St. Francis Institute of Technology
(An Autonomous Institution)
AICTE Approved | Affiliated to University of Mumbai

A+ Grade by NAAC: CMPN, EXTC, INFT NBA Accredited: ISO 9001:2015 Certified

Department of Information Technology

A.Y. 2025-2026
Class: BE-IT A/B, Semester: VII
Subject: Secure Application Development Lab

Student Name: **Durva Kadam** Student Roll No: **23**

Experiment – 7: Cross-Site Scripting (XSS) Vulnerability

Aim: To Study Cross-Site Scripting (XSS) Vulnerability

Objectives: Aim of this experiment is that the students will be able understand

- To study the different types of Vulnerabilities
- To study Cross-Site Scripting (XSS) Attack.

Lab objective mapped: ITL703.4 To apply Data Validation and Authentication for application

Requirements: Personal Computer, Windows operating system browser, Internet Connection

Pre-Experiment Theory:

Vulnerability:
Vulnerabilities are weaknesses or flaws in a software, system, network, or process that can be exploited by attackers to gain unauthorized access, steal sensitive data, disrupt operations, or cause damage to the system or organization.

Different classes of vulnerability:
Software vulnerabilities - These are vulnerabilities that are present in the code or design of software applications that could be exploited by attackers. Common examples include buffer overflows, SQL injections, cross-site scripting (XSS), and remote code execution vulnerabilities.
Network vulnerabilities - Network vulnerabilities refer to weaknesses in network infrastructure or protocols that can be exploited to gain unauthorized access or disrupt network services. Examples include insecure network protocols, misconfigured firewalls, weak encryption algorithms, and open ports.
Physical vulnerabilities - Physical vulnerabilities involve weaknesses in the physical infrastructure of a system or facility. This could include unauthorized physical access to sensitive areas, insecure storage of backup tapes or devices, or inadequate protection of hardware against theft or tampering.
Human vulnerabilities - People can be a significant source of vulnerabilities in security systems. This includes social engineering attacks, where attackers manipulate individuals to

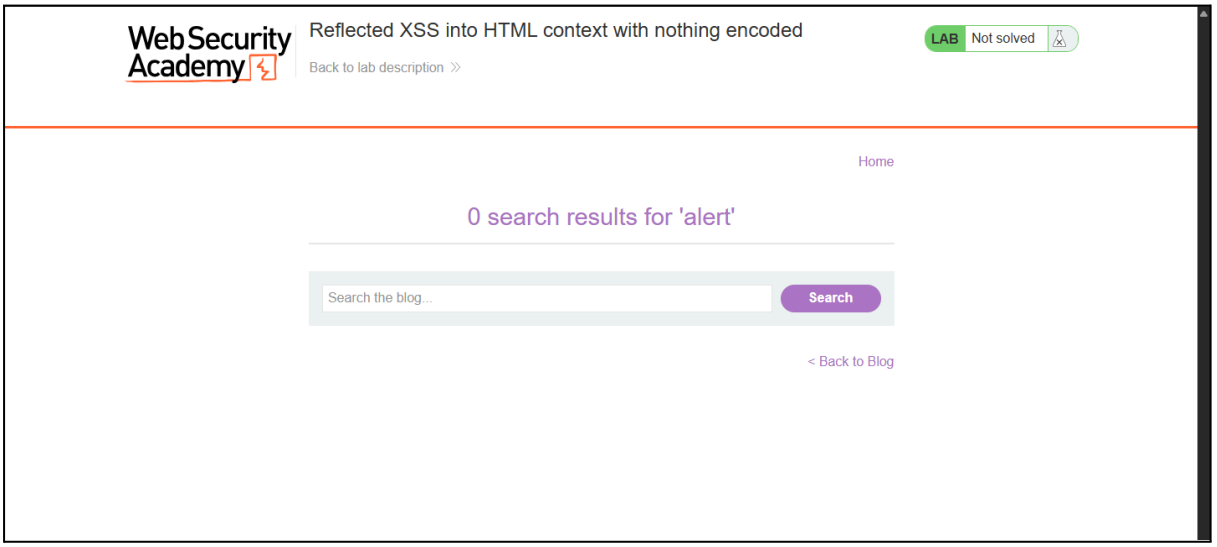
disclose sensitive information or perform actions that compromise security. Phishing, tailgating, and pretexting are examples of social engineering techniques.

