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

Severity: Medium

Lab description:

* This application reflects the user input without any sanitization of the input which leads to XSS attack, where the attacker can simply inject a malicious java script code into the application and hijack the application.

Impact:

* This attack can lead to hijacking of sessions or session tokens; this eventually affects the confidentiality.
* This can lead to other attacks.
* Users can be manipulated to reveal their personal information.
* Users can be convinced that they have entered some other website.

Recommendations:

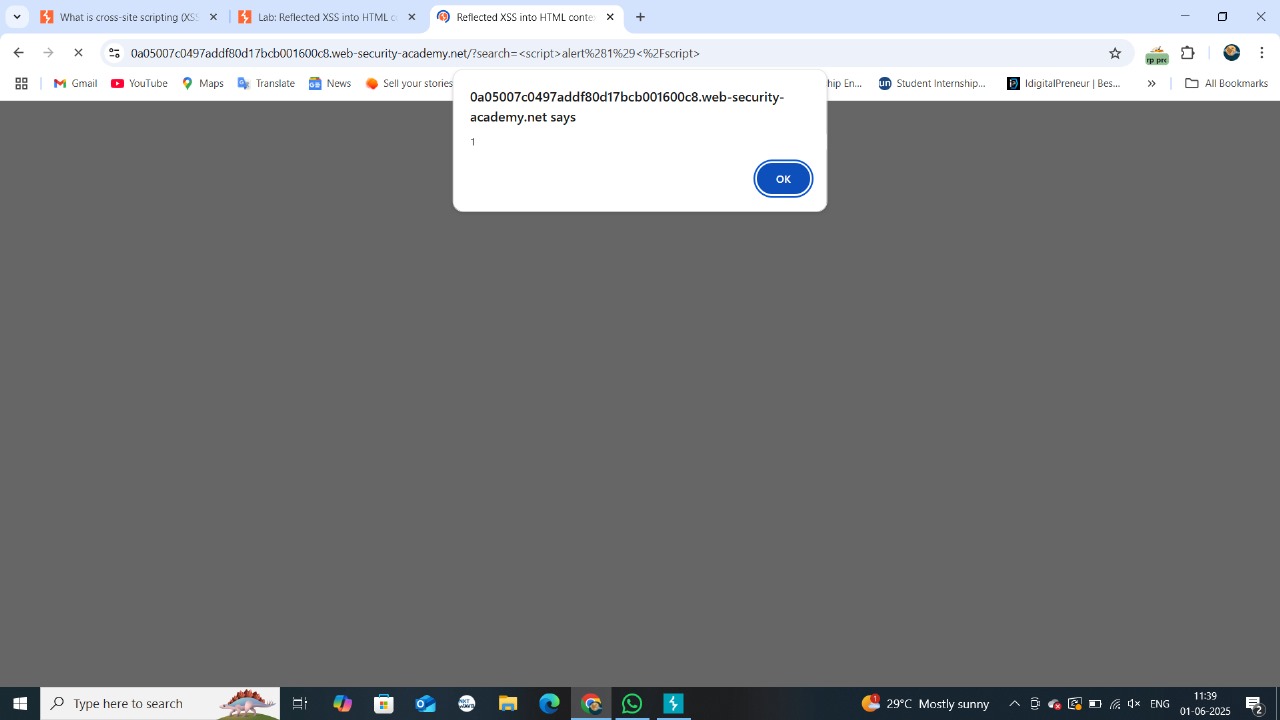
* Sanitize the input before accepting the request. Sanitizing includes removing special characters, removing spaces.
* Allowing only certain characters in the input field will avoid XSS kind of situation
* Use HTML encoding for data placed in HTML bodies likewise for Java script bodies.
* Don't reflect user input directly without sanitizing it.

Steps to reproduce:

* In the search box, type a java script code,

*<script>alert(1) </script>*



* It is because the search box takes input and reflects it as heading in the output page, so XSS is possible.
* The alert pop-up has been raised.
* Through these attackers can insert any kind of scripts.