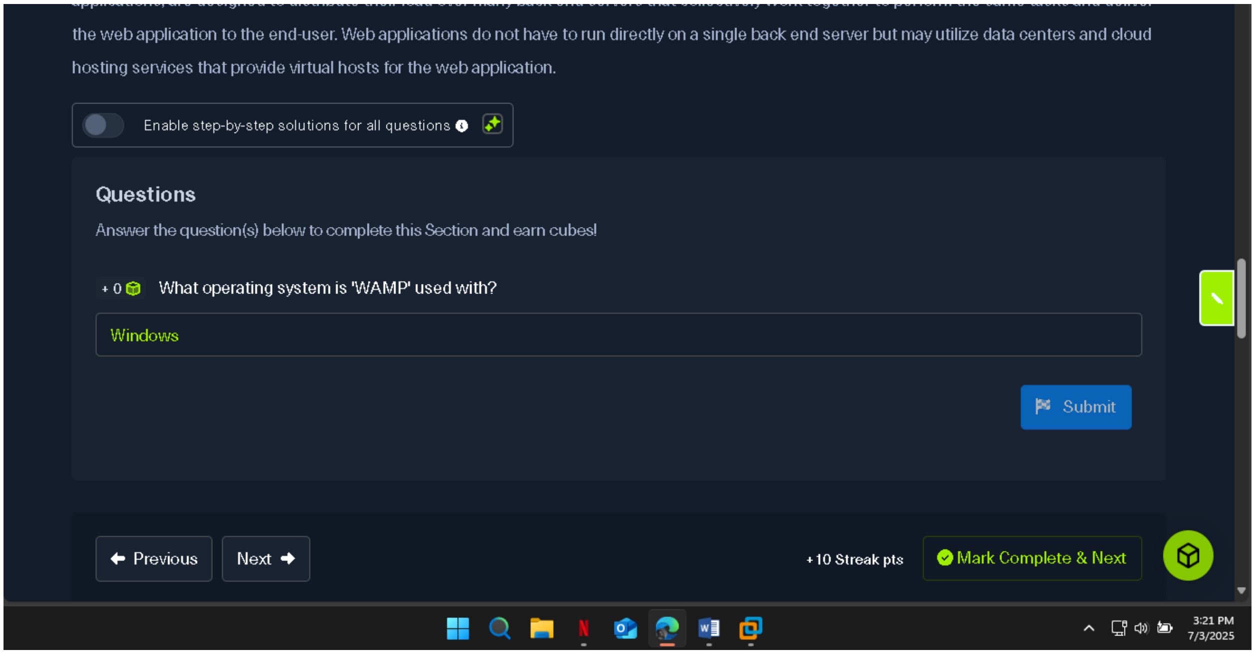
PREVENTION

Sanitization- Removing special characters and non-standard characters from user input before displaying it or storing it.

Validation- Ensuring that submitted user input matches the expected format (i.e., submitted email matched email format)

BACK END SERVERS

A back-end server is the powerhouse behind a web application, responsible for running essential processes and managing the data access layer. It includes key components like the **web server** (e.g., Apache, NGINX, IIS), **database** (e.g., MySQL, MS SQL), and **development frameworks** (e.g., PHP, Java, .NET). These elements are often bundled into popular tech stacks like LAMP, WAMP, and XAMPP. The server runs on robust hardware and may also include software like hypervisors, containers, and WAFs. Large-scale apps often use multiple back-end servers or cloud-based hosting to distribute load and improve performance.



the web application to the end-user. Web applications do not have to run directly on a single back end server but may utilize data centers and cloud hosting services that provide virtual hosts for the web application.

