Course: Cloud and Network Security-C1-2026

Cyber Shujaa Program

Week 5: Securing Network Layers 4, 5, 6 & 7

Assignment 1: Introduction to Web Applications

Student Name: Salim Katana Karuku

Student ID: CS-CNS11-26048

Table of Contents

Introduction

This assignment explores the fundamental building block of web applications, including Front- end technologies (HTML, CSS, and JavaScript), back-end processes and the HTTP/S protocol that facilitates communication between clients and servers. A thorough grasp of these components is essential for identifying misconfigurations and vulnerabilities

Objectives

The objectives of the assignment were:

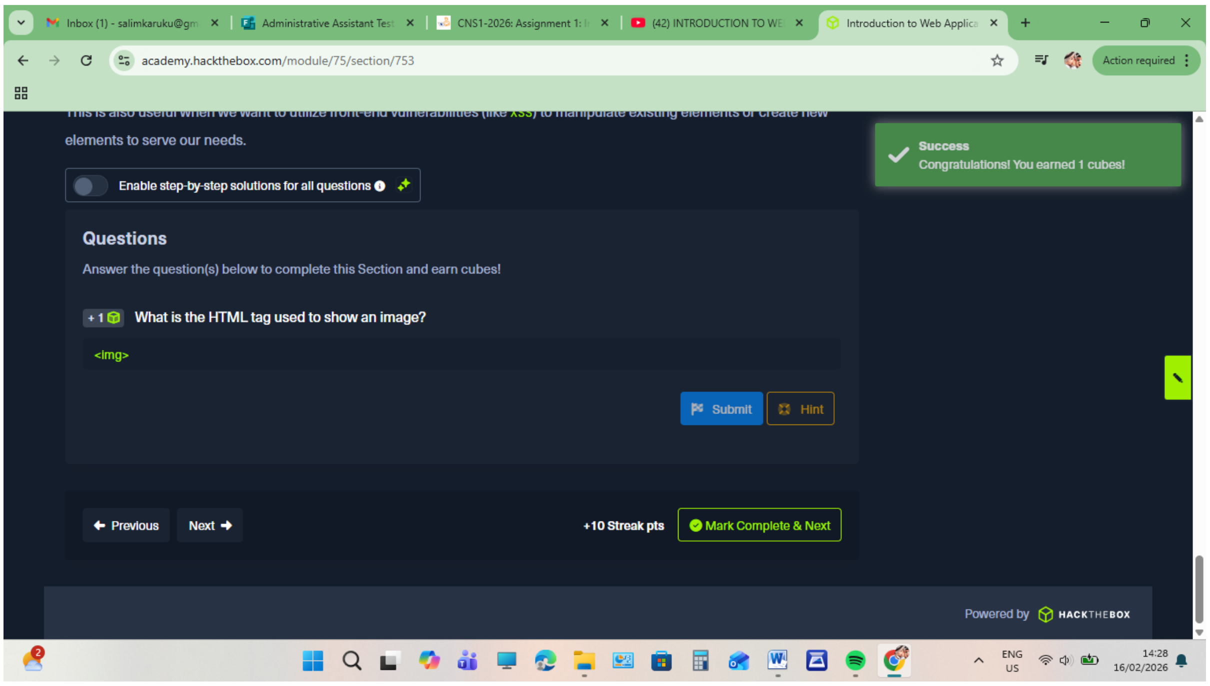
1. To analyse the request- response model
2. To identify web architecture components
3. To explore security implications
4. To master interception tools

Front end Components

In this section, I explored the client-side of the web application to understand how it renders in the browser.

HTML

I used Browser Developer Tools to inspect the page structure of the target host (10.129.231.155). I analyse the tags to understand how the content was organized.



Inbox (1) - salimkaruku@gm | Administrative Assistant Test | CNS1-2026: Assignment 1: | (42) INTRODUCTION TO WE | Introduction to Web Applica

academy.hackthebox.com/module/75/section/753

This is also useful when we want to utilize front-end vulnerabilities (like XSS) to manipulate existing elements or create new elements to serve our 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

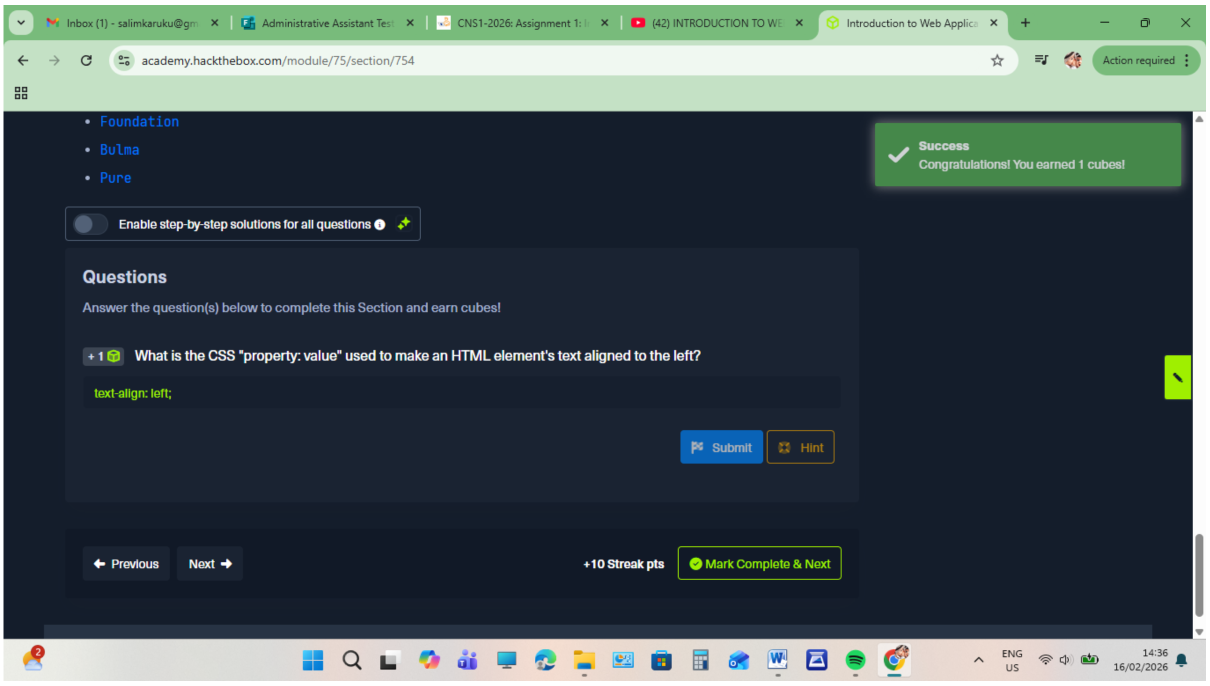
Success
Congratulations! You earned 1 cubes!

Powered by HACKTHEBOX

ENG US 14:28 16/02/2026

CSS

I examined the styling rules to see how the visual layout was constructed and to identify any hidden elements within the stylesheets



Inbox (1) - salimkaruku@gm | Administrative Assistant Test | CNS1-2026: Assignment 1: | (42) INTRODUCTION TO WE | Introduction to Web Applica

academy.hackthebox.com/module/75/section/754

- 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

Success
Congratulations! You earned 1 cubes!

