WEB APPLICATION FUNDAMENTALS

ASSIGNMENT REPORT

Peter Kinyumu,
cs-sa07-24067,
May 11th, 2024.

1. INTRODUCTION

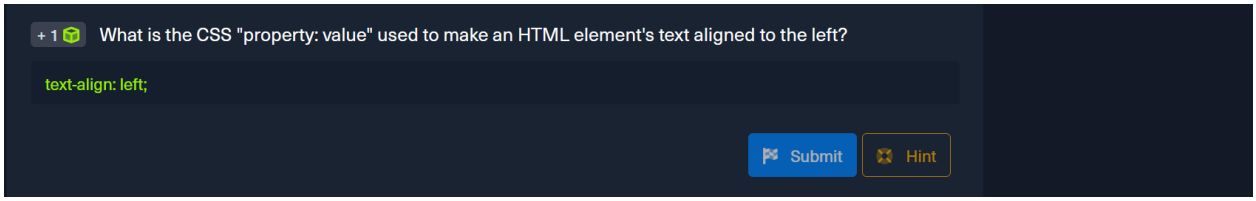
This report documents my completion of the **Introduction to Web Applications** Module on the HacktheBox platform. The module covered an introduction to web applications, explaining how the web works, its components and infrastructures, and its security risks and vulnerabilities. As security analysts, understanding web applications and their environment is essential to ensure the risks they pose and how their vulnerabilities can be prevented.

2. ANSWERS TO QUESTIONS

Front End Components(HTML, CSS)

a. What is the HTML tag used to show an image?

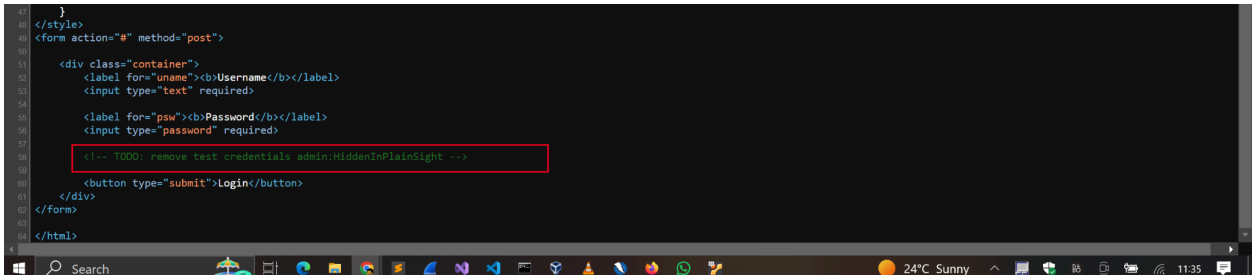
b. What is the CSS "property: value" used to make an HTML element's text aligned to the left?



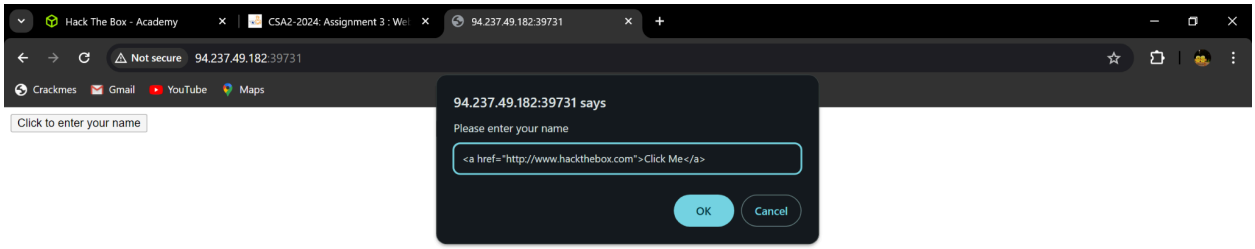
Front End Vulnerabilities

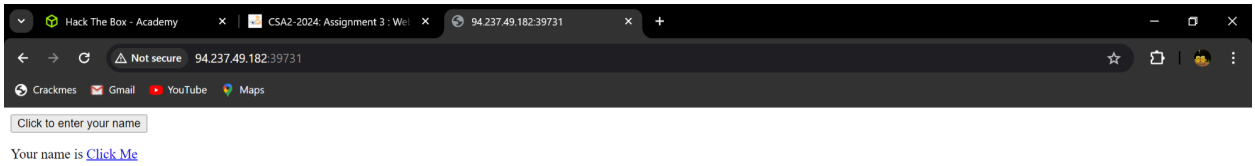
a. Check the above login form for exposed passwords. Submit the password as the answer.

