Reflected Cross Site Scripting (XSS) vulnerability was found in "/mcgs/admin/search-medicalcard.php" in PHPGurukul Medical Card Generation System v1.0 allows remote attackers to execute arbitrary code via "searchdata" POST request parameter.

Affected Project: Medical Card Generation System v1.0

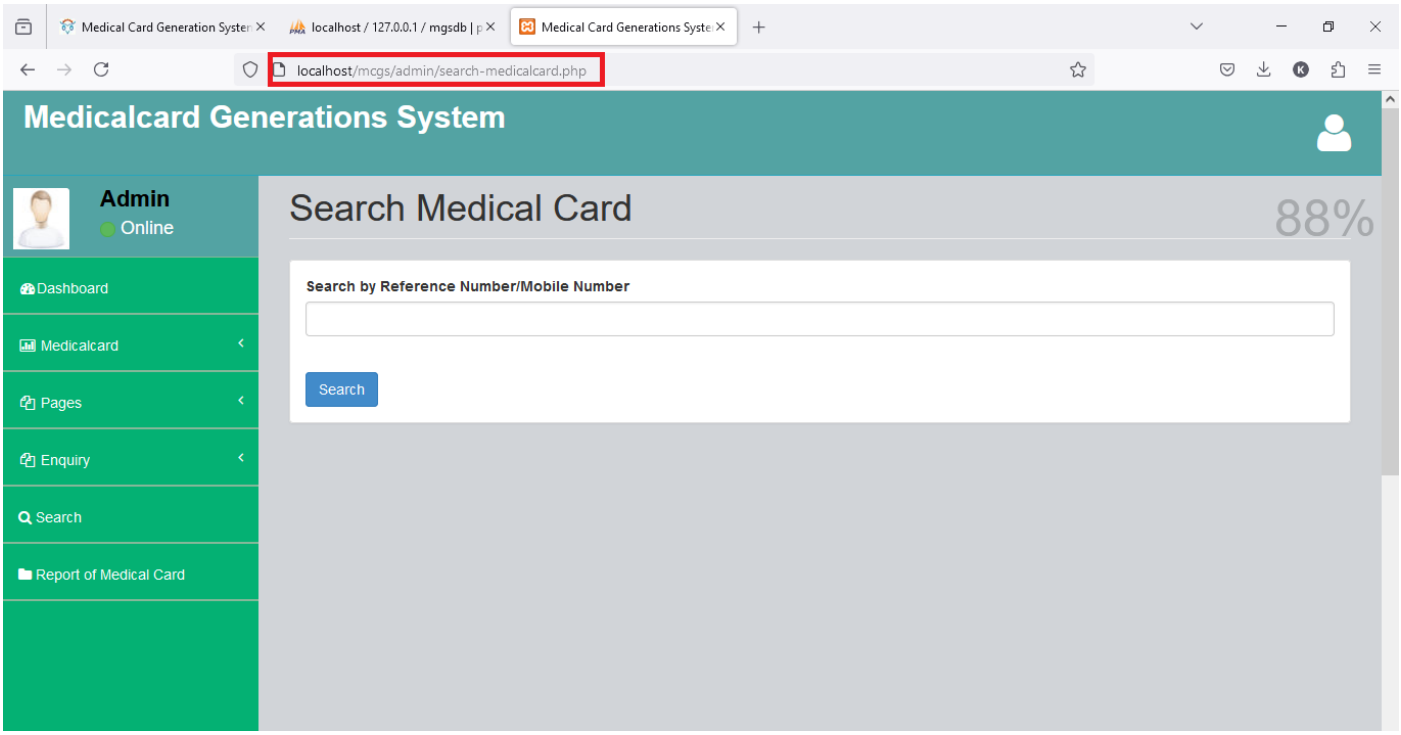
Official Website: https://phpgurukul.com/medical-card-generation-system-using-php-and-mysql/

Affected Components:

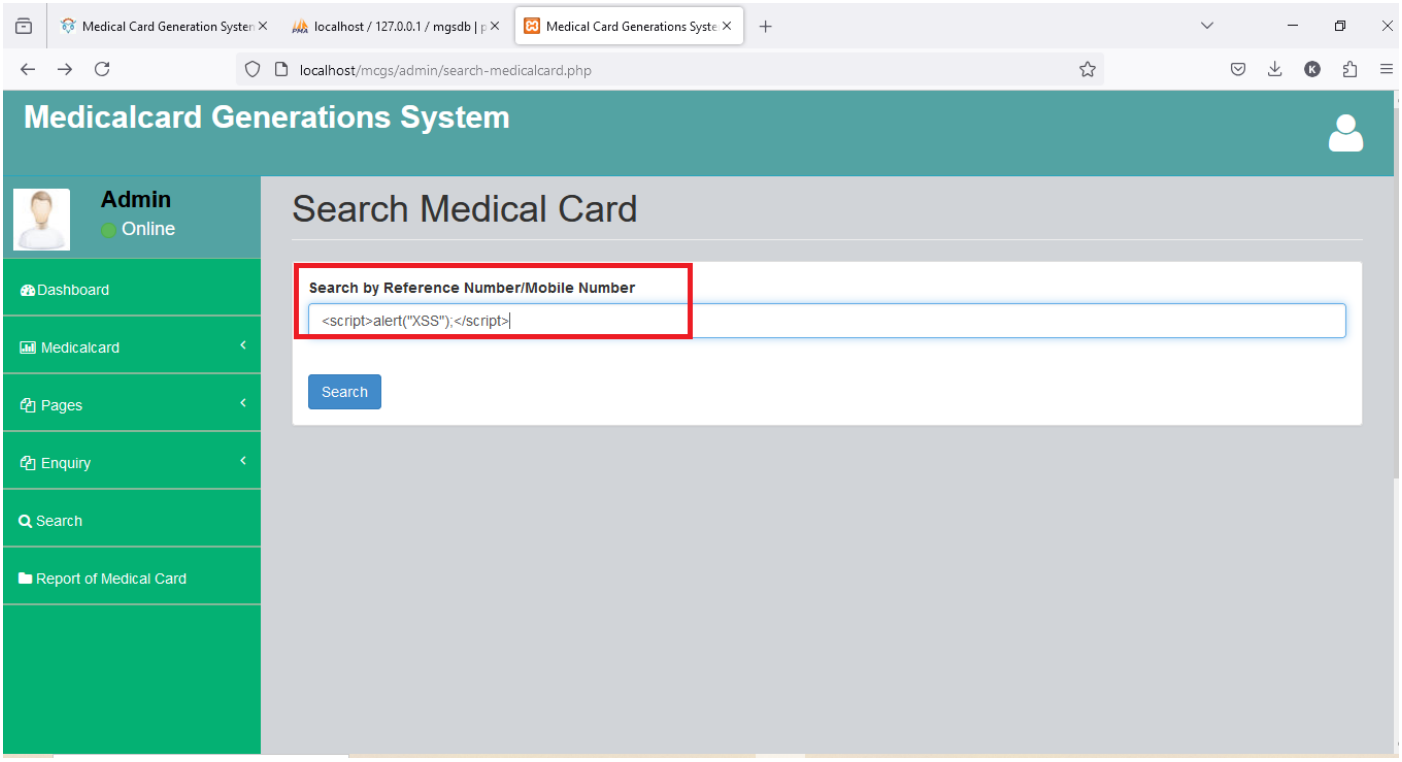
Affected File: /mcgs/admin/search-medicalcard.php