ENG US 14:36 16/02/2026

Java Script

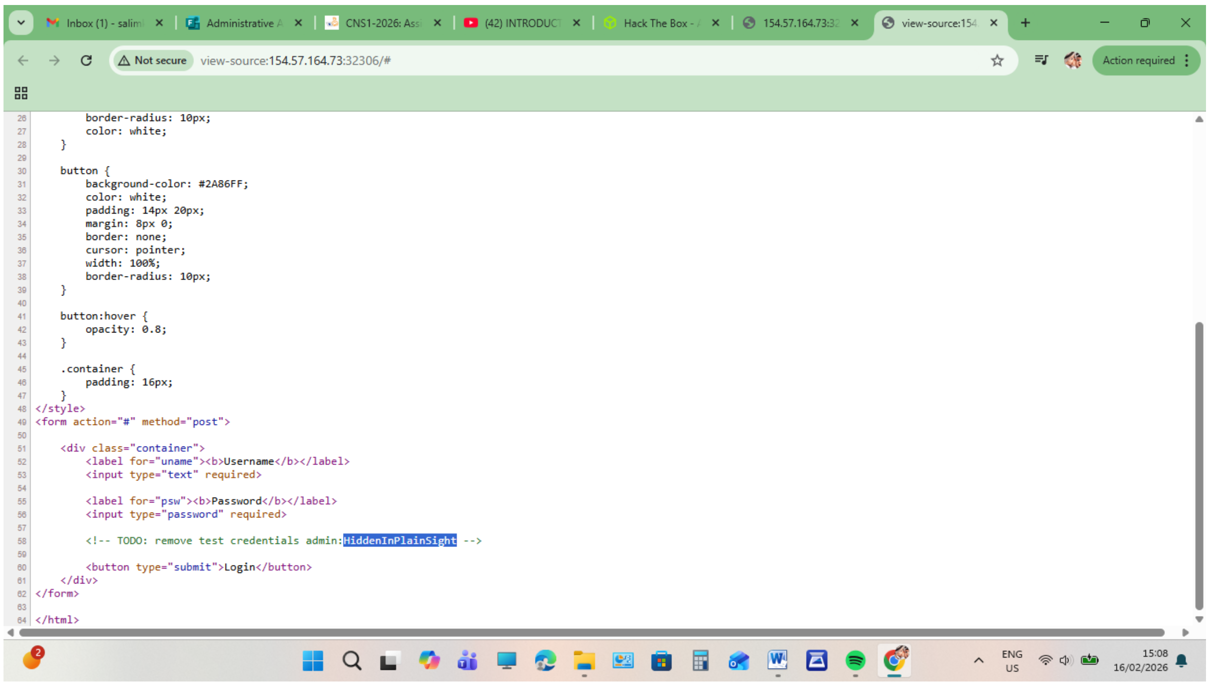
I reviewed the client-side scripts to understand the interactive features of the application and how it handles data before sending it to the server.

Front End Vulnerabilities

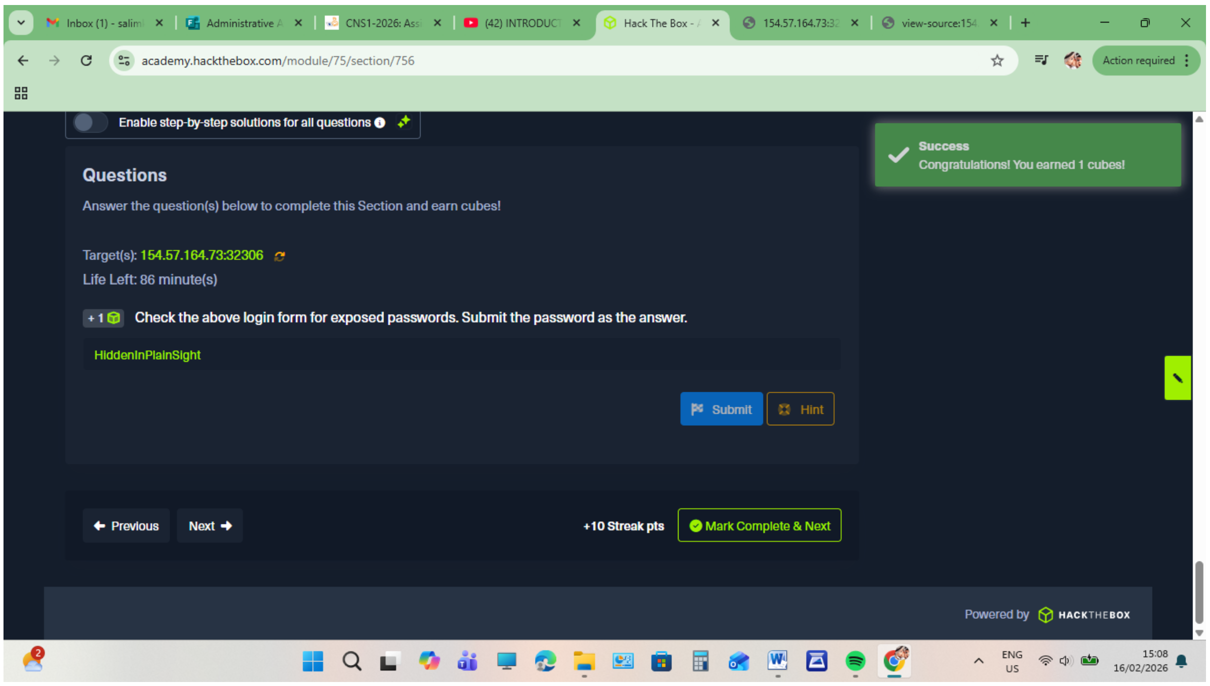
While analysing the front end, I looked for common security weaknesses

Sensitive Data Exposure

I checked the HTML source code for comments/ hardcoded credentials that should not be visible to users



```
        border-radius: 10px;
        color: white;
    }

    button {
        background-color: #2A86FF;
        color: white;
        padding: 14px 20px;
        margin: 8px 0;
        border: none;
        cursor: pointer;
        width: 100%;
        border-radius: 10px;
    }

    button:hover {
        opacity: 0.8;
    }

    .container {
        padding: 16px;
    }
</style>
<form action="#" method="post">

    <div class="container">
        <label for="uname"><b>Username</b></label>
        <input type="text" required>

        <label for="psw"><b>Password</b></label>
        <input type="password" required>

        <!-- TODO: remove test credentials admin:HiddenInPlainSight -->

        <button type="submit">Login</button>
    </div>
</form>

</html>
```



Enable step-by-step solutions for all questions

Questions

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

Target(s): 154.57.164.73:32306

Life Left: 86 minute(s)

