Lab name: [Stored XSS into HTML context with nothing encoded](https://portswigger.net/web-security/cross-site-scripting/stored/lab-html-context-nothing-encoded)

Severity: Critical

Lab description:

* This lab has vulnerability in the application’s comment box, where the application simply stores the input in the paragraph tag <p>
* Aim is to exploit and analyze this vulnerability.

Impact:

* This vulnerability can lead to account hijacking, credential theft
* Attackers can manipulate users to redirect to some other page through which they can collect personal information.
* The application might not be safe enough for users to use, because confidentiality and integrity are affected.

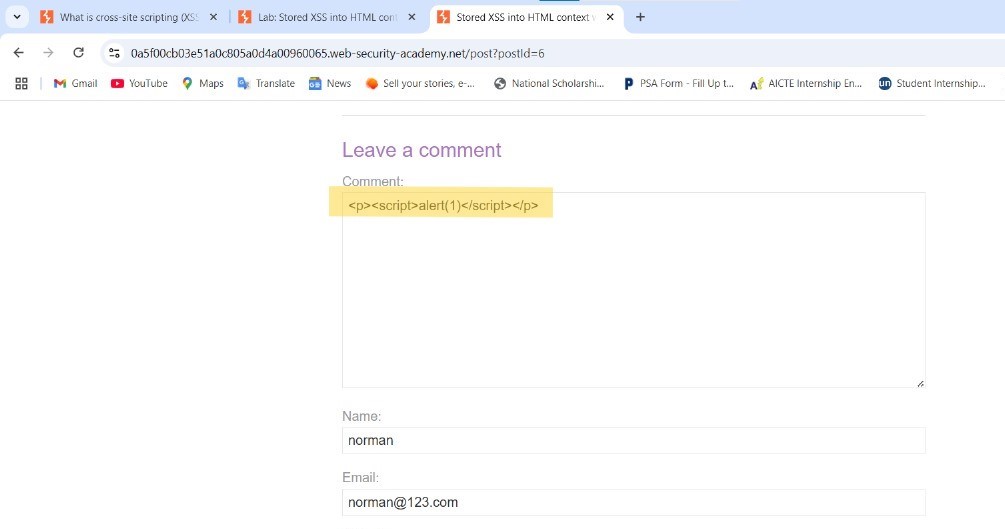
Recommendations:

* Sanitize and encode all user inputs before rendering them in the HTML context.
* Use security libraries or frameworks that auto-escape user input.
* Implement Content Security Policy (CSP) to reduce XSS impact.
* Regularly scan for XSS vulnerabilities using automated tools.

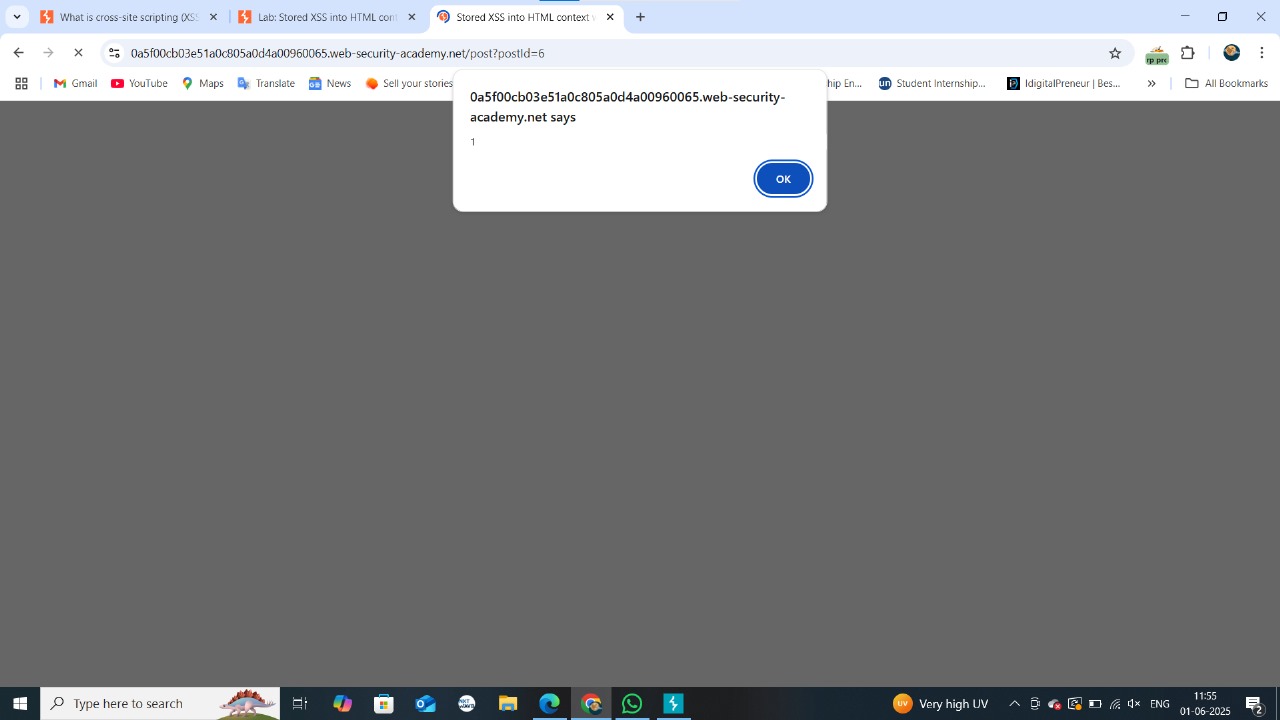
Steps to reproduce:

* Access the lab and Navigate to the product page with the comment form.
* Enter the following in the comment field:

<script> alert (1) </script>



* Submit the comment.
* After submission, the comment is stored and rendered on the product page.



* When the page reloads, the JavaScript executes, showing an alert box.