Enable step-by-step solutions for all questions

Questions

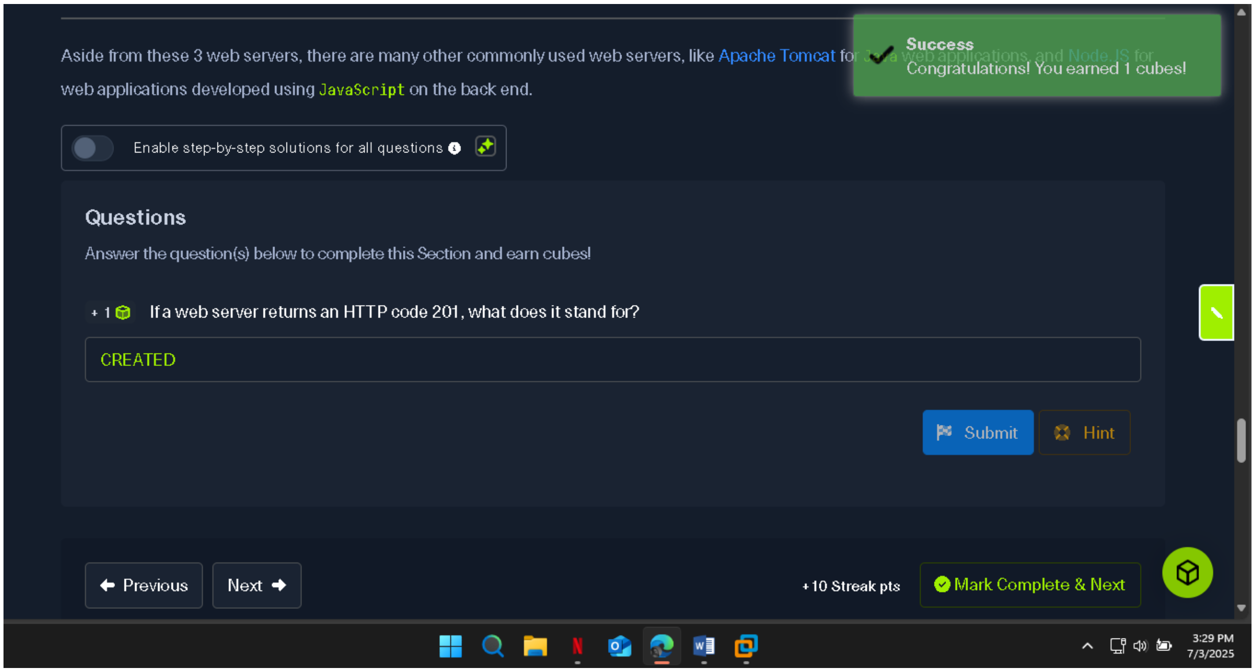
Answer the question(s) below to complete this Section and earn cubes!

+ 0 What operating system is 'WAMP' used with?

Windows

WEB SERVERS

A web server is an application that runs on the back end server, which handles all of the HTTP traffic from the client-side browser, routes it to the requested pages, and finally responds to the client-side browser. Web servers usually run on TCP ports 80 or 443, and are responsible for connecting end-users to various parts of the web application, in addition to handling their various responses.



Aside from these 3 web servers, there are many other commonly used web servers, like Apache Tomcat for Java web applications, and Node.JS for web applications developed using `JavaScript` on the back end.

Success
Congratulations! You earned 1 cubes!

Enable step-by-step solutions for all questions

Questions

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

+ 1 If a web server returns an HTTP code 201, what does it stand for?

CREATED

DATABASES

Web applications utilize back end databases to store various content and information related to the web application. This can be core web application assets like images and files, web application content like posts and updates, or user data like usernames and passwords. This allows web applications to easily and quickly store and retrieve data and enable dynamic content that is different for each user.

There are many different types of databases, each of which fits a certain type of use. Most developers look for certain characteristics in a database, such as speed in storing and retrieving data, size when storing large amounts of data, scalability as the web application grows, and cost.

