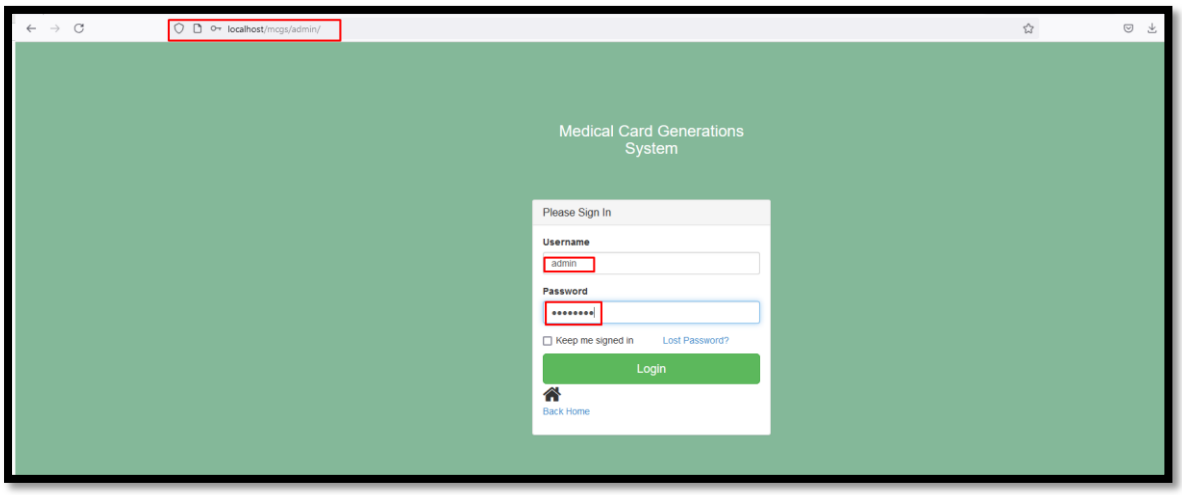
HTML Injection vulnerability was identified in the **mcgs/admin/card-bwdates-report.php page** of the **Medical Card Generation System using PHP and MySQL**. This flaw allows remote attackers to inject malicious HTML code via the **fromdate and todate** parameters in a **POST** HTTP request, potentially affecting page rendering, manipulating content, and compromising system integrity.

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

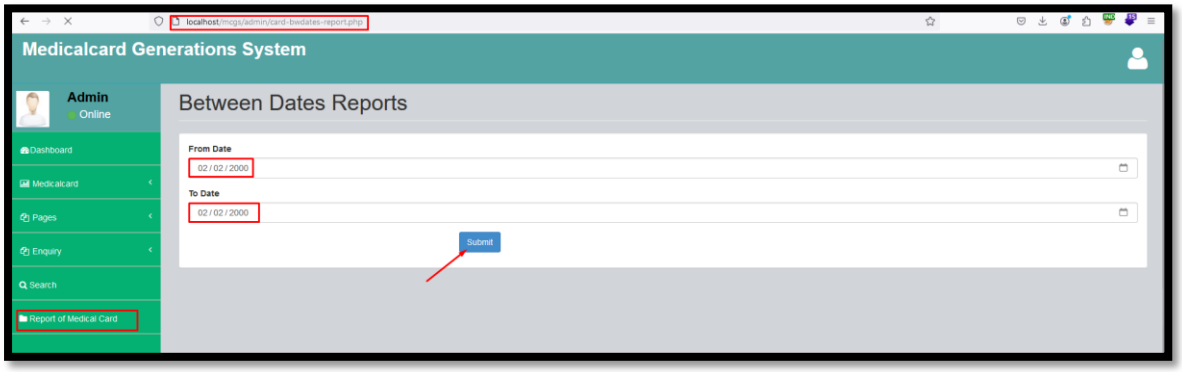
Affected Vendor	PHPGurukul
Affected Product Name	Medical Card Generation System using PHP and MySQL
Version	V1.0
Affected Code File	mcgs/admin/card-bwdates-report.php
Affected Parameter	fromdate, todate
Method	POST
Vulnerability Type	HTML Injection

Step to Reproduce:

Step1: Visit to http://localhost/mcgs/admin/ , log in with admin credentials (Username and Password).



Step2: Go to the Report of medical card tab feel the require details click on submit. And click on Add. Enable Burp Suite intercept, and send the request.



Step3: Insert the payload into the **fromdate** and **todate** parameters as shown in the screenshot. And forward the request.

Step4: Now notice the given HTML payload executed and stored on web server.