The exposed credentials could be viewed from the page source code.

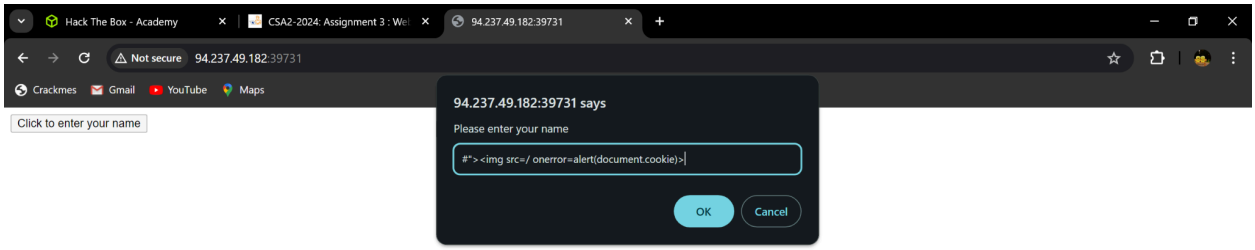


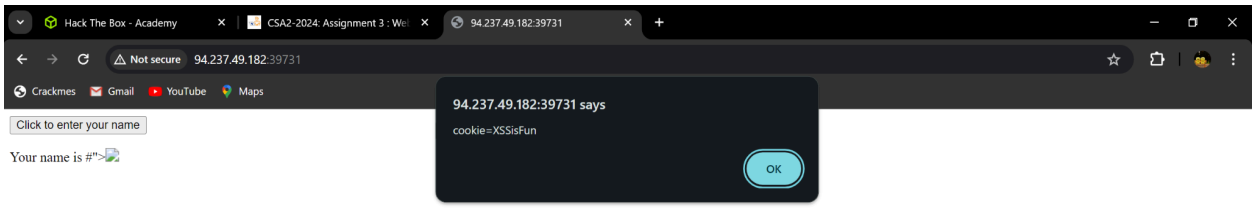
b. What text would be displayed on the page if we use the following payload as our input: Click Me





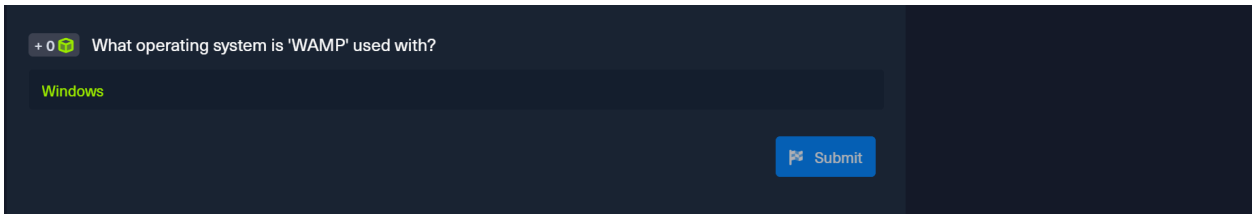
c. Try to use XSS to get the cookie value in the above page





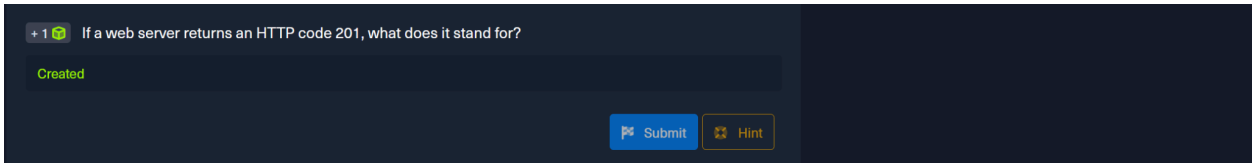
Backend Components

a. What operating system is 'WAMP' used with?