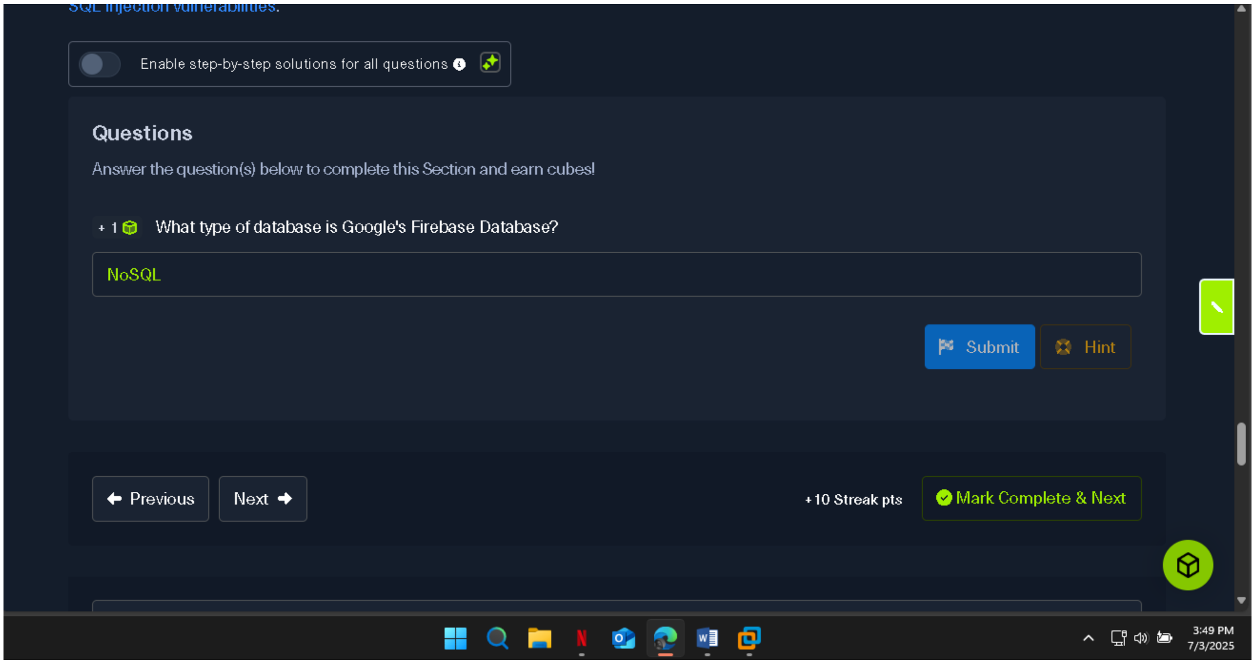
RELATIONAL (SQL)

Relational (SQL) databases store their data in tables, rows, and columns. Each table can have unique keys, which can link tables together and create relationships between tables.

NON-RELATIONAL (NOSQL)

A non-relational database does not use tables, rows, columns, primary keys, relationships, or schemas. Instead, a NoSQL database stores data using various storage models, depending on the type of data stored.

Due to the lack of a defined structure for the database, NoSQL databases are very scalable and flexible. When dealing with datasets that are not very well defined and structured, a NoSQL database would be the best choice for storing our data.



SQL injection vulnerabilities.

Enable step-by-step solutions for all questions

Questions

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

+ 1 What type of database is Google's Firebase Database?

NoSQL

DEVELOPMENT FRAMEWORKS & APIS

Web development frameworks that help in developing core web application files and functionality. With the increased complexity of web applications, it may be challenging to create a modern and sophisticated web application from scratch. Hence, most of the popular web applications are developed using web frameworks.