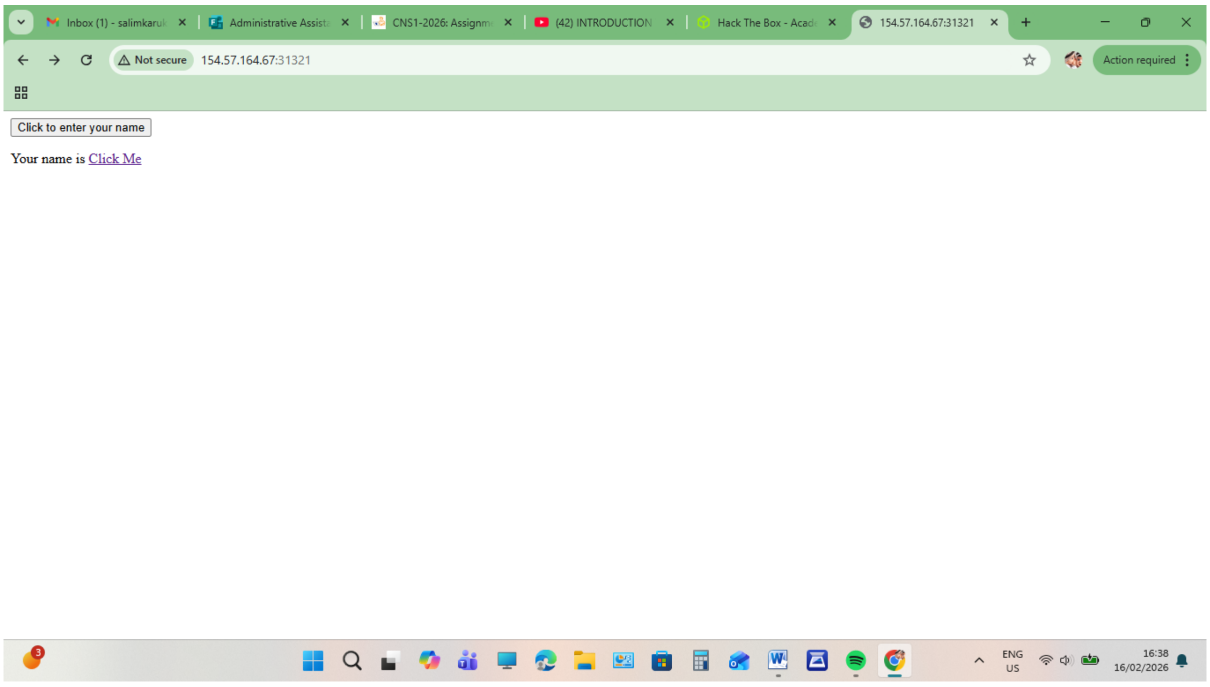
+1 Check the above login form for exposed passwords. Submit the password as the answer.

HiddenInPlainSight

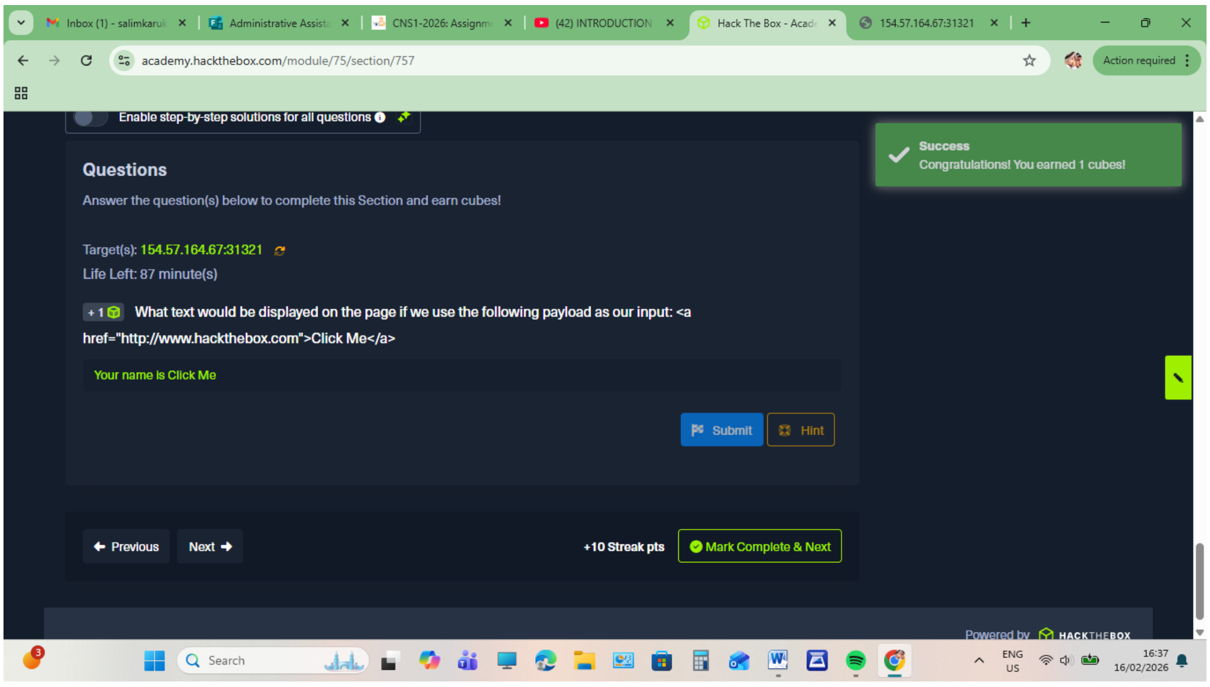
Success
Congratulations! You earned 1 cubes!

HTML Injection

I tested if the application correctly sanitizes user input or if it allows the injection of malicious HTML tags.


Click to enter your name

Your name is Click Me


Enable step-by-step solutions for all questions

Questions

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

Target(s): 154.57.164.67:31321

Life Left: 87 minute(s)

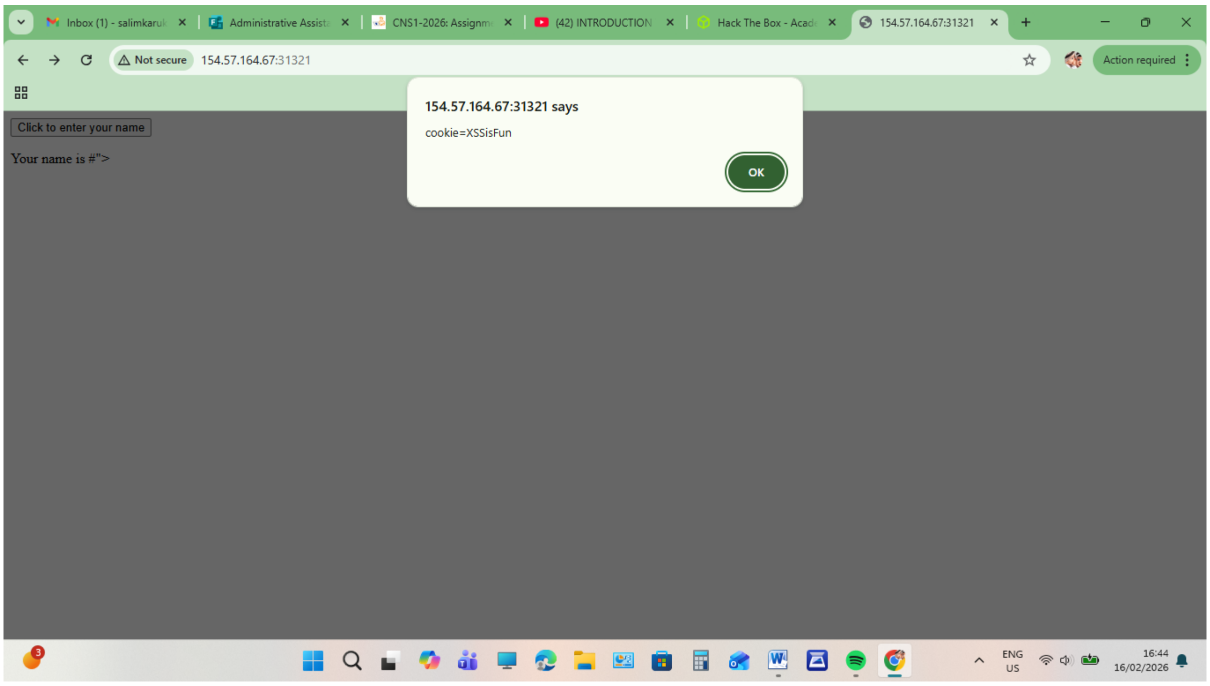
+1 What text would be displayed on the page if we use the following payload as our input: <a href="http://www.hackthebox.com">Click Me</a>

Your name is Click Me

Success
Congratulations! You earned 1 cubes!