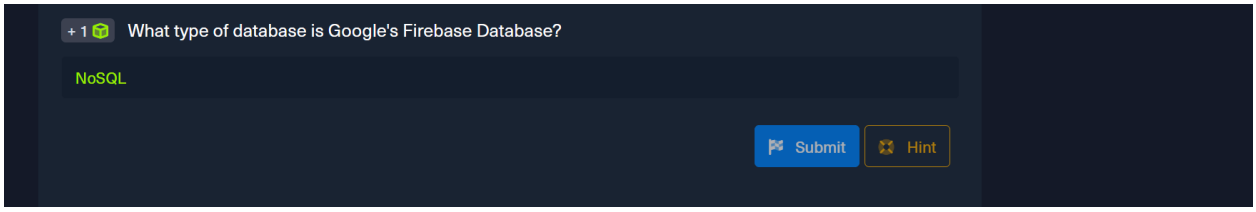


b. If a web server returns an HTTP code 201, what does it stand for?

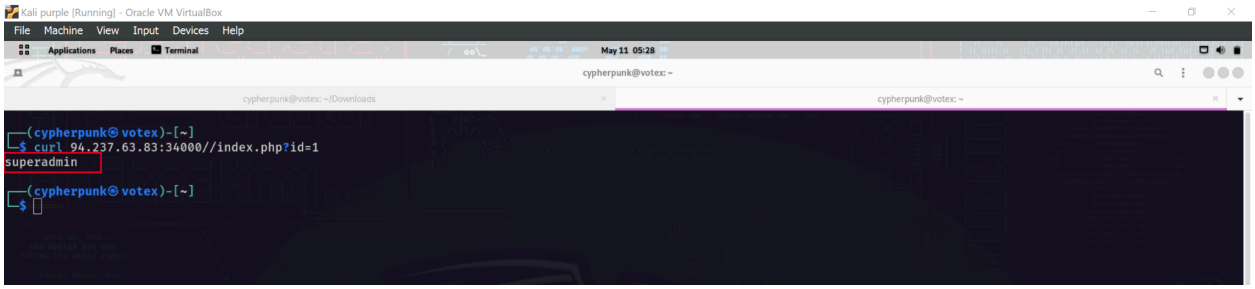
'The HTTP 201 Created success status response code indicates that the request has succeeded and has led to the creation of a resource.' - Mozzila documentation.



c. What type of database is Google's Firebase Database?



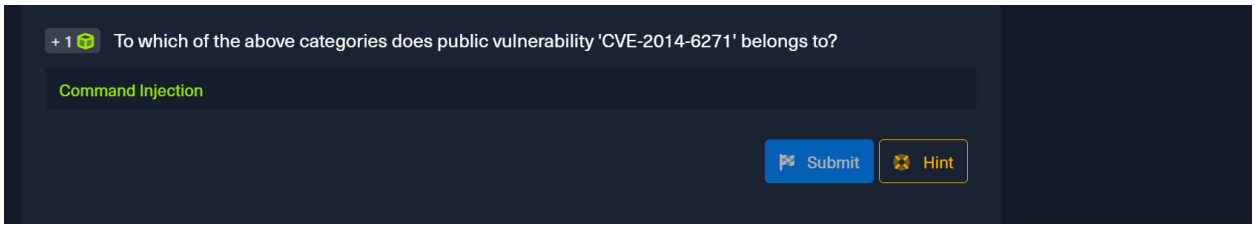
d. Use GET request '/index.php?id=0' to search for the name of the user with id number 1?