Affected Parameter: "/search-medicalcard " URL parameter

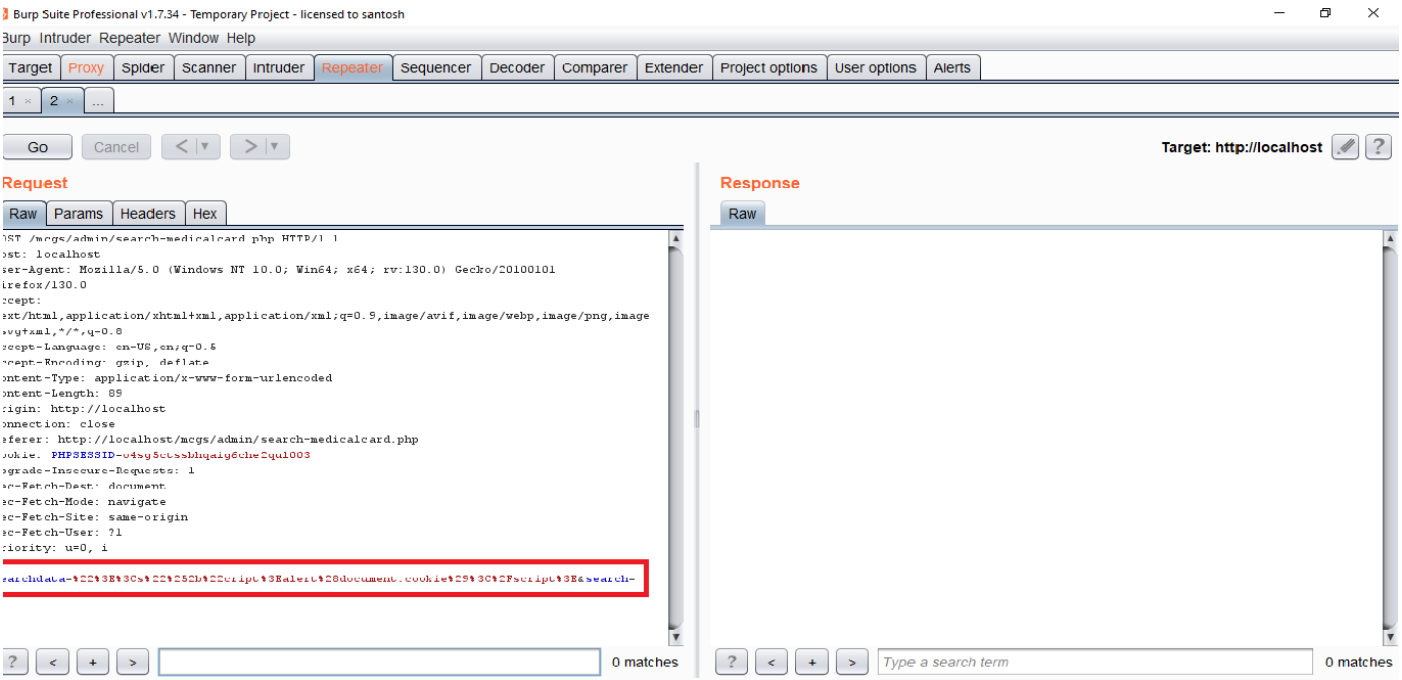
Step 1 : Access the Search Page URL: http://localhost/mcgs/admin/search-medicalcard.php