Cross- Site Scripting (XSS)

I investigated if the JavaScript could be manipulated to execute unauthorized scripts in the user’s browser.



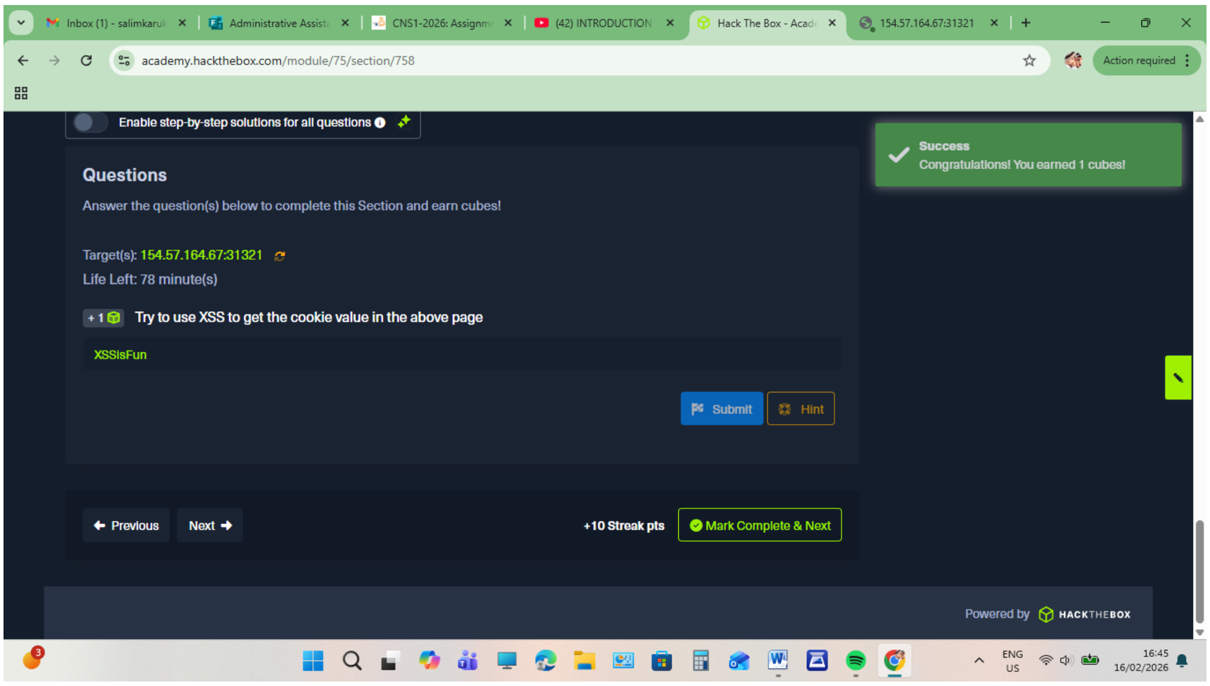
Not secure 154.57.164.67:31321

Click to enter your name

Your name is #">

154.57.164.67:31321 says

cookie=XSSisFun



academy.hackthebox.com/module/75/section/758

Enable step-by-step solutions for all questions

Questions

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

Target(s): 154.57.164.67:31321

Life Left: 78 minute(s)

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

XSSisFun

Success

Congratulations! You earned 1 cubes!

Cross-Site Request Forgery (CSRF)

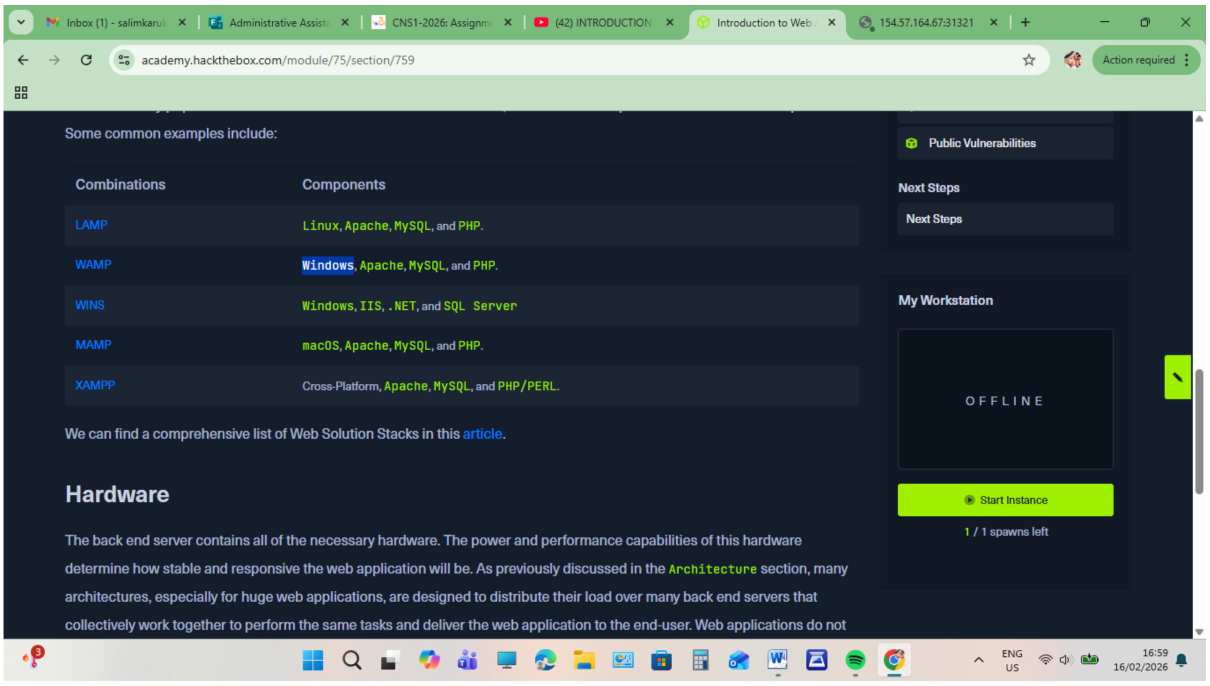
I analyse how the application handles user sessions and whether it protects against unauthorized command sent from a different site.

Back End Components

After the front-end analysis, I shifted my focus to the server-side architecture that powers the application.