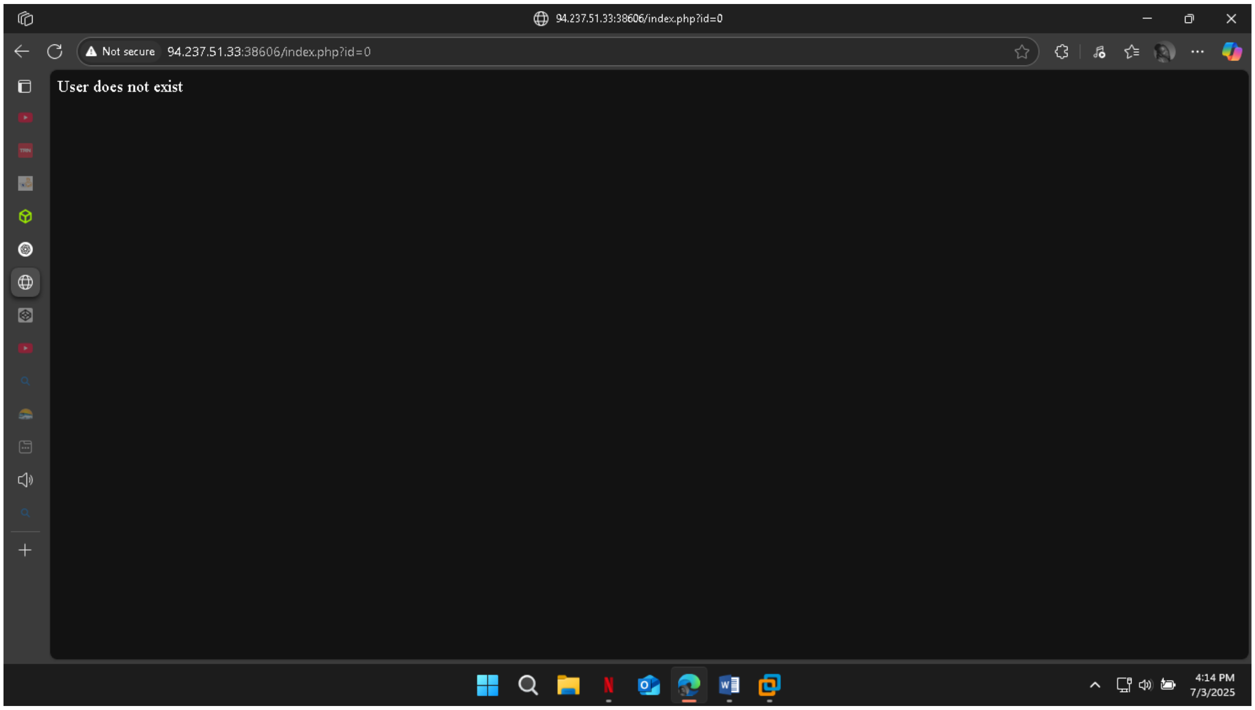
As most web applications share common functionality -such as user registration-, web development frameworks make it easy to quickly implement this functionality and link them to the front end components, making a fully functional web application.

APIs

An API (Application Programming Interface) is an interface within an application that specifies how the application can interact with other applications

