REPORT (TASK 2)

DESCRIPTION:

Title: Cross-Site scripting(xss) Vulnerability (found in the critical vulnerability of Out-of-date Version (Apache)).

Domain name: https://zero.webappsecurity.com/

Vulnerability found: CRITICAL.

Steps to reproduce the vulnerability:

1.Open netsparker and then copy the website link.

2.Paste the website URL in s dialogue box.

3.Define all the customise options for scanning.

4.Then the netsparker shows the vulnerabilities of different type such as critical, important, medium, low, information.

The present vulnerability is shown by netsparker in the critical type of out-date-version of Apache.

Impact of this vulnerability:

1. Xss leads to stealing user accounts by stealing their(users) sessions cookies.
2. Credential threat and data leakage are the issues related to xss.

This can be done by injecting malicious web script in the URL or other parameters.

Mitigation:

To reduce the risk developers should encode all fields when displaying them in the browser. User fields needed to be verified with proper special characters. And always update the old versions to reduce such vulnerabilities.

Conclusion:

Xss is attack needed to be monitored and resolved to protect user information and to keep up their belief.