Back End Servers

I identified the underlying server environment that processes the logic of the HTB target application



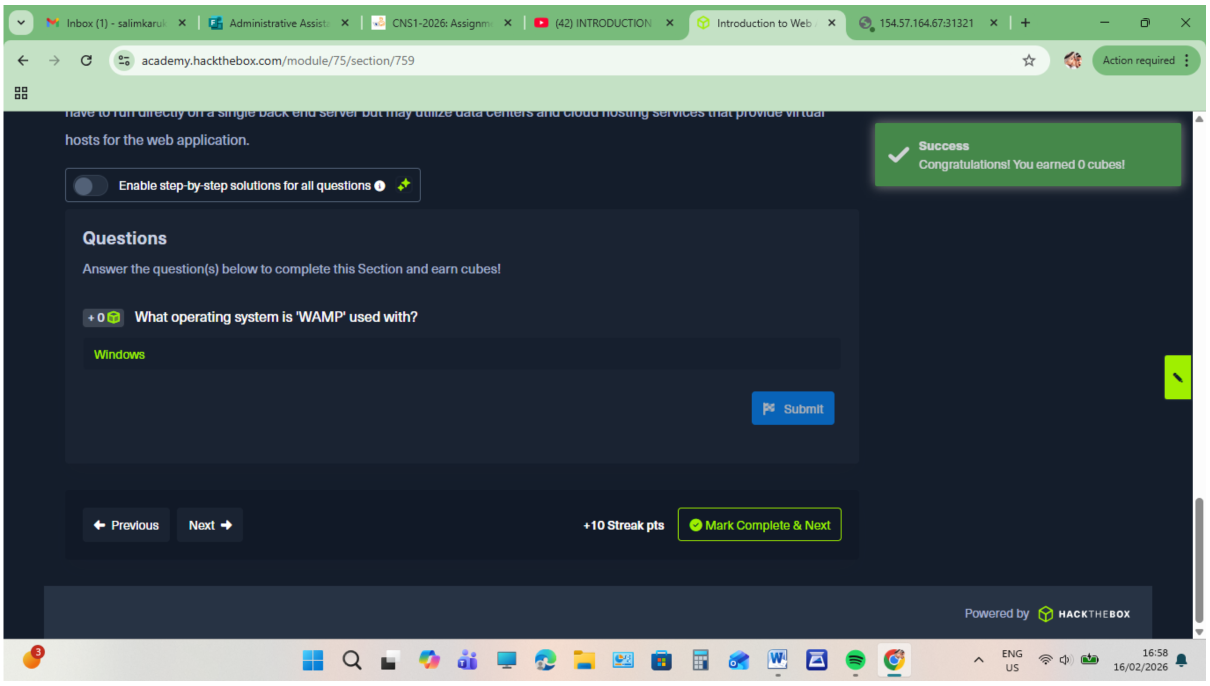
Some common examples include:

Combinations	Components
LAMP	Linux, Apache, MySQL, and PHP.
WAMP	Windows, Apache, MySQL, and PHP.
WINS	Windows, IIS, .NET, and SQL Server
MAMP	macOS, Apache, MySQL, and PHP.
XAMPP	Cross-Platform, Apache, MySQL, and PHP/PERL.

We can find a comprehensive list of Web Solution Stacks in this article.

Hardware

The back end server contains all of the necessary hardware. The power and performance capabilities of this hardware determine how stable and responsive the web application will be. As previously discussed in the Architecture section, many architectures, especially for huge web applications, are designed to distribute their load over many back end servers that collectively work together to perform the same tasks and deliver the web application to the end-user. Web applications do not



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!

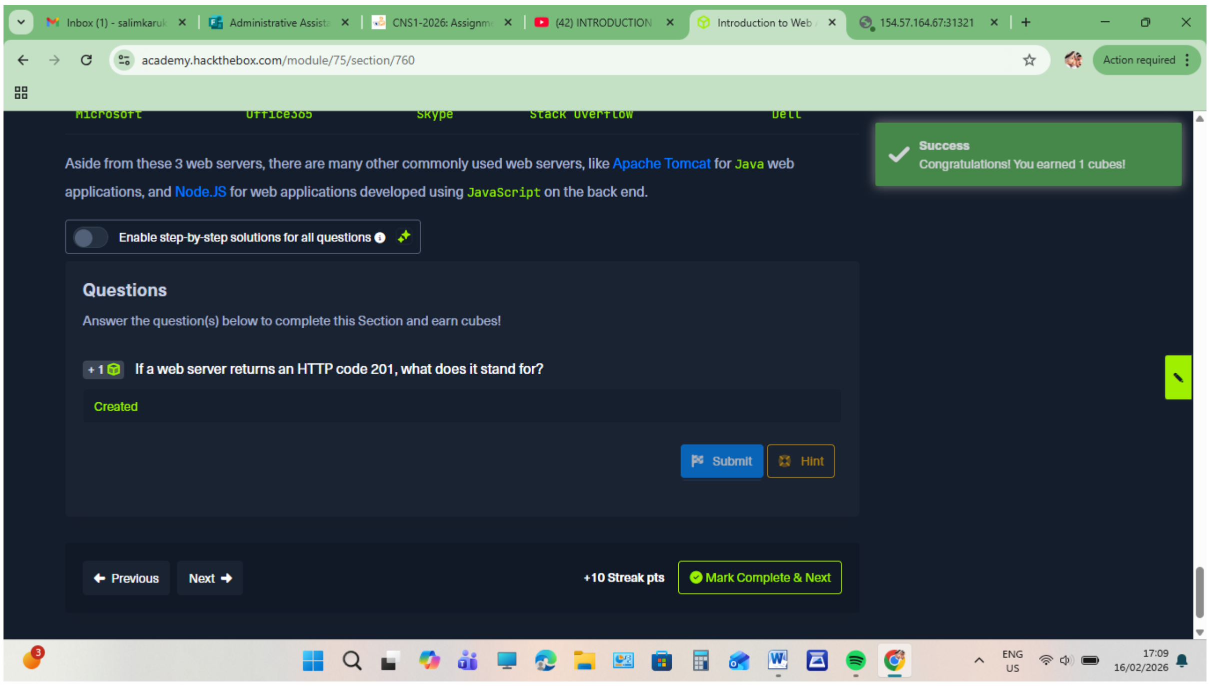
+0 What operating system is 'WAMP' used with?

Windows

Success
Congratulations! You earned 0 cubes!

Web Servers

I analysed the HTTP response headers to identify the type of web server being used (e.g. Apache or Nginx)



Microsoft Office365 Skype Stack Overflow Dell

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.

Enable step-by-step solutions for all questions

Success
Congratulations! You earned 1 cubes!

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?