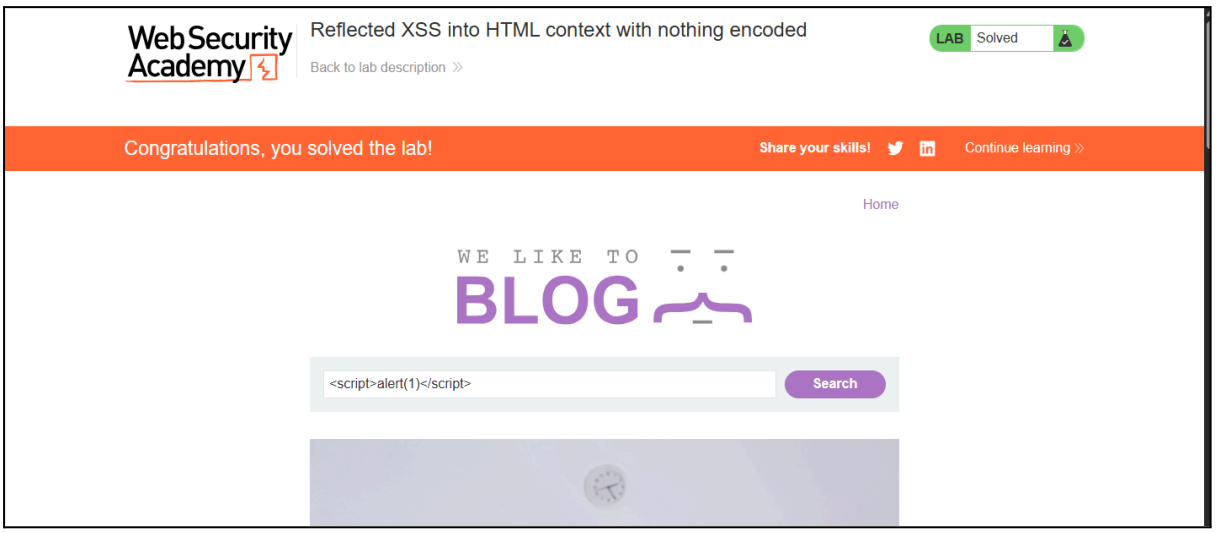
Social engineering vulnerabilities - These are vulnerabilities that arise due to the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information.

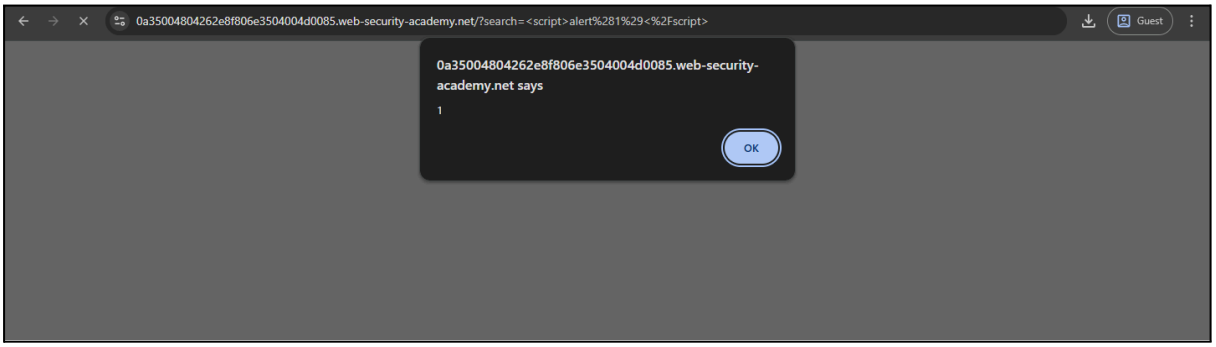
Procedure:

Exercise on Cross site scripting from
https://portswigger.net/web-security/cross-site-scripting#what-is-cross-site-scripting-xss

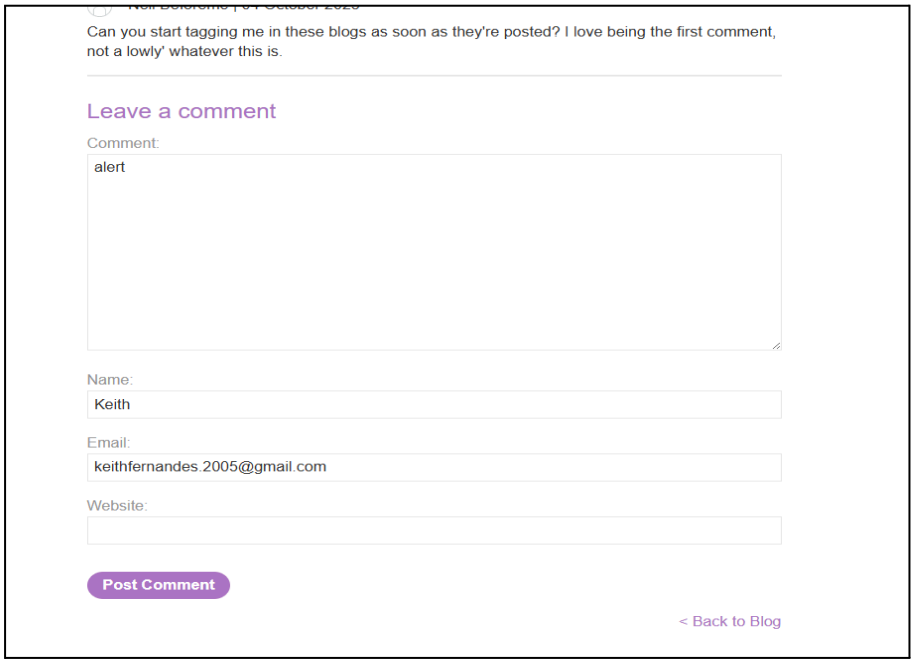
1. **Reflected XSS into HTML context with nothing encoded**

