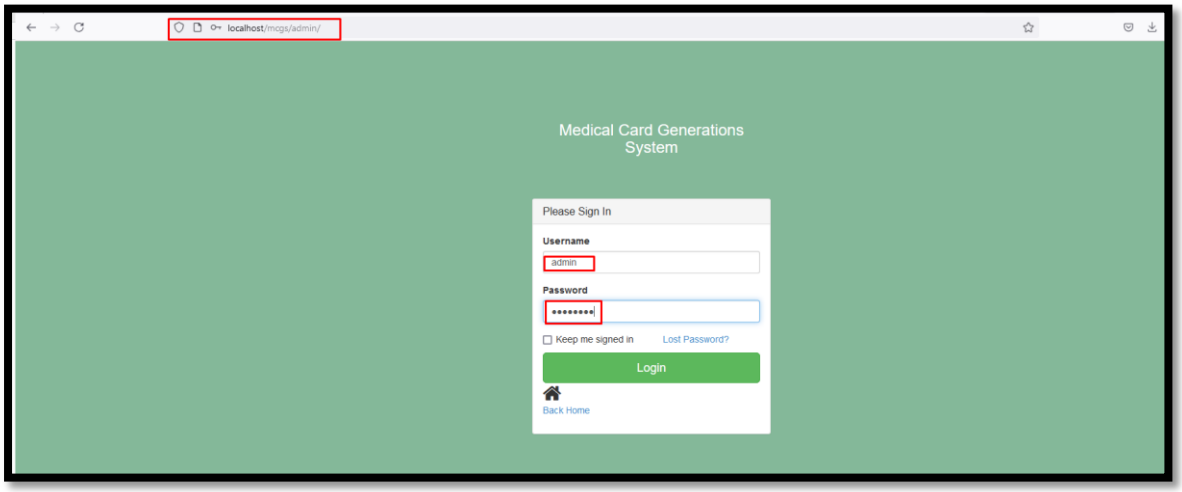
Stored Cross-Site Scripting (XSS) vulnerability was identified in the **mcgs/admin/aboutus.php** page of the **Medical Card Generation System using PHP and MySQL**. This flaw allows remote attackers to inject and store malicious scripts via the **"pagetitle"** parameter in a **POST** HTTP request, which will execute whenever the affected page is accessed, compromising user sessions and system integrity.

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

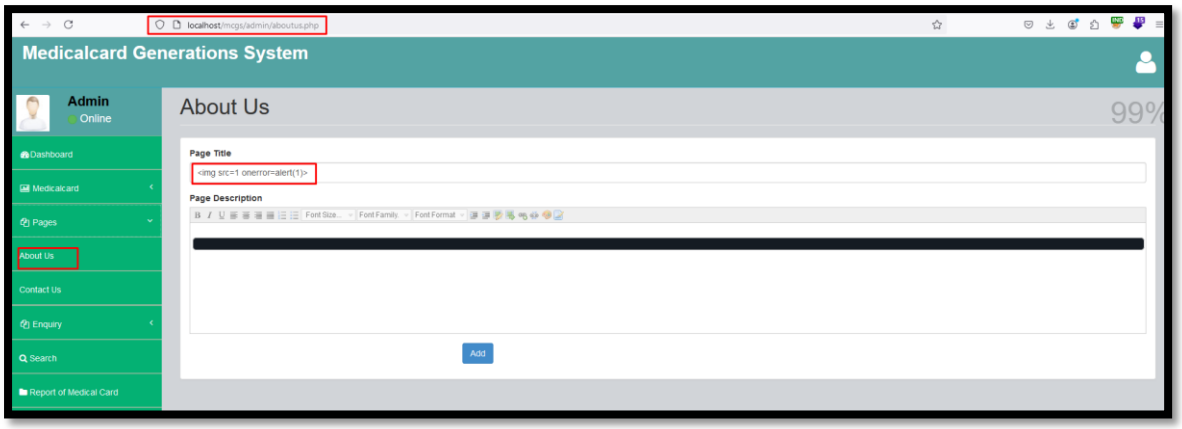
Affected Vendor	PHPGurukul
Affected Product Name	Medical Card Generation System using PHP and MySQL
Version	V1.0
Affected Code File	mcgs/admin/aboutus.php
Affected Parameter	pagetitle
Method	POST
Vulnerability Type	Stored XSS

Step to Reproduce:

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

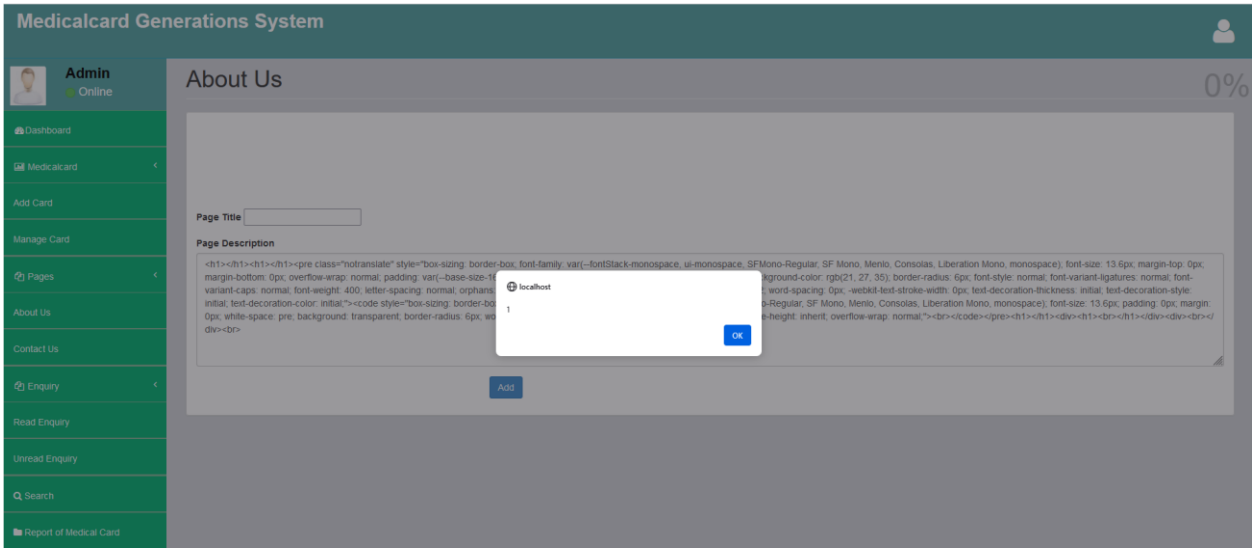


Step2: Now go to the Pages tab and click on About Us. Here insert the payload **(<img src=1 onerror=alert(1)>)** and click on Add. Enable Burp Suite intercept, and send the request.



Step3: Intercept the request and click on forward the request.

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



Mitigation/recommendations

- Cross Site Scripting (XSS) Prevention Techniques - GeeksforGeeks
- Cross Site Scripting Prevention - OWASP Cheat Sheet Series