Backend Vulnerabilities

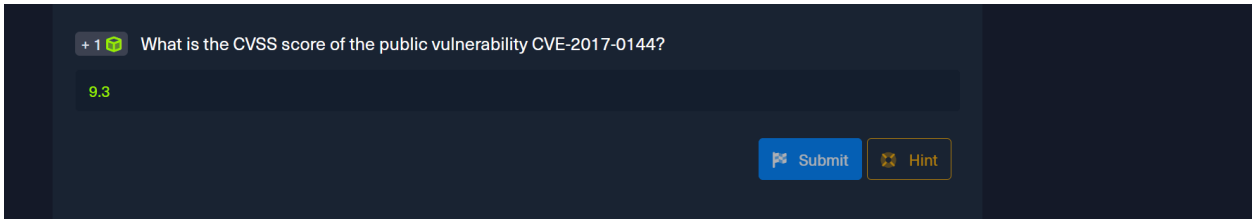
a. To which of the above categories does public vulnerability 'CVE-2014-6271' belongs to?

The CVE-2014-6271 is the ShellShock - Linux Bash vulnerability. The vulnerability could be exploited by an attacker to execute arbitrary commands invoking the Bash shell. This makes it a Command Injection vulnerability.



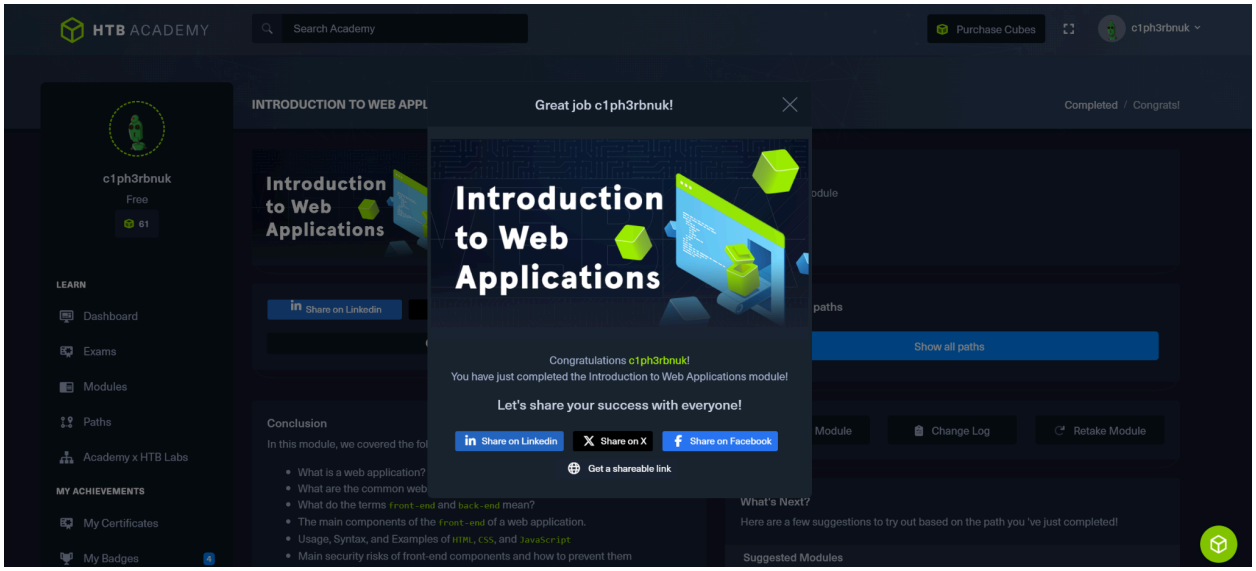
b. What is the CVSS score of the public vulnerability CVE-2017-0144?

CVE-2017-0144 is known as the Windows SMB Remote Code Execution Vulnerability in Microsoft Server Message Block 1.0 (SMBv1). It is a critical vulnerability, and a successful exploit could allow code to be executed on the target server.



3. MODULE COMPLETION

The following is a sharable link to the badge I earned after completing the module.
https://academy.hackthebox.com/achievement/144829/75



4. CONCLUSION

This module has truly been enlightening. It was exhilarating to understand how the web works, the different components it encompasses, and the security risks associated with it as a whole. I also learnt that web applications could be a potential attack surface for attackers to gain access to a system. Vulnerabilities like Cross-site scripting, Cross-site request forgery and SQL injection must be prevented by never trusting the user input through input validations and sanitizations.

I look forward to exploring more about how to identify these vulnerabilities, exploiting and mitigating them as a security analyst later in the course chapters.