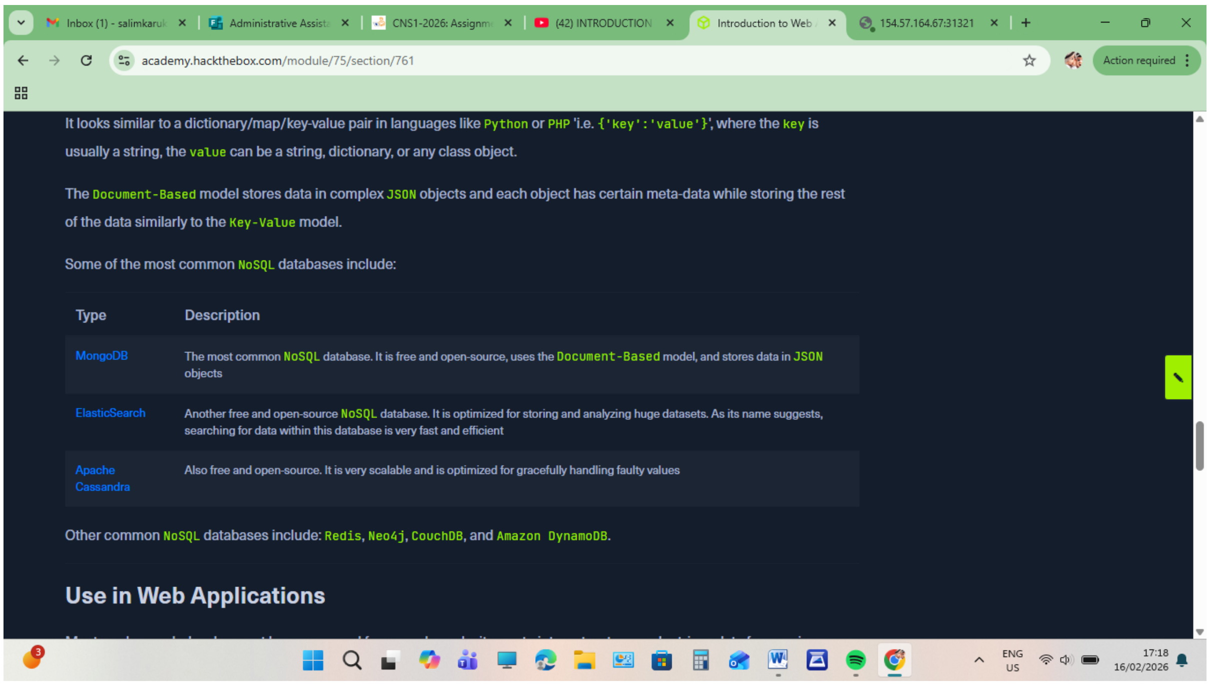
Created

Submit Hint

Previous Next +10 Streak pts Mark Complete & Next

Databases

I studied how the application stores and retrieves information, which is the core of any dynamic web service



It looks similar to a dictionary/map/key-value pair in languages like Python or PHP 'i.e. {'key':'value'}', where the key is usually a string, the value can be a string, dictionary, or any class object.

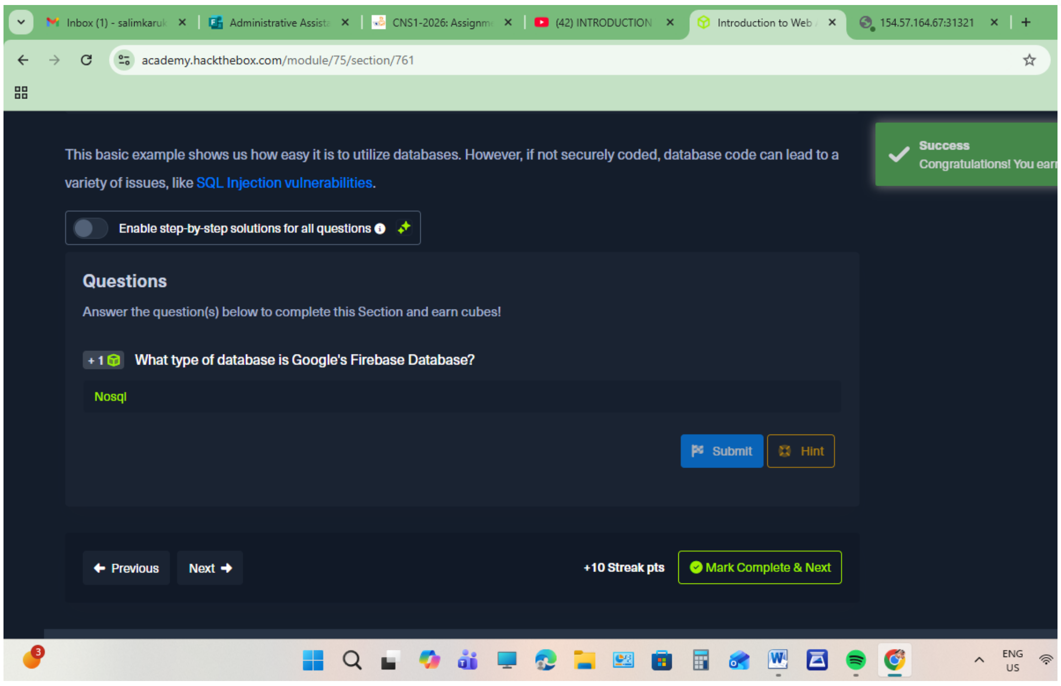
The Document-Based model stores data in complex JSON objects and each object has certain meta-data while storing the rest of the data similarly to the Key-Value model.

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.

Use in Web Applications


This basic example shows us how easy it is to utilize databases. However, if not securely coded, database code can lead to a variety of issues, like SQL Injection vulnerabilities.

Enable step-by-step solutions for all questions

Success
Congratulations! You earn

Questions

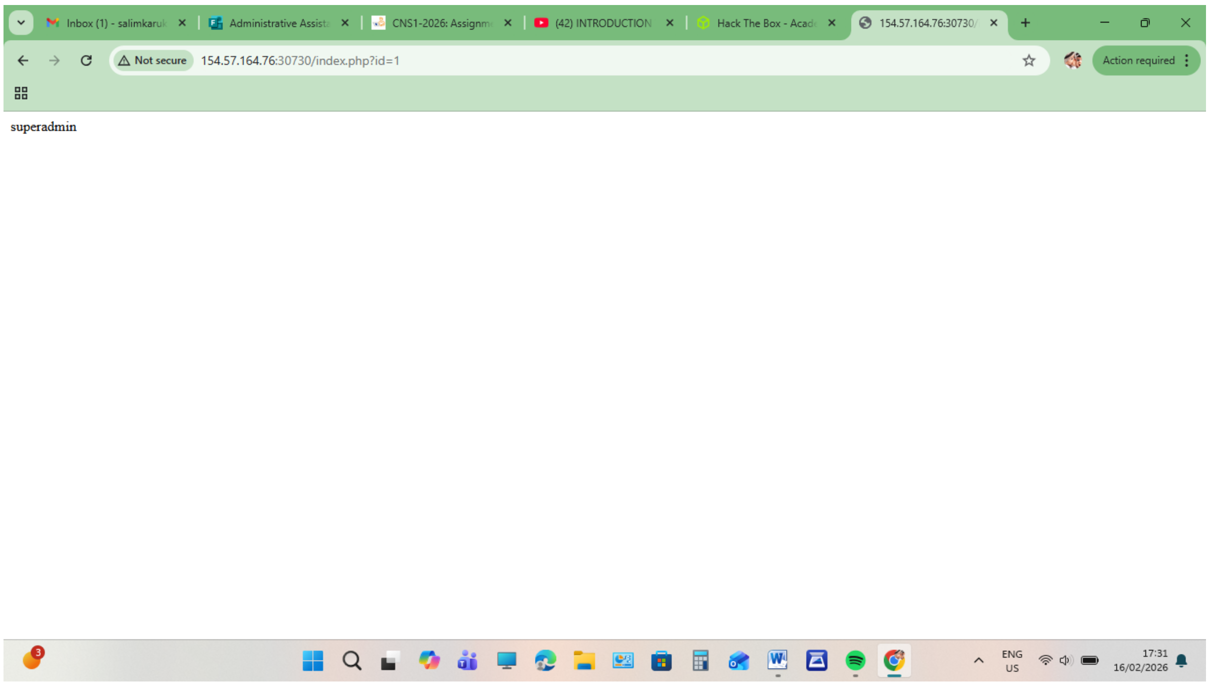
Answer the question(s) below to complete this Section and earn cubes!