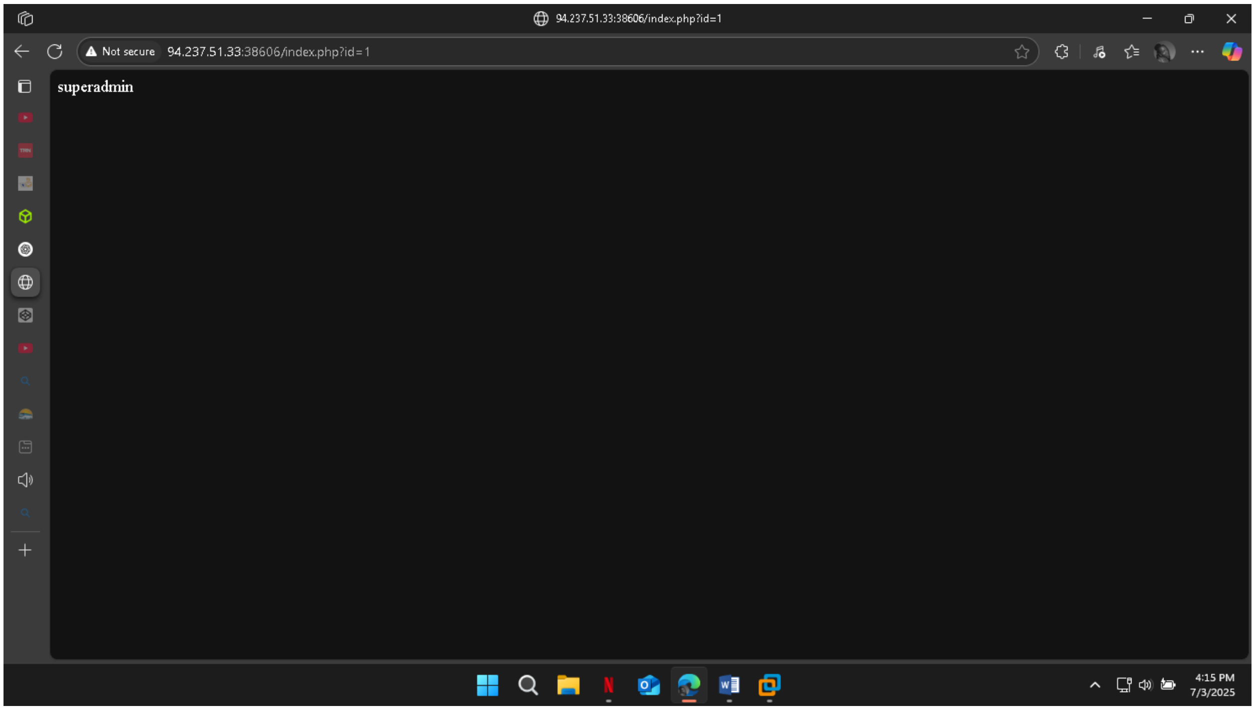
WEB APIS

Web Applications, it is what allows remote access to functionality on back end components. APIs are not exclusive to web applications and are used for software applications in general. Web APIs are usually accessed over the HTTP protocol and are usually handled and translated through web servers. To enable the use of APIs within a web application, the developers have to develop this functionality on the back end of the web application by using the API standards like SOAP or REST.



94.237.51.33:38606/index.php?id=0
Not secure
94.237.51.33:38606/index.php?id=0
4:14 PM
7/3/2025

User does not exist

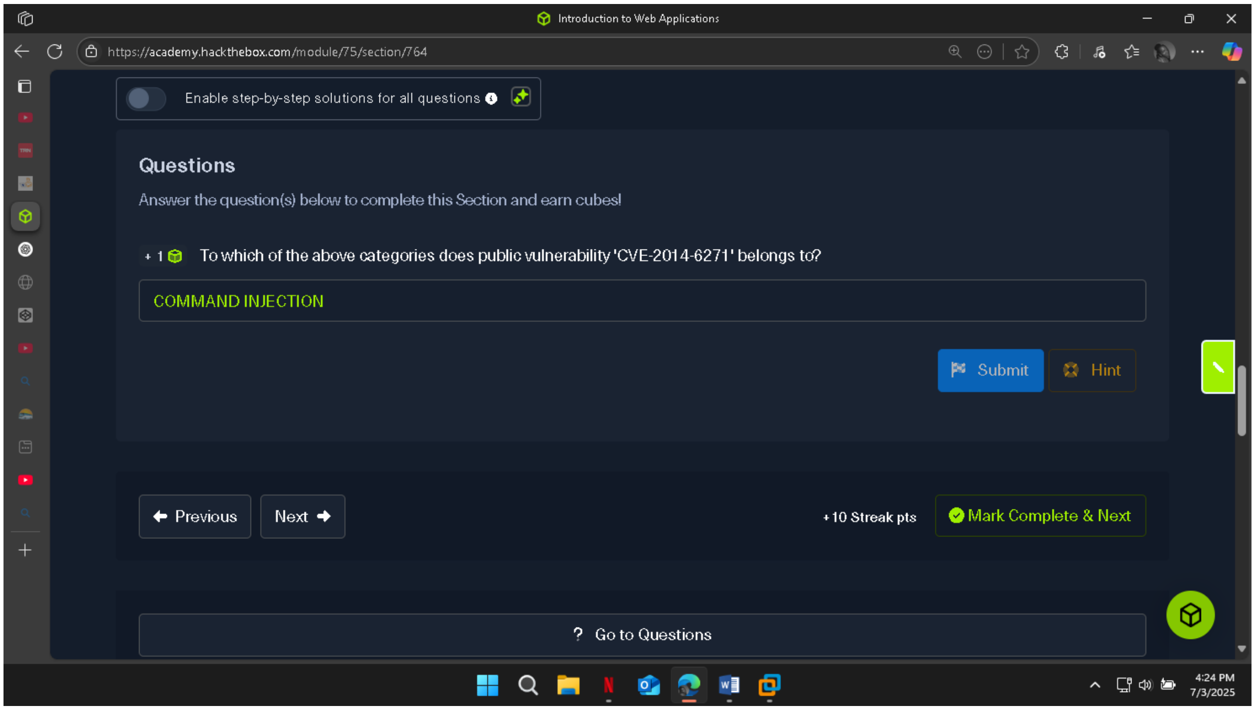


94.237.51.33:38606/index.php?id=1
Not secure
94.237.51.33:38606/index.php?id=1
4:15 PM
7/3/2025

superadmin

COMMON WEB VULNERABILITIES

This section covers common web vulnerabilities often found during penetration testing, especially when no public exploits exist or when developers misconfigure applications. Key issues include Broken Authentication and Access Control, which allow unauthorized access or privilege escalation; Malicious File Upload, enabling attackers to execute scripts by uploading dangerous files; Command Injection, where unsanitized input leads to OS-level command execution; and SQL Injection, which allows manipulation of database queries through user input. These vulnerabilities are part of the OWASP Top 10 and critical to understand for identifying and exploiting weaknesses in web applications.


