| | |
|---|---|
| **Vulnerability Name:** | HTML Injection |
| **Affected Vendor** | PHPGurukul |
| **Affected Product Name** | Medical Card Generation System using PHP and MySQL |
| **Product Official Website URL** | https://phpgurukul.com/medical-card-generation-system-using-php-and-mysql/ |
| **Affected Components** | Version: V1.0<br>Affected Code File: /mcgs/admin/contactus.php<br>Affected Parameter: pagedes<br>Method: Post |

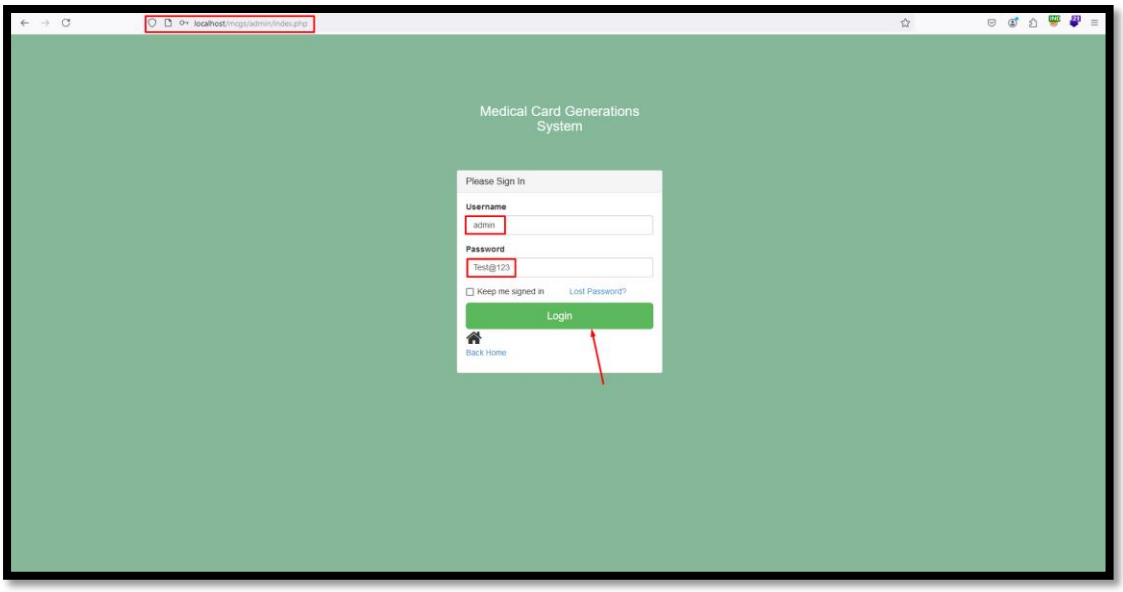
**Description:** HTML Injection, or Cross-Site Scripting, is a cybersecurity vulnerability wherein attackers insert malicious HTML code into a web application. This code is subsequently executed by unwitting users accessing the compromised page, potentially resulting in unauthorized actions or the exfiltration 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.

