Ex. No. 8	Cross Site Scripting (XSS)
Date of Exercise	25/10/23

Aim:

To perform a Cross Site Scripting attack using testfire.net

Lab Environment:

To carry out the Experiment, you need:

- Penetration testing operating system [Kali Linux / parrot]
- Web browser with Internet access
- Administration privileges to run the tools

Description:

Cross Site Scripting Attack:

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.

Site: testfire.net

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects.

Implementation:

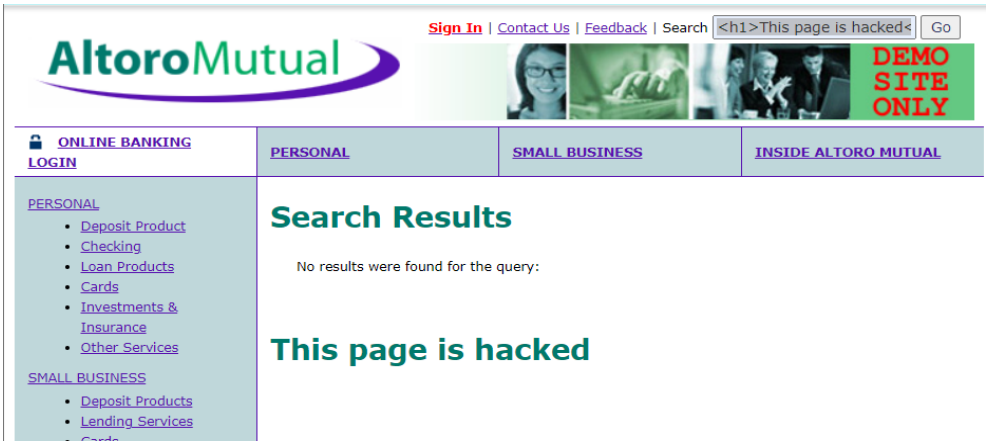
1. Go to the site testfire.net
2. In the search bar type the Cross Site Scripting scripts
3. <h1>This page is hacked</h1> using this script we can display the

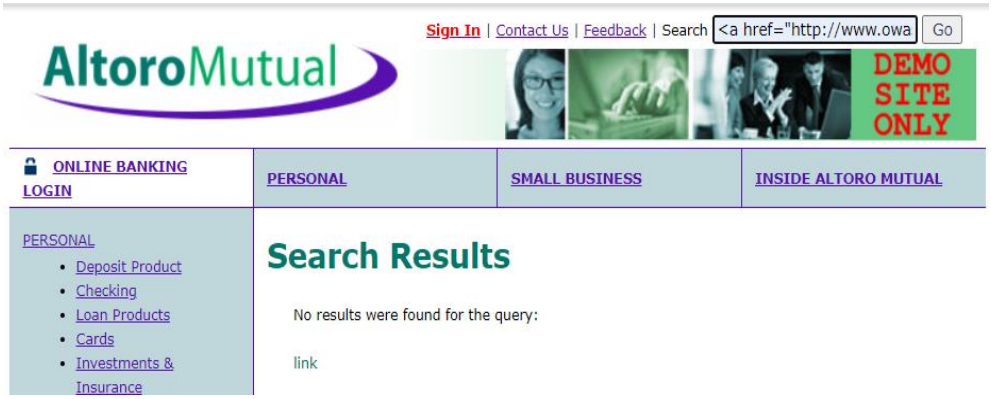
Text on main page.

4. Run other scripts to manipulate the site. For example:

link it will redirect to owasp page when we click on the link present in the main.

Output:





Result:

The Cross Site Scripting attack using site testfire.net was implemented successfully.