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

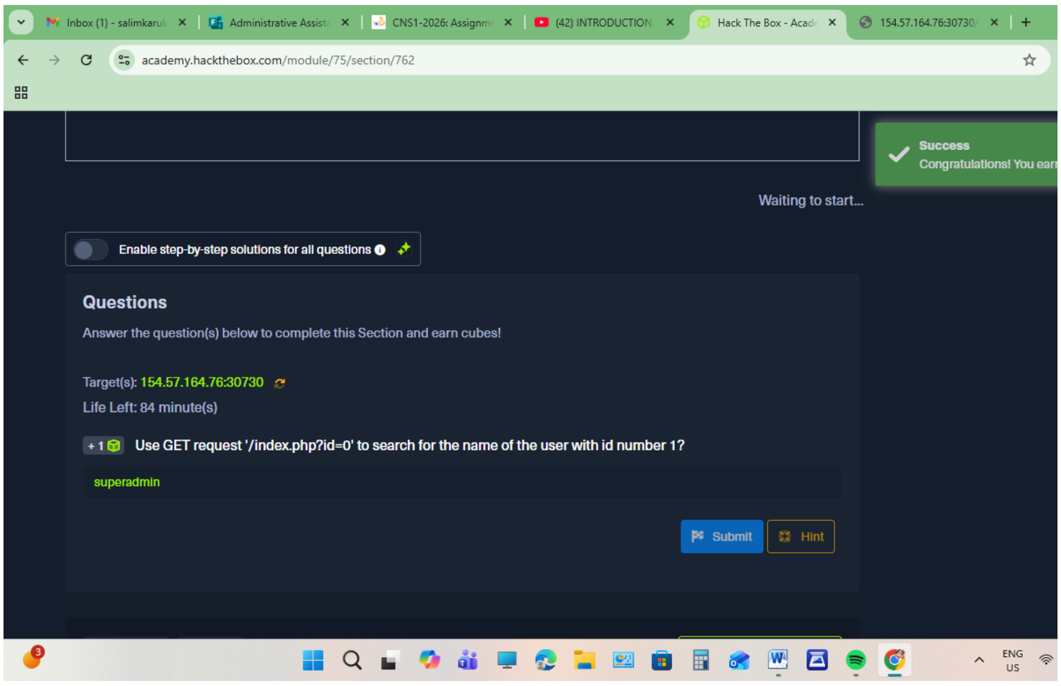
Nosql

Development Frameworks & APIs

I looked for signs of specific frameworks like (Express or Django) and observed how APIs are used to transfer data between the front end and the back end.



superadmin



Questions

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

Target(s): 154.57.164.76:30730

Life Left: 84 minute(s)

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

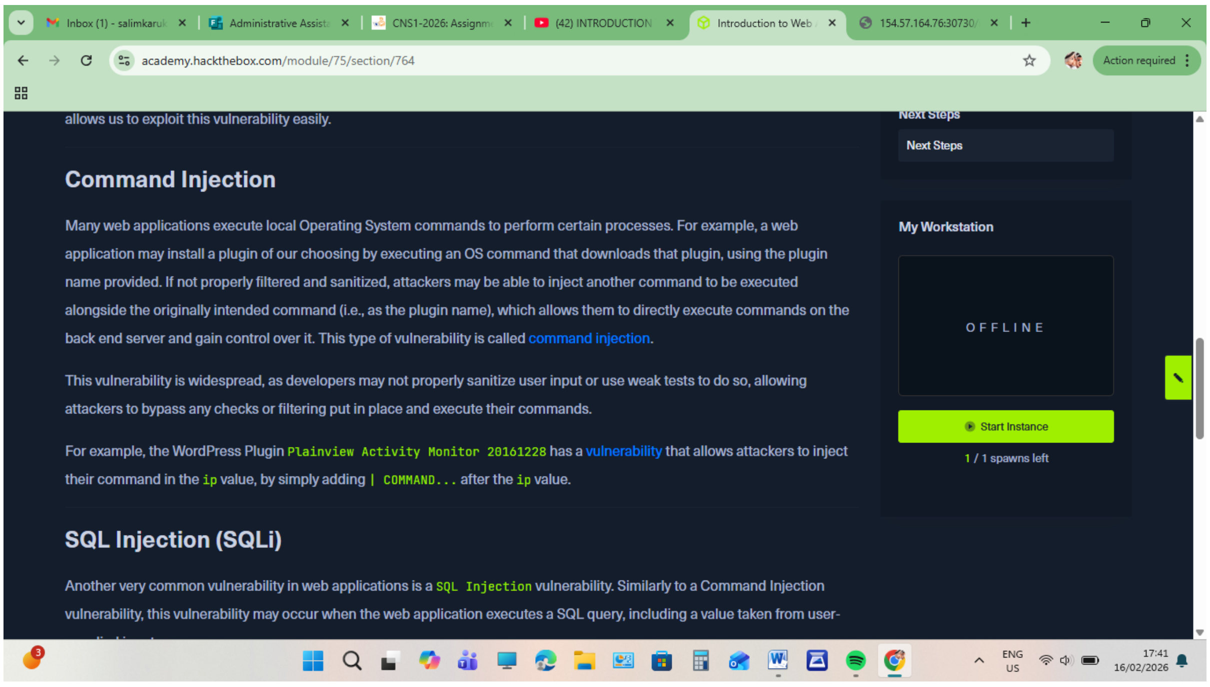
superadmin

Back End Vulnerabilities

I concluded my work by reviewing potential server-side risks.

Common Web Vulnerabilities

I looked for misconfigurations in the server settings that could lead to unauthorized access



allows us to exploit this vulnerability easily.

Command Injection

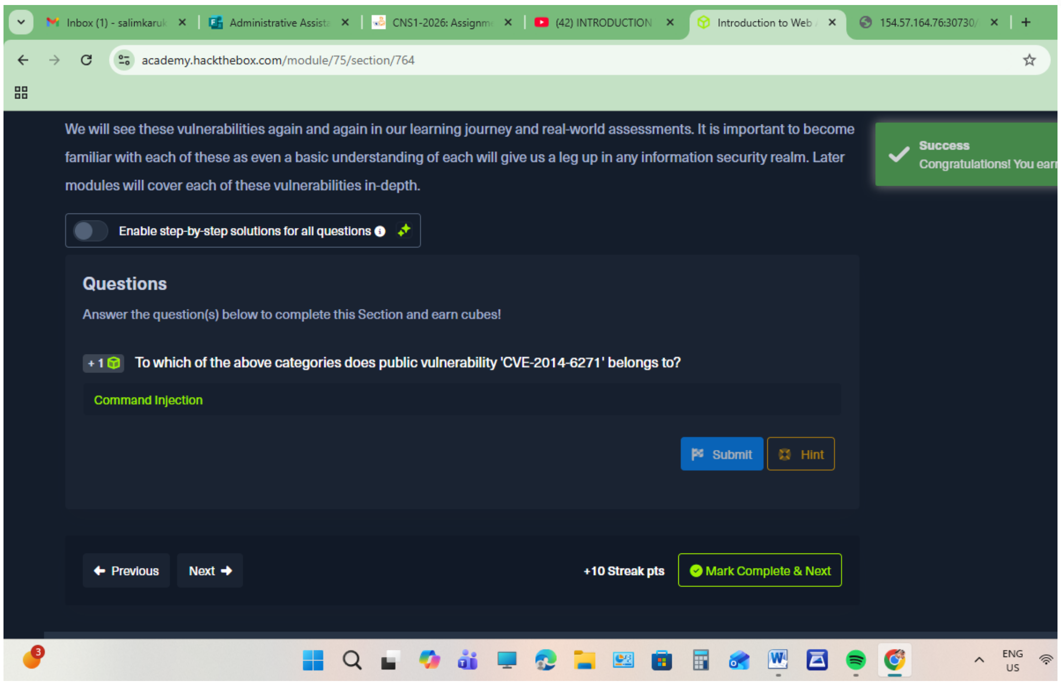
Many web applications execute local Operating System commands to perform certain processes. For example, a web application may install a plugin of our choosing by executing an OS command that downloads that plugin, using the plugin name provided. If not properly filtered and sanitized, attackers may 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.