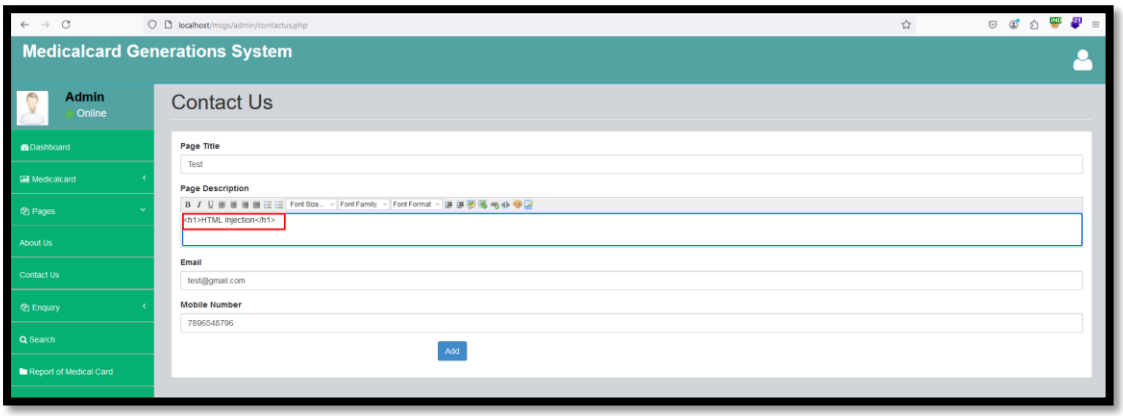
**Proof of Concept:**

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

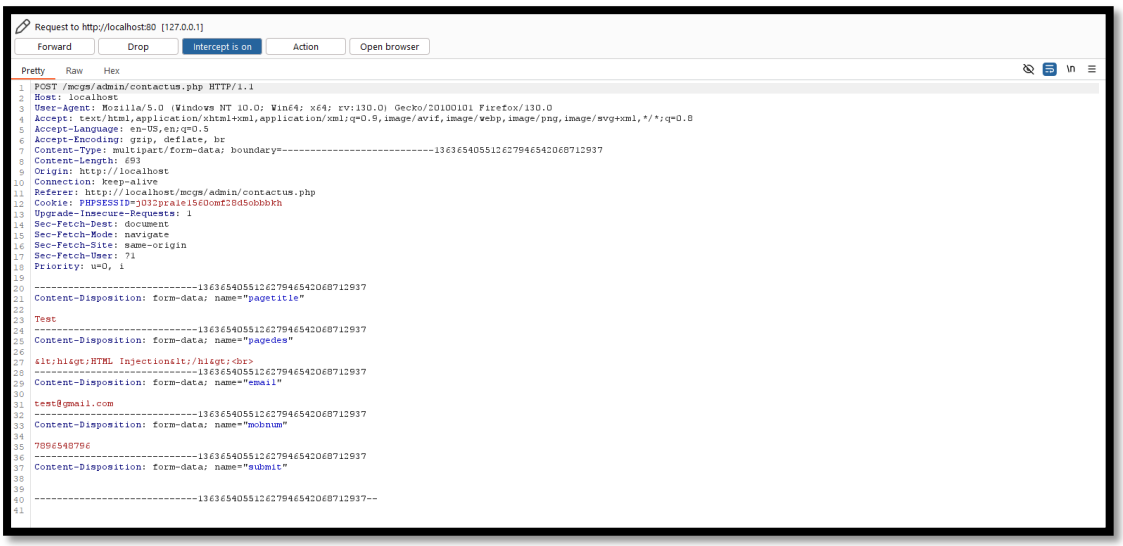


**Step 2:** Here login with admin and click on search which is shown on below image.

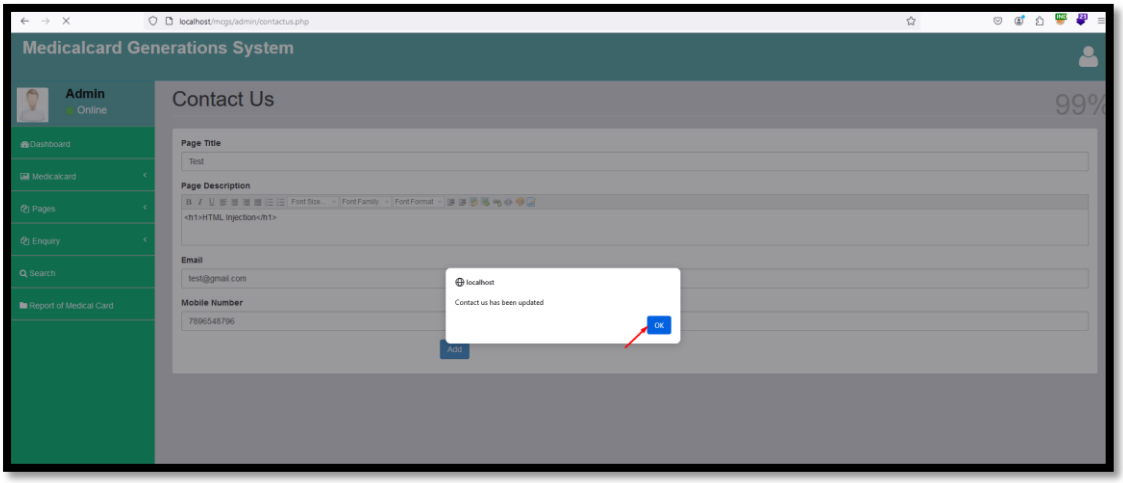

**Step 3:** In search bar, provide values **<h1>HTML Injection</h1>** and enable burpsuite to confirm the parameter.




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



**Step 5:** As request is forwarded notice in the browser, here pop button click on ok.




**Step 6:** Payload is executed with HTML Injection.