Introduction to Web Applications
https://academy.hackthebox.com/module/75/section/764
Enable step-by-step solutions for all questions
Submit
Hint
Previous
Next
+10 Streak pts
Mark Complete & Next
Go to Questions
4:24 PM
7/3/2025

Questions

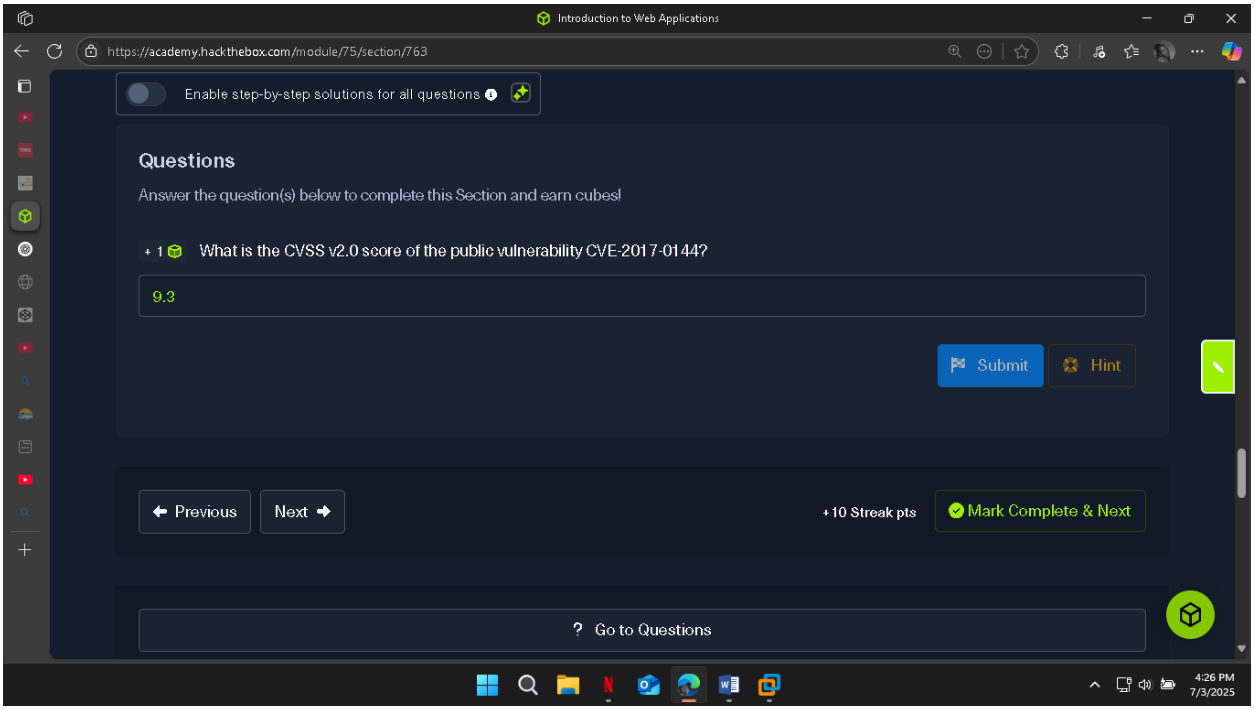
Answer the question(s) below to complete this Section and earn cubes!

+ 1 To which of the above categories does public vulnerability 'CVE-2014-6271' belongs to?

COMMAND INJECTION

PUBLIC VULNERABILITIES

This section explains public vulnerabilities in back-end components that can be exploited externally, especially those with assigned CVE (Common Vulnerabilities and Exposures) records. It emphasizes the importance of identifying web application versions to search for known public exploits in databases like Exploit DB or Rapid7. The Common Vulnerability Scoring System (CVSS) helps measure the severity of vulnerabilities, using CVSS v2.0 and v3.0 scoring systems, with scores guiding how urgently a vulnerability should be addressed. Back-end server vulnerabilities, like Shellshock, can also be exploited remotely and must be patched to secure the web application.