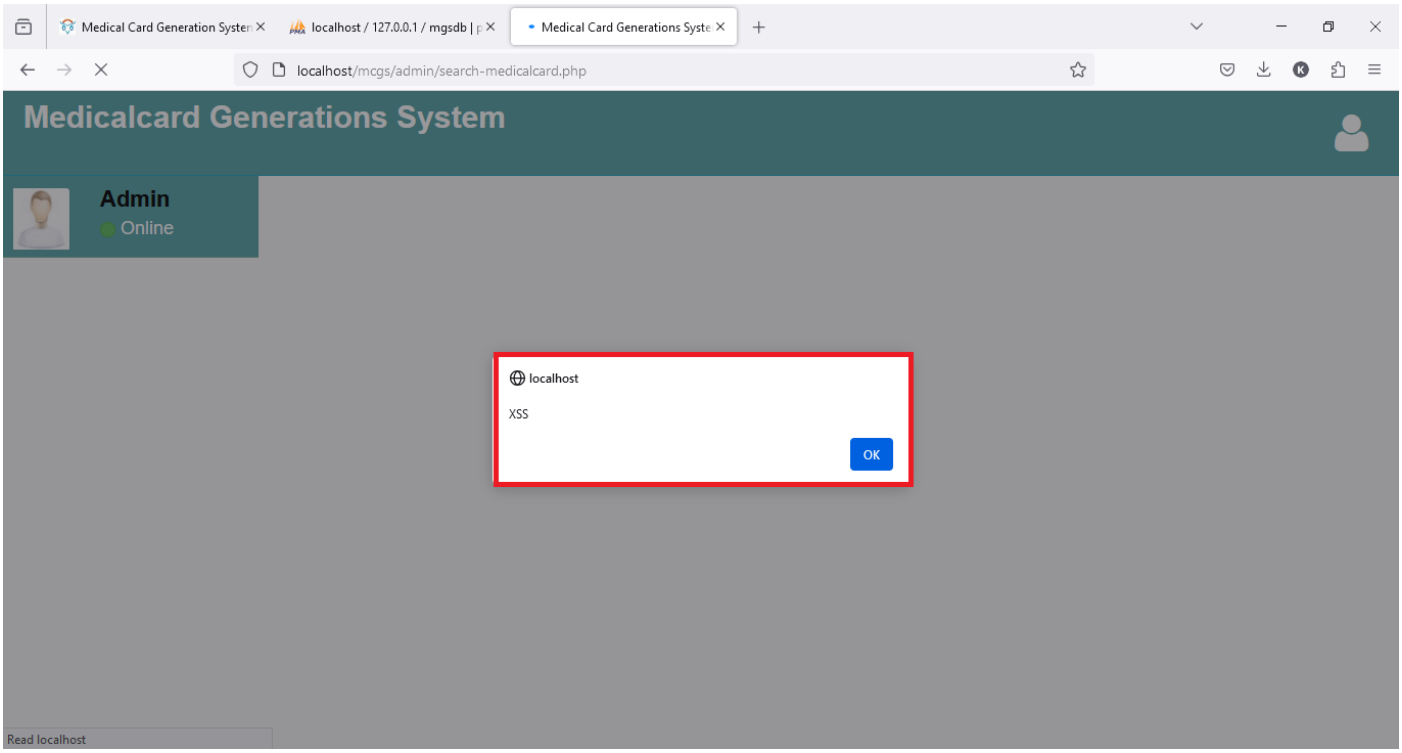


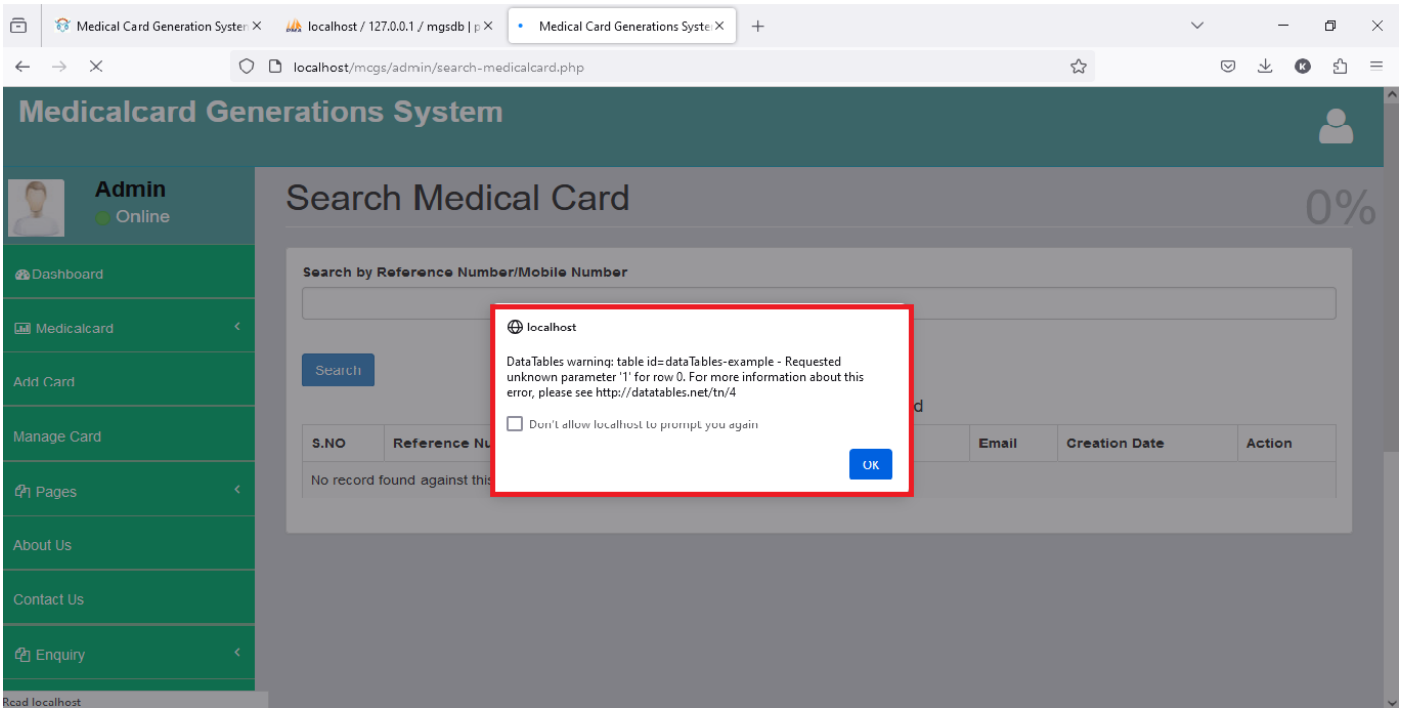
2. **Enter the test payload with XSS <script>alert("XSS");</script> in the search box and click "Search" button**



3. The XSS script is reflected back in the browser. The XSS script will get executed.







Output Encoding -> When you need to safely display data exactly as a user types it in, output encoding is recommended.

What is cross-site scripting (XSS) and how to prevent it? | Web Security Academy (portswigger.net)

https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html