

# AI for Cyber Security with IBM Qradar

Name: Prince Levin Panditi

Email: [prince.21bce9648@vitapstudent.ac.in](mailto:prince.21bce9648@vitapstudent.ac.in)

1. Target Website: Let us assume you have a basic web page with a search bar where users can search for products. The search query is displayed on the search results page without proper sanitization. Here I have taken [demo.testfire.net](https://demo.testfire.net)

Vulnerability: We'll test for a reflected XSS vulnerability, where an attacker injects malicious code that is executed in the victim's browser when the search results are displayed.

Steps:

**Go to [demo.testfire.net](https://demo.testfire.net)**

Identify Input Point:

Identify the input point where user data is displayed without proper validation or sanitization. In this case, it is the search query displayed on the search results page.

Test for Vulnerability:

Search for a product using the search bar and enter a payload that triggers an XSS attack. For example, use the following payload:

**Run this code in the search box:**

**<script>alert('XSS')</script>**

If the payload is executed as JavaScript code on the search results page and an alert box pops up, the vulnerability is present.

**Click on GO**

The screenshot shows a web browser at [demo.testfire.net/search.jsp?query=<script>alert\('XSS'\)</script>](https://demo.testfire.net/search.jsp?query=<script>alert('XSS')</script>). The page displays the AltoroMutual logo and a navigation menu. A search bar at the top right contains the payload `<script>alert('XSS')</script>` and a 'Go' button. Below the search bar, a 'demo.testfire.net says XSS' alert box is visible. The search results section shows 'No results were found for the query:'. The footer contains a disclaimer: 'The Altoro 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. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW110>. Copyright © 2008, 2023, IBM Corporation. All rights reserved.'

Fill the feedback form, in the place of the name inject a Javascript code. If the code works then it is vulnerable to Reflected XSS.

The screenshot shows a web browser at `demo.testfire.net/feedback.jsp`. The page has a header with the AltoroMutual logo and navigation links: [Sign In](#), [Contact Us](#), [Feedback](#), and a search bar. Below the header is a sidebar with links for **PERSONAL**, **SMALL BUSINESS**, and **INSIDE ALTORO MUTUAL**. The main content area is titled **Feedback** and contains a form with the following fields:

- To: **Online Banking**
- Your Name: `<script>alert('Prince')</script>`
- Your Email Address: `xyz@gmail.com`
- Subject: `djfnjdjn`
- Question/Comment: `dsjfnjs`

Buttons for **Submit** and **Clear Form** are at the bottom of the form. Below the form, a footer contains links for [Privacy Policy](#), [Security Statement](#), [Server Status Check](#), [REST API](#), and copyright information for 2023 Altoro Mutual, Inc. A red banner at the bottom states: **This web application is open source! Get your copy from GitHub and take advantage of advanced features**.

A disclaimer at the bottom of the page reads: "The Altoro 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. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided 'as is' without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www.142.ibm.com/software/products/us/en/subcategory/SW110>. Copyright © 2008, 2023, IBM Corporation, All rights reserved."

The screenshot shows the `demo.testfire.net/sendFeedback` page, which displays a **Thank You** message. A JavaScript alert box is overlaid on the page, displaying the text: `demo.testfire.net says Prince` with an **OK** button. The background page content is identical to the previous screenshot, showing the sidebar, footer, and disclaimer.

#### Mitigation:

To mitigate XSS vulnerabilities, the website should properly validate and sanitize user input before displaying it on the page. In this case, the search query should be properly encoded or sanitized to prevent the execution of malicious scripts.

- To mitigate SQL Injection vulnerabilities, websites should use parameterized queries or prepared statements to handle user input. Parameterized queries ensure that user input is treated as data and not executable SQL code.