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.

For example, 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.

SQL Injection (SQLi)

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 taken from user-


We will see these vulnerabilities again and again in our learning journey and real-world assessments. It is important to become familiar with each of these as even a basic understanding of each will give us a leg up in any information security realm. Later modules will cover each of these vulnerabilities in-depth.

Enable step-by-step solutions for all questions

Questions

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

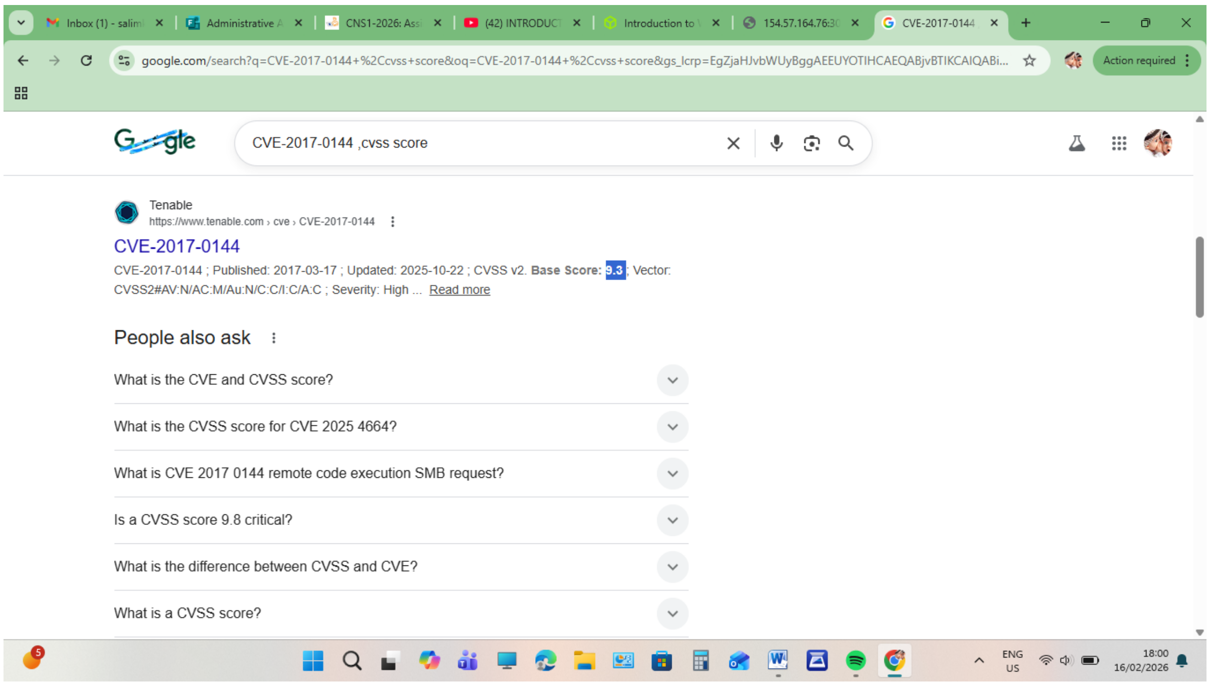
+1 To which of the above categories does public vulnerability 'CVE-2014-6271' belongs to?

Command Injection

Success
Congratulations! You earn

Public Vulnerabilities

I cross referenced the identified server versions with known public vulnerability database (CVEs) to see if the target was running outdated or unpatched software


google.com/search?q=CVE-2017-0144+%2Ccvss+score&oq=CVE-2017-0144+%2Ccvss+score&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIHCAEQABjvBTIKCAIQABi...

CVE-2017-0144 ,cvss score

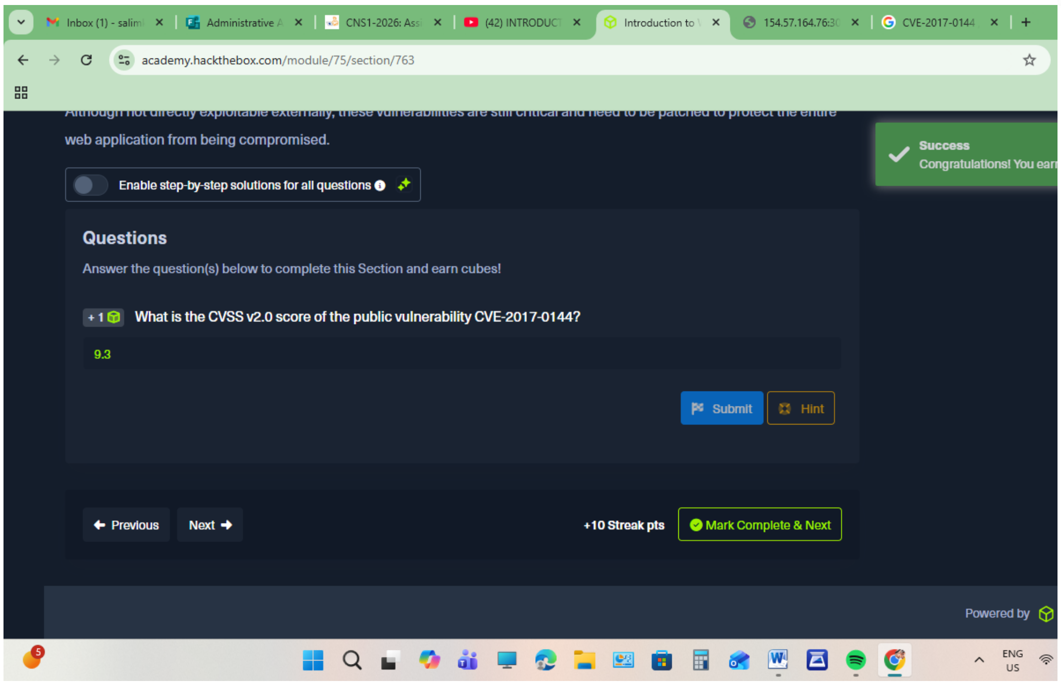
Tenable
https://www.tenable.com › cve › CVE-2017-0144

CVE-2017-0144

CVE-2017-0144 ; Published: 2017-03-17 ; Updated: 2025-10-22 ; CVSS v2. **Base Score:** 9.3 ; Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C ; Severity: High ... Read more

People also ask

- What is the CVE and CVSS score?
- What is the CVSS score for CVE 2025 4664?
- What is CVE 2017 0144 remote code execution SMB request?
- Is a CVSS score 9.8 critical?
- What is the difference between CVSS and CVE?
- What is a CVSS score?


Inbox (1) - salim | Administrative A | CNS1-2026: Ass | (42) INTRODUCT | Introduction to | 154.57.164.76:3 | CVE-2017-0144

academy.hackthebox.com/module/75/section/763

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

Success
Congratulations! You earn

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

Powered by

ENG US

Here is the link to view he module which in have completed

- ➢ https://academy.hackthebox.com/achievement/2402182/75

Conclusion

In conclusion the completion of this assignment on web Application Fundamental marks a critical step in understanding the security landscape of modern web services. By exploring the Request- Response model and the architecture of both Front-end and back-end system, it is clear that even minor misconfigurations in a web application can lead to significant security risks. Ultimately, this module demonstrates that a deep understanding of how a web application functions is the essential prerequisite for securing it. The skills gained here through the Hack the Box Academy curriculum provide a solid foundation for more advanced vulnerability research and penetration testing.