Introduction to Web Applications
https://academy.hackthebox.com/module/75/section/763
Enable step-by-step solutions for all questions

Questions

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

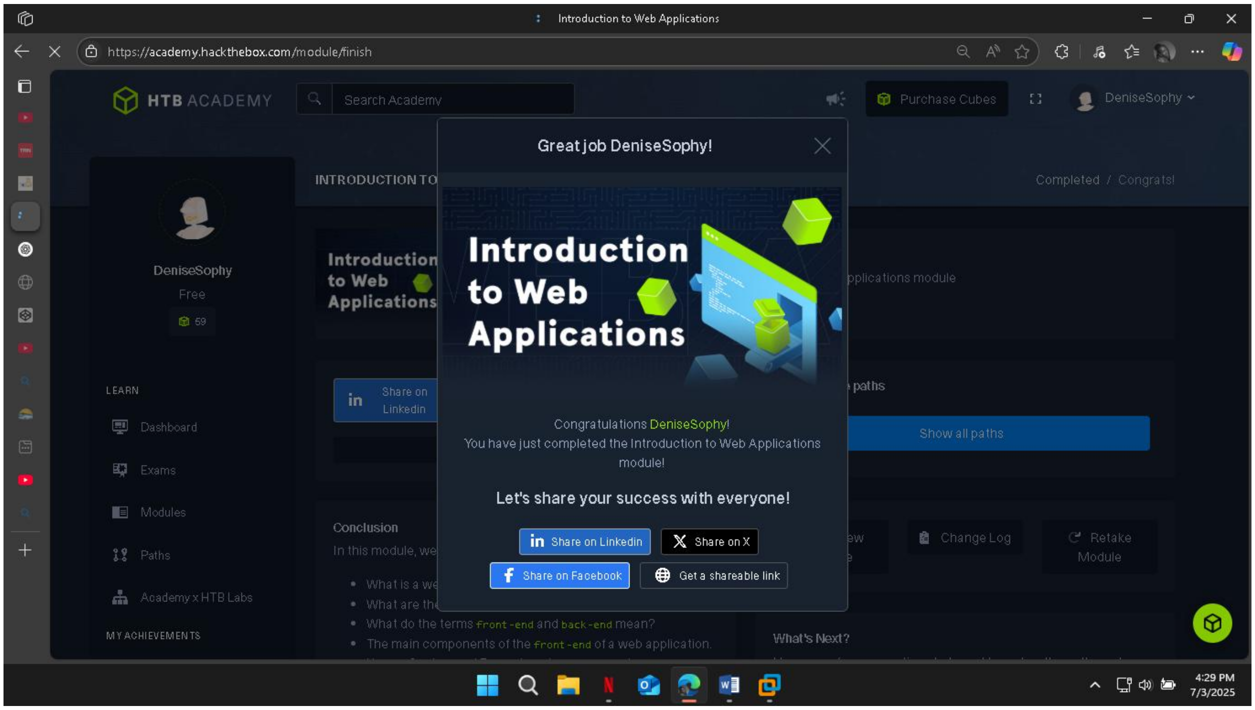
+ 1 What is the CVSS v2.0 score of the public vulnerability CVE-2017-0144?

9.3

Submit
Hint
Previous
Next
+10 Streak pts
Mark Complete & Next
? Go to Questions
4:26 PM
7/3/2025

CONCLUSION

By completing this lab, I’ve gained foundational knowledge of how web applications operate and how attackers exploit their weak points. From client-side vulnerabilities like XSS and HTML injection to server-side risks such as SQLi and command injection, it’s clear that improper input handling and insecure configurations can expose applications to severe threats. The exploration of public vulnerabilities and CVSS scoring has reinforced the importance of patching and staying informed through platforms like Exploit DB and NVD. Ultimately, understanding these vulnerabilities is key to strengthening application security and becoming a more effective cybersecurity practitioner.



Great job DeniseSophy!

Congratulations DeniseSophy!
You have just completed the Introduction to Web Applications module!

Let's share your success with everyone!

Conclusion

In this module, we

- What is a we
- What are the
- What do the terms `front-end` and `back-end` mean?
- The main components of the `front-end` of a web application.