

XSS injection vulnerability exists in category parameter of index.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' details for a POST to /std1/index.php. The 'category' parameter in the request body is highlighted with a red box, showing the injected payload: `1'()%26%25<zzz><ScRiPt%20>alert(9508)</ScRiPt>`. The right pane shows the 'Response' details, which is an HTTP 200 OK. The response body contains HTML output, and the injected JavaScript code is highlighted with a red box, showing: `<ScRiPt > alert(9508) </ScRiPt>`. The bottom status bar indicates 'Done' and '404 bytes | 3 millis'.

Payload: `category=1'()%26%25<zzz><ScRiPt%20>alert(9508)</ScRiPt>`

Source Download:

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