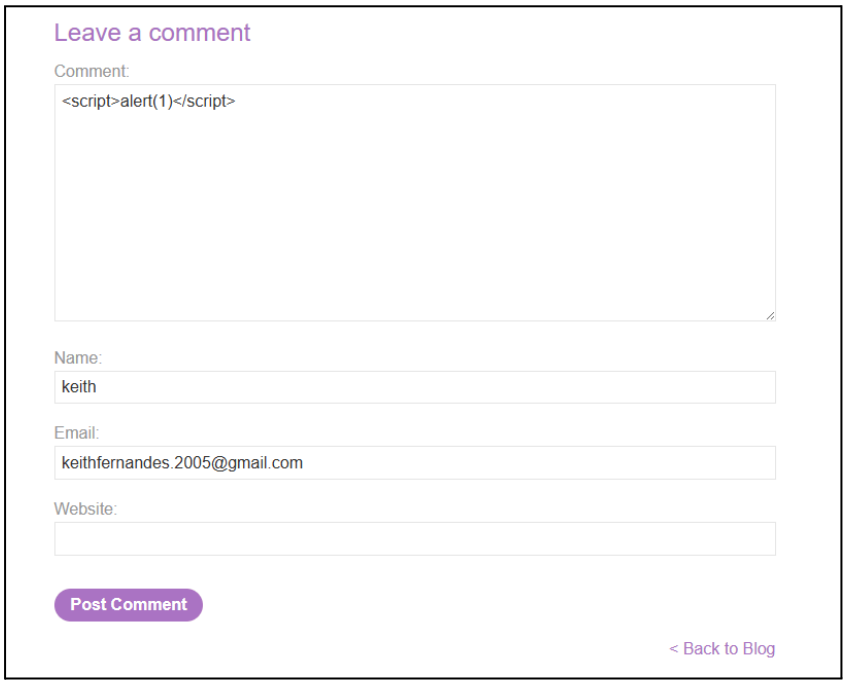


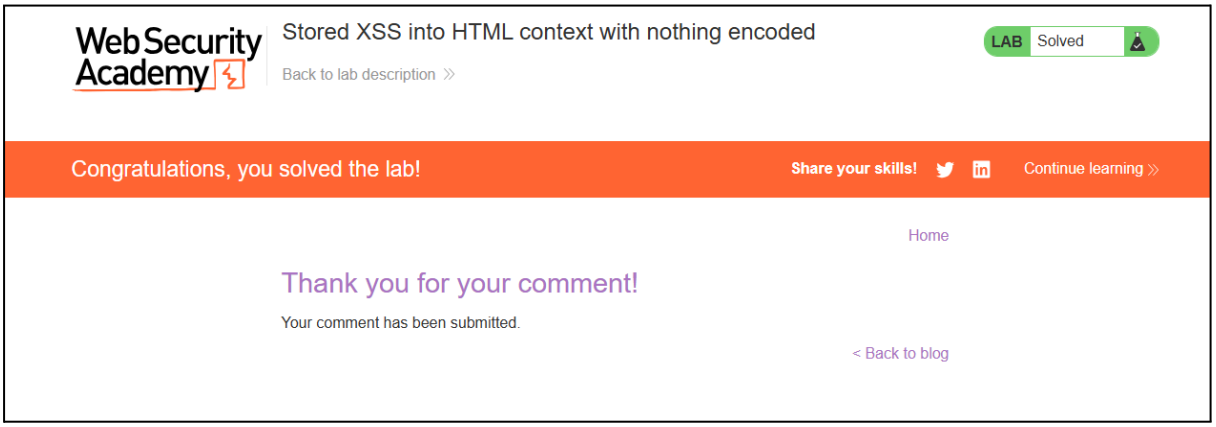




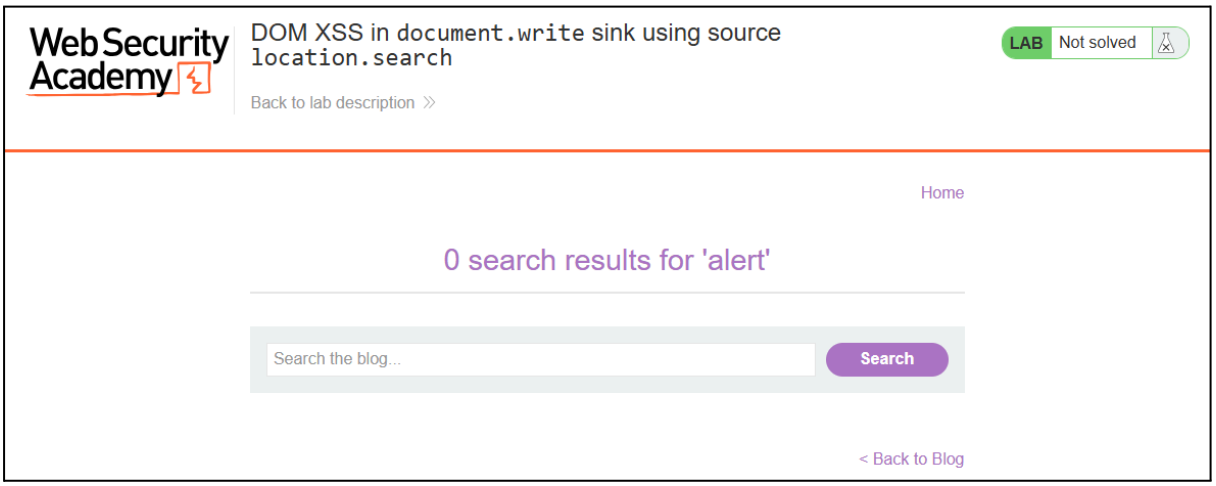
2. Stored XSS into HTML context with nothing encoded

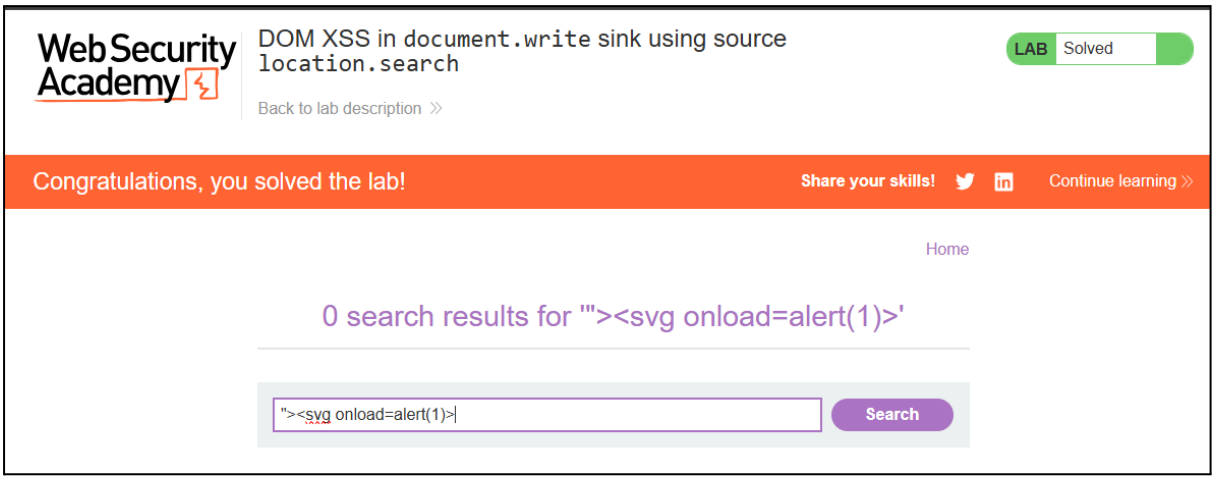






4. DOM XSS in document.write sink using source location.search





Extended Theory: Nil

Post Experimental Exercise:
Questions:

- Define cross site scripting.
- Explain the types of cross-site scripting.
- What steps can developers take to secure their web applications against XSS?
- Discuss the potential impact of a successful XSS attack on a real user.

Conclusion:

- Why is it essential for individuals, organizations, and security professionals to understand and address this type of vulnerability?

References:

1. William Stallings and Lawrie Brown, “Computer Security Principles and Practice”.
2. https://www.geeksforgeeks.org/what-is-cross-site-scripting-xss/
3. https://www.techtarget.com/searchsecurity/definition/cross-site-scripting