

XSS injection vulnerability exists in exam parameter of /view/exam\_timetable\_grade\_wise.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 and Response tabs of a web browser's developer tools. The Request tab on the left shows an HTTP GET request to `/std1/view/exam_timetable_grade_wise.php?do=show_exam_Timetable&exam=6'()%26%25<zzz><ScRiPt%20>alert(9932)</ScRiPt>&grade=13`. The Response tab on the right shows the HTML output, which includes a warning about `mysqli_fetch_assoc()` and a button with an `onClick` event. The injected payload `<ScRiPt>alert(9932)</ScRiPt>` is visible in the response, and the search bar at the bottom right shows a match for `alert(9932)`.

Payload: `exam=6'()%26%25<zzz><ScRiPt%20>alert(9932)</ScRiPt>`

Source Download:

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