Vulnerability Name: HTML Injection

Severity: Medium

Affected URL: http://localhost/mcgs/admin/search-medicalcard.php

Affected Project: PHPGurukul Old Age Home Management System v1.0

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

Version: 1.0

Affected Components:

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

• Affected Parameter: "searchdata" URL parameter

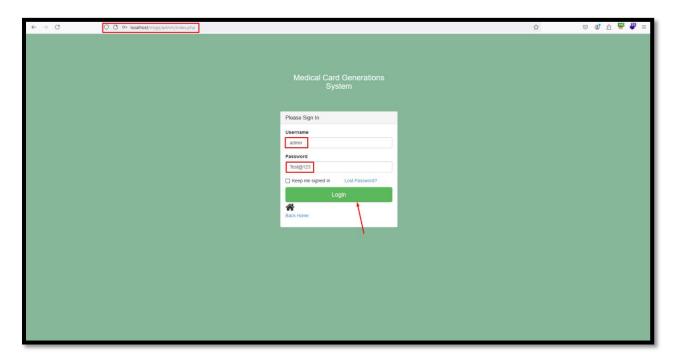
Description: HTML Injection, or Cross-Site Scripting, is a cybersecurity vulnerability wherein attackers insert malicious HTML code into a web application. This code is subsequently executed by unwitting users accessing the compromised page, potentially resulting in unauthorized actions or the exfiltration of sensitive data. HTML injection manifests in different types, including stored, reflected, or DOM-based XSS, based on where and how the injected code is handled.

Impact: Exploiting this vulnerability empowers attackers to manipulate the appearance and functionality of a webpage. This may result in compromised user accounts, malware dissemination, or the execution of phishing attacks.

Remediation: Prevention entails implementing input validation, output encoding, and security measures such as Content Security Policy (CSP) to mitigate HTML injection risks and bolster the security of web applications.

Proof of Concept:

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



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



Step 3: In search bar, provide values **<h1>HTML INJECTION</h1>** and enable burpsuite to confirm the parameter.



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

```
Forward Drop interceptis on Action Open browser

Pretty Raw Hex

1 POST /mcgs/admin/search-medicalcard.php HTTF/1.1

2 Host: Localhost
3 User-Agent: Nozilla/5.0 (Vindovs NT 10.0; Vin64; x64; rv:130.0) Gecko/20100101 Firefox/130.0

3 User-Agent: Nozilla/5.0 (Vindovs NT 10.0; Vin64; x64; rv:130.0) Gecko/20100101 Firefox/130.0

4 Accept-Lenguage: en-US,en;qu0.5

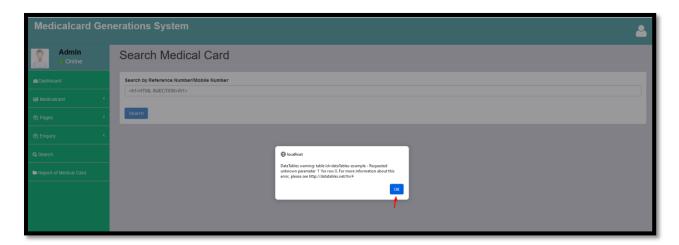
5 Accept-Lenguage: en-US,en;qu0.5

6 Content-Type: application/xml-year-form-urlencoded

8 Content-Type: application/xml-year-form-urlencoded

9 Cotinin http://localhost
10 Connection: Keep-alive
11 Refere: http://localhost
10 Gookie: PHPSESID-903;praie;SoComf28dSobbbkh
11 Refere: http://localmost/search-medicalcard.php
13 Sec-Fetch-Dest: Gookies: 121
14 Sec-Fetch-Dest: Gookies: 121
15 Sec-Fetch-Dest: Gookies: 121
16 Sec-Fetch-Dest: Gookies: 121
17 Sec-Fetch-Site: seame-origin
18 Ptiority u=0, i
19 Ptiority u=0, i
```

Step 5: Here pop button click on ok.



Step 6: Here is show on HTML Injection

